CSX 2018 conferences featured over 120 SESSIONS AND WORKSHOPS focused on innovation, the technology workforce, disruptors, best practices, and professional development. WORLD-RENOWED KEYNOTES covered the current landscapes of cybersecurity and global cybercrime, with insights into future challenges. ISACA LEADERSHIP unveiled recent research on digital transformation and the culture of cybersecurity, and sponsors demonstrated their solutions to industry challenges.

The 2019 ISACA global conferences feature exciting changes and enhancements; see the last page of this report for CSX 2019 conference dates and locations, and view all ISACA conferences here.
Ten years ago, cyber threats were IP theft, botnets, surveillance and privacy. While these threats still exist, they are compounded by the addition of new trends and new incentives for cyber attacks. CSX 2018 North America keynote P.W. Singer said that we will decide the future of cybersecurity: by doing something or by doing nothing.

Singer believes that ransomware will only get worse, with more wide-ranging implications and victims. “So far the targets have been digital files, which made it difficult for the organization to run its business. What we see looming is holding THINGS hostage – like thermostats and medical devices.” The Internet of Things (IoT) is already known to be a hotbed of risk, with little to no regulation, security not built into devices, and customers unaware of the dangers. Singer said that 70 percent of IoT devices have known vulnerabilities.

James Lyne treated CSX Europe attendees to a live hacking demonstration while describing the commercialization of cybercrime. “You can purchase malware on the dark web to hire bots that take over hundreds of thousands of systems. You can buy access to a platform that builds your ransomware for you. You can even purchase malware that comes with quality assurance.”

Laura Galante brought her extensive knowledge of cyber threats and the political, military and financial implications of cyber operations. “We are on the front lines of thinking about the biggest threats to societies and economies, not just networks,” she said.

There is one key takeaway: given all of the change going on – whether new technologies or the culture of the system – nations, organizations and individuals that don’t look at change, don’t understand change, and change along with it, will lose the future,” said Singer.


“Stop calling end users the weakest link. Empower them to be the first responders; they make thousands of security decisions. The art of cybersecurity is 30-40 percent people and 60-70 percent science.”

- KEREN ELAZARI
TOP-RATED SESSIONS

Cybersecurity Nexus Cyber Hunt
Dustin Brewer, Manager, Cybersecurity Technical Content at ISACA and
Frank Downs, Director, Cyber Security Practice at ISACA [CSX North America]

DevSecOps: Bringing the Security—The Missing Link in Delivering on the Promise of Business Velocity and Quality to DevOps
Rob Clyde, CISM, NACD Board Leadership Fellow, Board Chair of ISACA, Executive Chair of White Cloud Security and Board Director of Titus [CSX North America]

Don’t Hack My Brain! The Coming Security & Privacy Risks Behind Brain Computer Interface Solutions
Pablo Ballarin, Co-founder of Balusian [CSX Europe]

Developing a GDPR-Ready Incident & Breach 72-Hour Action Plan
Alex Bermudez, CIPP/E, CIPM, Privacy Solutions Consultant at OneTrust [CSX North America]

Why Awareness Efforts Fail
Tracy Celaya, Principal Consultant at Go Consulting International, LLC and Ira Winkler, President at Secure Mentem [CSX Europe and CSX North America]

The Art of Red Teaming Without Insulting
Frans Szabo, Senior Security Specialist at Rabobank [CSX Europe]

Cyber Crisis Management Tabletop Simulation for Senior Management and Board of Directors
Guy Dagan, CAO at Consienta and Oren Elimelech, Founder & CISO at CyberTeam 360 [CSX Europe]

Taking Down the Cyber Criminal: Post-Breach Incident Analysis & Investigation
Jarrett Koltzoff, President/CEO at SpearTip, LLC [CSX North America]

The Five ‘P’ s of Breach Response
Ben Smith, CRISC, Field Chief Technology Officer at RSA [CSX Europe and CSX North America]
Featuring a range of opinions from industry experts, two panels focused on enterprise-wide culture of cybersecurity at CSX North America and CSX Europe. Unveiling new research from ISACA and CMMI Institute in which more than 4,800 global respondents identified their cybersecurity culture challenges, the panels offered advice on how leadership and staff can promote ongoing awareness and training.

All panelists agreed that “enterprise means everyone” – that cybersecurity is a responsibility of all leaders and of all staff. “This isn’t a technology problem,” Chris Moschovitis, CEO of tmg-emedia said at CSX Europe. “This is about leadership.”

