message from the board

Mid-Columbia Members,

We hope everyone enjoyed their summer break and was able to take some time off to vacation and spend time with family and friends. Anyone else ready for the cooler weather and back to normal routines?

We are ramping up for another eventful year and welcome any input you may have. Please familiarize yourself with the board member list below and let any of us know if you have topics you would like discussed over the year or suggestions. We are looking forward to another great year ahead.

This month’s luncheon will feature Eric Thomas, IT Security Engineer from Gesa Credit Union.

Have a great month and happy auditing!

Mid-Columbia Chapter Board Members

audit career center

Advance your internal audit career or strengthen your team with The IIA’s Audit Career Center resources.

upcoming webinars

Agile Auditing: Transforming the Internal Audit Process and Value Proposition Using the Scrum Process Framework

Members-only Webinar:
Tuesday, September 17, 2019
1:00 – 2:00 p.m. ET

“How many auditors does it take to change a light bulb?”
Answer: How many did it take last year?

mid-columbia chapter board

President
Stacie Anderson

President Elect
Sara Hudson

Secretary
Lucy Flores

Treasurer
Taylor Meirndorf

Programs
Jennifer Hegdal

Events
Susan Rodabaugh

Membership
Christina Pesicka

Certification Officer
Zack Corcoran

Elections
Kori Pyle

Academic Relations
Denton Romans

Website
Kelly Custer

Audit Committee
Lisa Copeland

Newsletter
Shelby Rose
Upcoming Luncheon

“Data is the New Bacon”
Thursday, September 19, 2019
11:30 a.m. – 1:00 p.m. (lunch provided)

Location: Richland Federal Building
825 Jadwin Ave
Conference Room No. 142

[Note: Please arrive a few minutes early with photo ID, as you will have to go through security/metal detectors. We apologize for any inconvenience.]

Speaker: Eric Thomas, IT Security Engineer
Gesa Credit Union

RSVP to Susan Rodabaugh by Thursday, September 12

CPE Fee: Free CPE for IIA Members! $15/ea. for Non-Members; first time attendance by a Non-Member is free. Members and Non-Members that RSVP and do not attend will be charged a $15.00 fee. The CPE fee will be collected at the door upon arrival.

About the Speaker
Eric Thomas, IT Security Engineer

Eric Thomas is an Information Security professional who graduated from WSU Tri-Cities in 2016 with a B.S. in Computer Science. Since then he has worked as an IT Security Engineer for Gesa Credit Union. He is passionate about technology, privacy, learning, the outdoors, and dogs.

Are you a New Member to IIA? First off, Welcome! The IIA has put together a webinar designed to educate you on the basics of the IIA as a whole. Click for access to the Webinar and PowerPoint.

WHAT’S IN THE NEWS?

Meet the IIA’s New Global Chairman – Mike Joyce
J. Michael “Mike” Joyce is 2019–20 Chairman of the Institute of Internal Auditors (IIA) Global Board of Directors. In this role, Joyce serves as an officer of the Global Board, is Chairman of the Supervisory Committee, and presides over the Global Assembly. Joyce is the Vice President, Chief Auditor & Compliance Officer for Blue Cross Blue Shield Association (BCBSA), a national federation of 36 independent, community-based and locally operated Blue Cross Blue Shield companies. The Blue System is the nation’s largest health insurer, covering more than 107 million members.

Joyce has more than 36 years of professional experience and has been actively volunteering with The IIA since 1989. Before becoming Chairman of The IIA Global Board, Joyce’s volunteer roles included serving as the Global Board’s Senior Vice Chairman (2018–19) and Chairman of the North American Board (2015–16). Joyce served on the Board of Governors for the Chicago...
Chapter of the IIA from 1995 until 2015, including a term as chapter president (2001–02). Joyce also was a founding Advisory Board member for DePaul University's IIA-endorsed Internal Audit Program.

**Mitigating Cybersecurity Risk: Close the Open Windows**

By: Jim Pelletier

Major leaks of consumer data have become a fact of life, as are the resulting fines in the mega millions and the damage to reputations that can take years to overcome. In a July 30 article, *The New York Times* reported there have been 3,494 successful cyberattacks already this year — a number that only includes financial institutions.

The latest, Capital One, involved a former Amazon software engineer who allegedly accessed the bank's computer network through what the bank described as a "configuration vulnerability" in its security software. The alleged thief compromised the personal information of more than 100 million people.

A new IIA Bulletin — Cloud Security, Insider Threats, and Third-party Risk — lists 10 questions chief audit executives should be ready to answer from their boards and audit committees. The Bulletin also provides a list of resources available to members, including three IIA Global Technology Audit Guides: Information Technology Outsourcing, Cybersecurity Risks, and Auditing Insider Threat Programs. The resource list also includes available training, two IIA practice guides, a book, and the link to The IIA's Cybersecurity Resource Exchange.

While vulnerabilities may continue, internal audit can help the organization resist intrusions and eliminate any thinking that the organization is defenseless against sophisticated criminals.

In the case of Capital One, reports indicate the breach of the bank's computer system was not particularly sophisticated. The alleged perpetrator accessed customer records the bank had stored on Amazon's cloud service, seemingly by exploiting a vulnerability in the firewall of a Capital One web application that connects to the Amazon Web Services cloud. Capital One representatives refused to answer questions about whether the alleged perpetrator "hacked into its systems or simply climbed through a window that had accidentally been left open."

Internal audit leaders should begin by knowing if their organization relies on cloud services in the first place and to what extent. If the cloud is used, what information is stored there, and how sensitive is it? What steps has the organization taken to ensure data in the cloud is secure? More simply, could the vulnerability have been mitigated by better patch management?

The opportunity for internal audit is to become fully versed in the critical aspects of cybersecurity — cloud, insider threats, and third-party risks, among others — not necessarily to become a technical expert, but to know enough to ask the right questions and follow up where needed. The talent shortage for resources with expertise in this space is not going away anytime soon, and failure to take action is not an option. Leverage the research and educational materials around you, step into this space, and help your organization close the windows.

That's my point of view; I'd be happy to hear yours.