President's Message
Kristina Davis

I can’t believe it is already 2018. With the new year, comes new hopes/plans/resolutions. One of my hopes for this year is that more of our members get active in the chapter and come out to our CPE events and chapter activities.

In full disclosure, IIA HQ is monitoring our chapter for activity and financial viability. I was contacted in December to discuss ways to increase our chapter’s participation in events and activities. They also questioned why we were having quality speakers (aka not free) with our low seminar attendance. I guess I am guilty of having the “little engine” syndrome in that I think our chapter can hold quality CPE events and at least break even or get close. But that has not been happening these past few seminars. While the chapter does have money in the bank, our surplus is beginning to wain based on losing money on the seminars.

In saying that - our Winter Seminar will be Thursday, January 25th, 2018 at TMC in Daphne. I think getting 8 CPEs for a little over $100 is a deal – hope you do, too, and sign up soon. Please support the chapter!

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.

Hope to see you soon - Kristina

Alfred Lord Tennyson

“Hope smiles from the threshold of the year to come, whispering, 'It will be happier.'"
Realistic Security: Counter Advanced Threats With Basic Controls

January 16, 2018  Course Duration: 1 hour
1:00–2:00 p.m. ET  CPEs Available: 1

Organizations direct immense effort into advanced security solutions, only to be undone time and again by basic attacks. Why do organizations struggle, and usually fail, to secure themselves when the market is flooded with highly sophisticated tools all contending to be “the solution to advanced threats”? The answer is straightforward but unpleasant. Most organizations simply are not ready for “advanced solutions” because they have not properly implemented basic solutions. In many cases the boring, grinding, annoying basic solutions will do more good for an organization, but it is just so much easier to write a check and pretend that you can buy security. In this session, we will walk through real-world data breaches from the last few years and discuss what simple (and elementary) solutions would have prevented these attacks.

Learning Objectives

In this session, participants will learn:

- The standard flow of how attackers work.
- How removing simple attacks significantly reduces the population of attackers that are skilled enough to actually breach your organization.
- The most common basic controls that, when implemented correctly, give you the best “bang for your buck” for protecting your network.

Speaker: Daimon Geopfert
National Leader, Security and Privacy Services, RSM US LLP
Daimon Geopfert specializes in penetration testing, vulnerability and risk management, security monitoring, incident response, digital forensics and investigations, and compliance frameworks within heavily regulated industries. Daimon has over 20 years of experience in a wide array of information security disciplines. He serves RSM’s national leader for the security and privacy practice, responsible for the development of the firm’s overall strategy related to security and privacy services and applicable methodologies, tool kits and engagement documentation

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.
Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA, is president and CEO of The IIA. In Chambers on the Profession, he shares his personal reflections and insights based on his 40 years of experience in the internal audit profession.

**Five Internal Audit Resolutions for 2018 and Beyond**

When a new year dawns, people tend to embrace it with optimism and confidence despite the uncertainty that lies ahead. I don't know whether this hopeful outlook is driven by the celebration that surrounds the date or whether that optimism is what drives the merriment. Whatever the case, the New Year also pushes us to set goals and resolve to better ourselves.

My custom for the past several years is to use my first blog post of the year to set out New Year’s resolutions for the profession that highlight emerging or anticipated issues. For example, the upcoming May 2018 deadline to meet new European Union rules on personal privacy protection would meet the criterion. This year, however, I'm taking a more strategic view that sets out resolutions that will help practitioners become more engaged and future focused in 2018 and beyond.

Like never before, stakeholders are turning to internal audit to help the organization navigate risks and opportunities. To me, this is clear evidence that the profession is making steady progress toward earning “a seat at the table” and becoming the trusted advisor in every organization. We must, therefore, focus on developing new skills to meet new demands and draw on the fortitude and courage needed to take difficult challenges head on.

These five resolutions will help us get there.

**Maintain a Laser Focus on the Horizon** Over the past year, I have frequently used the analogy of weather to describe the work we do, and it fits into this resolution. Internal auditors should position themselves to become the Doppler radar for emerging risks that threaten their organizations.

