New for 2023/2024

Privacy, Data Theft & Digital Fraud

Keynote, 2 hour, Half Day Seminar, One Day Seminar

How did Home Depot wind up sharing customer information with Meta? How did a Cincinnati hospital wind up sending patient information to Meta and other third parties? Why did a Mall use facial recognition software to target shoppers inside the building?

There's no two ways about it. Cybersecurity is on everyone's mind. Data breaches have dominated the news cycle long enough for small and large businesses, front-line employees and risk managers alike to know how serious cybersecurity risk can be. But what happens when the data wasn't stolen but willingly shared?

Privacy Impact Audits are essential for any sustainable privacy compliance framework to ensure that organizations are aware, from the outset, of the possible consequences of their data leaking to outside sources. The role of internal audit is especially important regarding this topic and how to mitigate risk of data exposure.

Discussion points include:
The protocols and policies needed to prevent these types of incidents from occurring
Understanding the risks of free promotional materials and how to assess them.

Battling Disinformation: How Hackers & Trolls Attack your Company, your Staff and your Mind

Keynote, 2 hour, Half Day

Social media is a dominant force in today's world of connectedness. A report published by Hootsuite states that there are over 3 billion people using social media today. That is about 40% of the world's population. This has given social media platforms unprecedented power to wreak havoc on societies and individuals.

There is little effective legislation to regulate social media companies and individuals are mostly powerless in curbing the enormous damages caused by the technology. Initially a perfect platform for scammers, it didn't take long for corporations, governments and malicious actors to want a part of the social media landscape.

A less discussed component is the risk social media proffers on battling the human instinct to believe and share bad news, fake news and all news without question. Battling artificial intelligence, trolls and bots is an overwhelming task that has humanity beat at present.

Learning how social media works against us and having strategies to navigate its many problems is more valuable than ever before. It's time to make digital literacy a priority for individuals.

**Contact us for a detailed outline of the seminar*

Cybersecurity: The Social Risk & The Latest Scams

Keynote, 2 hour, Half Day Seminar, One Day Seminar

Social media is a dominant force in today's world of connectedness. Its use is still growing in all parts of the world, and with that, the risk is growing exponentially. Within an organization, use of social media by different departments can compromise the reputation of the organization and staff. Changes in internet usage, such as the proliferation of mobile devices and the rising use of social media, have presented new challenges for cybersecurity.

A significant sticking point when it comes to properly leveraging social media is dealing with the many risks to which companies are exposed. Assessing corporate risk on social media is only one area that needs to be watched. The social media usage of our employees and suppliers is another area that needs to be monitored as it is the easiest way hackers gain entry into our networks.

No One Cares About Your Data (Not Even You): Securing Your Data in the Digital Age.

Keynote, 2 hour, Half Day, Full Day

540 million Facebook records. 5 billion Yahoo accounts. 500 million Marriott guests. Voting records for 198 million Americans. These are just a few of the massive breaches we've learned about in recent years... and just as quickly forgotten. Hack after hack, company after company, we simply do not know where to begin to secure our data or our privacy - not as consumers, not as companies, and not as governments. This session will explain how and why our cybersecurity is in such steep decline, and what we can do to truly protect our data.

Protecting your online privacy is more important today than it ever was. Around the world, online activities have increasingly become a central part of daily life. You send email, check your social network account or the weather, stream videos, tweet, share photos, download music, back up files using online services like OneDrive or Dropbox, and create documents.

Organizations that collect and use your information have responsibilities to protect it. However, you can take various precautions to protect yourself from identity fraud or the misuse of your information, or to ensure that your privacy is respected in the way you would want.

Learning Objectives:

- Understand what information is available about you online
- How to control the information that is out there about you
- How to remove personal data about you online
- Learn to actively manage your online footprint

Words Never Lie but People Do – Improve Your Interviewing Skills

Keynote, half day, full day, two day, three day

Learn the techniques used by FBI profilers. Gathering truthful information is an integral part of any corporate environment. How important is it for us to learn the truth from our employees, managers, and clients? This overview presents how linguistic lie detection is used in business, audit, and investigative areas to help you become more effective in all your business communications. As a session participant, you'll learn the basics of information gathering and how to interpret the information you receive. You'll also learn how linguistic lie detection techniques can be applied to a variety of high-profile media cases to illustrate examples of deception including:

Day One, Level 1 learning outcomes

- How to determine if a person is speaking truthfully or untruthfully.
- How often deception is used in the workplace.
- Specific linguistic triggers that indicate deception.
- What types of questions produce the most effective responses?
- How linguistic lie detection is used for human resources, audit, and investigative areas.

Day Two, Level 2 learning objectives

- reinforce the skills learned from day 1 and put them to use analyzing statements
- learn to hear linguistic triggers from listening to verbal testimony
- learn new linguistic markers in detecting deception
- refine your interview strategies

NEW Level 3 Linguistic Lie Detection: Color Coding & Analysis

Half Day, Full Day

Now that course participants have completed two levels of linguistic analysis training, level 3 brings us to the color coding stage of statement analysis. Participants will use this technique to map out analysis in a detailed format. From this we advance to the

determination of interview questions. Learn how to formulate questions based on the information revealed in the analysis of the statement. Build a non-confrontational rapport with the person you are interviewing.

Learning outcomes:

- Incorporate color coding techniques to assist in analyzing statements
- Learn new linguistic triggers

Half day session only covers color coding

Social Engineering & Social Media Risk: What every professional needs to know

Keynote, 2 hour, half day seminar & full day seminar

Social media is a dominant force in today's world of connectedness. Its use is still growing in all parts of the world, and with that, risk is growing exponentially. Within an organization, use of social media by different departments can compromise the reputation of the organization and staff. Changes in internet usage, such as the proliferation of mobile devices and the rising use of social media, have presented new challenges for cyber security.