For many, this will require stepping out of the traditional comfort zones of financial, compliance, and operational internal auditing. However, we cannot offer our organization that crucial glimpse beyond the vanishing point without understanding broader strategic risks driven by geopolitics, macroeconomics, cybersecurity, technology, and other factors.

**Take the Offense in the War on Talent** One of the greatest challenges we must overcome is to obtain and retain talent. If we are to not just meet but exceed growing stakeholder demands, we must ensure we have the necessary resources and skill sets on hand. This begins by understanding the unique risk pool for your organization and the industry in which it operates. For example, the risk pool for finance is worlds apart from the risk pool for chemical manufacturing. Once you have a handle on those risks, recruit or train staff that is attuned to those areas and has the requisite skills to audit them.

We also must hire talent or secure co-sourcing relationships that allow us to expand and improve our ability to audit specialized risks or those that require specialized expertise. We cannot look away from risks simply because we do not have the expertise to address them.
**Sharpen and Deploy the Best Navigation Tools** Technology has always provided the means to attain higher levels of efficiency and efficacy. We must become expert at employing the tools available to internal auditing from audit management systems, data analytics, and artificial intelligence to new technologies that will inevitably emerge. The challenge is to identify and embrace technology that will make internal audit functions agile and future focused.

**Innovate Your Way Through Transformation** Disruption often presents lethal risks where only innovation can provide the path forward. Internal audit should champion transformation built on innovative thinking and actions.

This may require some changes if the corporate culture is averse to failure. Innovation involves trial and error, so a culture that punishes or fixates on failure will struggle to innovate. One important caveat is to not simply conflate innovation with technology. While technology often drives and supports innovation, the two are not synonymous.

**Sail Toward the Storms** Great internal audit departments do not fear difficult or uncomfortable topics. They sail toward the storms in order to alert management and the board when risks are not being managed and controls are not adequately designed and implemented.

In a blog post last year I wrote that internal audit may sometimes be the lone and unwanted voice alerting the organization to risks or problems. This at times places practitioners in the crosshairs of those who are quick to shoot the messenger. Do not let this discourage you. The best internal auditing requires courage, and courage does not wait for a chorus.

As always, I look forward to your comments.

---

**IIA Releases New Practice Guide on Liquidity Risk**

Recognizing that financial services auditors face unique challenges that require tailored guidance, The IIA has released Auditing Liquidity Risk, An Overview, the first IPPF practice guide specifically for financial auditors.

This practice guide takes the reader through an overview of Auditing Liquidity Risk covering the following topics at a high level:

- History of the regulatory environment surrounding liquidity risk management.
- Importance of liquidity risk management to a financial institution.
- The fundamental principle for the management and supervision of liquidity risk
- Governance of liquidity risk management:
- Liquidity risk appetite and risk tolerance/
- Planning for internal audit engagements regarding liquidity risk management.
- Measurement and management of liquidity risk.
- Public disclosure requirements.
- Role of supervisors.

IIA members are invited to download guidance as a benefit of membership. Nonmembers may purchase Supplemental Guidance by visiting The IIA Bookstore.
Casinos and other gambling-related businesses should protect themselves from being money-laundering tools for fraudsters.

Art Stewart

The Royal Canadian Mounted Police (RCMP) have seized more than CAN$9 million as part of a multinational money-laundering investigation dubbed E-Pirate, the Vancouver Sun reports. Government documents allege that Paul King Jin, who owns a British Columbia spa, orchestrated a CAN$500 million money laundering service involving casinos and underground banks in Canada, China, and Macau. Investigators say Jin helped wealthy Chinese individuals gamble in British Columbia casinos using suspected drug cash he supplied through underground banks linked to Chinese organized crime groups. The RCMP seized more than CAN$2 million during a raid of Silver International Investment, an unlicensed British Columbia-based bank that allegedly funneled money to gamblers, and another CAN$1 million in suspected drug money when it stopped two individuals seen entering Silver’s offices. According to ledgers uncovered during its raids, Silver laundered CAN$220 million in cash and sent more than CAN$300 million offshore in a single year.

Lessons Learned

Money laundering doesn't necessarily involve fraud, but the two are linked because the proceeds from fraud often need to be laundered in order to be kept or spent. The amounts of money involved can be enormous, and the laundering schemes are complex, making their deterrence and detection challenging. The RCMP's E-Pirate investigation illustrates how money laundering works. In this case, investigators say drug dealers laundered their profits — $1 million, for example — through underground banks in Canada and then in China. In turn, the Chinese bank lent the $1 million to a gambler who went to a legitimate casino and converted the money into chips. The gambler then cashed in the chips for $1 million, now "laundered," which was available for investment or other uses.

To combat such money laundering schemes, regulators and gambling institutions must establish rigorous anti-money laundering (AML) programs and thoroughly monitor them to keep them up to date. In a similar case in Australia involving wagering company Tabcorp, a federal court judge cited the "insufficient resourcing together with insufficient processes for consistent management oversight, assurance, and operational execution" in approving a AUS$45 million fine against the company for violations of Australia's Anti-Money Laundering and Counter-Terrorism Financing Act between 2010 and 2014, according to The Sydney Morning Herald. Casinos and other gambling-related businesses can address such concerns by making these improvements:

- Undertake a risk-based approach and assessment. Many countries have laws requiring companies to have a policy and procedure in relation to assessing and managing money laundering risks. This involves discrete steps for assessing the most proportionate way to manage and mitigate the specific money laundering and terrorist financing risks the organization faces. These methods include policies, procedures, controls, monitoring, and review.

- Conduct customer due diligence inquiries. These inquiries should confirm the identity of customers engaged in large or frequent transactions by examining valid, government-issued photo identification documents. Casinos also should look into a player’s source of wealth and funds to measure risk. For customers who are assessed as higher risk, casinos should limit the types of permitted transactions.

- Monitor and report large cash transactions and payments to customers. Canada requires reporting of transactions of CAN$10,000 or more as well as of suspicious transactions of any amount. Unlike banks, casinos don't refuse many money transactions because of revenue considerations. However, they should stop...
suspicious transactions to help prevent money laundering. Moreover, political will is needed to require casinos to report large transactions.

- **Report suspicious activity.** Casino employees should be required to report information that comes to them within the course of business where they know or where they have reasonable grounds for suspecting that a person is engaged in money laundering or terrorist financing. Employees should report these activities to the nominated officer — a member of senior management responsible for dealing with anti-money laundering issues. If the nominated officer determines that a report provides grounds for knowledge or suspicion, he or she should report the matter to regulators. Additionally, lawmakers and regulators should review and strengthen penalties where they find this reporting is deficient.

- **Clearly mark all checks as a return of gaming funds or as a payout of a verified win to make clear whether funds actually are from gambling wins versus chip-to-cash conversion.**

- **Control the exchange of currencies.** Where there is minimal play, casino policy should result in a refusal to issue a check or even a ban on future play for the individual involved if money laundering is suspected.

- **Promote or require the use of cash alternatives such as debit cards and customer accounts through which bank drafts and electronic funds transfers may be used, especially for large money transactions. These alternatives are somewhat easier to implement with online gambling, where transaction limits are more common.**

- **Provide mandatory AML training for casino staff that is updated regularly.**

- **Establish a dedicated unit consisting of members who are Certified Anti-Money Laundering Specialists and have expertise in AML investigations, programs, and intelligence. This unit should work with police and regulatory agencies, and share information regarding individuals it believes may be engaged in criminal activity, including money laundering and terrorist financing-related offenses.**

Governments can help address money laundering by making it easier to prosecute cases. It also would help if authorities could seize assets believed to be directly connected to money laundering.

---

**Got News?**

Just email your news, important events, or information to Kristina at kristina.davis@infirmaryhealth.org and it will be added to the following month’s newsletter.