As long as staff are connected and online, the risk of cyberattacks is imminent. Discover how the social engineer uses social media to gather information on your organization and people

This session is designed for those responsible for governance and risk management to align strategies to adapt to the changing social media landscape.

- Discuss fallout from real life cases of cybersecurity breaches from social media.
- Tips on cybersecurity strategies & social media policies.
- Discuss a pragmatic approach toward combating cyber threats.
- What needs to be in the social media policy

Beyond Google: Conducting Investigations & Research Online (OSINT)

Keynote, 2 hour, Recommended as 2 day class – available as one day seminar

The internet is a valuable tool for gathering information and building investigation data. Online research and analysis skills are necessary requirements at every level of an organization today. Both the public and private sectors need to acquire useful and relevant information from resources online. Open Source Intelligence (OSINT) requires much more than just an ability to surf the Web.

Aimed at managers, auditors, frontline investigators, researchers, and analysts alike, this one or two day course will provide detailed instruction on effectively using the Internet as an Open Source Intelligence, research, and investigation tool.

- Staying safe and private while online.
- Learn how to effectively use search engines to gather information.
- Learn how to obtain information from social media sources.
- Access information from corporate and public record searches.

Ethics

Ethics: Making Ethical Decisions in a time of Uncertainty
Keynote, 2 hour, half day, full day

Ethics & the Fake News Dilemma
1 hour, 2 hour, 4 hour, full day

Hailed by many participants as the best ethics course ever, Ethics Viewpoint illustrates the challenges in implementing an organization wide ethics policy. Explore how best to embed ethics into a corporate culture.

Ethical issues are associated with workplace deviance or corruption and its counterparts – lying, evasion of accountability, and abuse of authority. What causes them and how should they be dealt with? This session focuses on integrating ethics with everyday corporate life. Ethics breaches begin with people – understand the team you work with. In an interactive session, participants will put into practice ethics issues that will help build a strong ethical business culture.

The seminar's topics include:
- Personal ethics vs. professional ethics
- How easy are ethics to define in the workplace?
- Does employee behavior influence ethical practice?
- Most common ethical breaches

Ethics learning outcomes:
- Identify the various components that go into assessing ethical breaches
- Gain experience in presenting and evaluating ethical arguments
- Develop ethical frameworks, so as to attack moral/ethical problems critically and comprehensively

****We offer 4 different ethics courses for repeat clients****

Social Engineering: The New Corporate Espionage. A Primer
Keynote, half day or full day

Discover how vulnerable your organization can be to social engineering and it's easier than we think. The greatest security threat any organization faces today is the human

threat. This session exposes the good, the bad, and the ugly about social engineering today. You will discover how easily confidential information leaks out of your organization daily.

In this session, participants will:

- Recognize how the bad guys can infiltrate your organization.
- Understand how the good guys mitigate the problem.
- Learn how to incorporate human vulnerability checks into your organization.

Targeting the Top: How Senior Management Poses a Great Risk for Cyberattacks

Keynote, 1.5 hour

The FBI reported that over 3 billion dollars were lost between 2015 and 2016 due to CEO scams. Discuss the most common scams organizations encounter that relate to senior management.

- Find strategies to assist cyber awareness
- How to reduce fraud and anticipate cyber-attacks against your organization;

For additional information please contact
Nejolla Korris, CEO
www.interveritas.com
nkorr@interveritas.com

Nejolla Korris Bio

Nejolla Korris is an international expert in the field of Linguistic Lie Detection and Cybersecurity - Social Engineering and Social Media Risk. She is the Chief Executive Officer at Interveritas International.

She is skilled in Scientific Content Analysis (SCAN), a technique that can determine whether a subject is truthful or deceptive. Since 2000, Korris has analyzed documents for fraud, international security, arson, sexual assault, homicide, and missing persons' cases, causing some of her clients to dub her the "Human Lie Detector." Nejolla was one of five sanctioned trainers worldwide in the SCAN methodology. She has worked with Singapore police, FBI & cold case units of Scotland Yard and Irish Garda as well as several other law enforcement agencies. She introduced the methodology to the business community helping train professionals in detecting deception and honing interview skills.

In 2010 Ms. Korris added social media risk and social engineering training and consulting to her portfolio. She was approached by a firm of penetration testers to develop the social engineering ruses used to hack into corporations otherwise known as people hacking. This is used to train staff to recognize online threats and scams. Korris works with all levels of management, IT and internal audit to determine risk and prevention strategies for corporations and their staff.

In 2017, Nejolla was invited to present a keynote at the World Association of Newspapers conference in Singapore. She was invited by the Canadian High Commission to speak on the Fake News epidemic and how citizen groups are fighting it.

Ms. Korris is a highly sought after speaker in the areas of linguistic lie detection, social media risk, social engineering, fake news and the dark side of ethics. Nejolla is a unique voice in the world of intelligence and security. Her sessions are highly entertaining and interactive bringing rave reviews from audience members. Her speaking is insightful as well as entertaining.

Nejolla has worked in over 40 countries throughout the world. Her clients include corporations, government agencies, law enforcement, and the military. Nejolla has a BA in Law from Carleton University in Ottawa, Canada. She was awarded the Queen's Diamond Jubilee Medal in 2012 for her international work in linguistic lie detection. She has one son Taddes and is owned by her dachshund Picasso.