Ira Winkler, president of Secure Mentem, shared provocative insights such as, “You create the culture for the people to live in. Tell them what to do. If you don’t enforce it, it doesn’t exist – you’re letting employees set the culture.” He also believes that cybersecurity compliance must be held to the same standard as financial controls and harassment policies. “You pay your employees to do their job, and that includes being secure. Build security into business processes and tell them the steps. If they don’t want to buy in, fire them.”

“If management is setting lofty goals and forgetting to get buy-in from the rest of the employees – well, there’s your problem,” said Heather Wilde, chief technology officer of ROCeteer.

How to accurately measure a culture of cybersecurity, and set appropriate Key Performance Indicators [KPIs]? “KPIs are numerous and overwhelming; choose a few and escalate them,” advised Don Gallien. Wilde agreed: “Do the simple KPIs, like number of password resets and number of logins from strange IP addresses, because they’re great leading indicators,” she said.

Tammy Moskites, senior security managing partner at Accenture, recommended that enterprises develop security liaisons in an ambassadors program to serve as resources and help change mindsets to reinforce that security is everyone’s job.

Candace Worley, vice president and chief technical strategist at McAfee, said that highlighting good cybersecurity behaviors can make a difference in creating a culture of cybersecurity. “Focus on the positive; recognize people who do the right thing,” she said. “If you can get people to feel like cybersecurity is ‘helping them’ and make cybersecurity itself engaging, you’ll see a lot more success. Focus on the psychological aspects of training so employees can recognize when they are being manipulated.”

“Cybersecurity is about human behavior, after all,” agreed Tim Callahan, senior vice president, global chief security officer at Aflac.

Read more: ISACA Now blog post by panelist Heather Wilde: “Three Keys to a Cybersecurity Culture That Will Stick”

ISACA/CMMI CULTURE OF CYBERSECURITY RESEARCH FOUND:

- VERY FEW ENTERPRISES HAVE THE CYBERSECURITY CULTURE THEY WANT. 95% say there is a gap between their desired culture and the one they have. Nearly a third say that gap is significant.
- ORGANIZATIONS NEED TO ENGAGE STAFF MORE EFFECTIVELY IF THEY WANT THEIR CULTURE TO IMPROVE. Only 34% say staff have a solid understanding of the role they play in the organization’s security culture.
- THERE ARE REAL BUSINESS BENEFITS TO A STRONGER SECURITY CULTURE. Nine in ten respondents say establishing a stronger cybersecurity culture would increase their organization’s profitability and viability.
- EXECUTIVE SUPPORT IS KEY TO SUCCESS. Among the organizations that perceive a significant gap in achieving their desired cybersecurity culture, one in three cite a lack of executive support as the major stumbling block.

ATTENDEE POLL:

**WHAT CAN MAKE — OR BREAK — AN ORGANIZATION’S CULTURE OF CYBERSECURITY?**

- "The people. Make them feel a part of the organization — invite their ideas and participation. Let them help raise awareness; hang posters that highlight who has had good ideas, who has done things the right way. Assign cybersecurity leads in each department to spread the word about good practices.”
  Dalim Basu
  CISA, CRISC, Chairman, BCS North London Branch and Events Director, ISACA London Chapter, England

- "A board of directors can sometimes only pay lip service to cybersecurity, and they need to go beyond that. Another challenge is when talking about cybersecurity, and asking for more training or tools, it is hard to explain, to convey, the return on that investment.”
  Michael Connor
  CISM, AVP of Enterprise Risk Management and Information Security Officer, Vantage West Credit Union, USA

- "The tone at the top, starting at the board-level, giving direction to management that cybersecurity is a priority. Another factor that is important is time spent — organizations should spend as much time on cybersecurity as they do on other aspects of the organizational culture.”
  Michael Leung
  CISA, CISM, CGEIT, CRISC, Managing Director, Canadian Cybersecurity Inc., Canada

- "Culture needs to be enforced. There can’t be a lack of buy-in from management, and they must invest in training.”
  Dikeledi Mzimba
  ICT Security Risk Analyst, State Security Agency, South Africa

- "You have to have a strategic cybersecurity plan and stick to the plan. Don’t put it on the shelf. Also, execute on security awareness training for employees. If we don’t, and employees are not trained, we will have an attack, and it will come from inside.”
  Robert Yamasaki
  Information Security Officer, Community West Bank, USA

- "We see our clients have different levels of security. Risk assessments paired with training and awareness programs are critical. Environments change very fast and we need to catch up; monitoring is very important, especially with GDPR.”
  Ilian Stoianov
  CISA, Risk Assurance Director, PricewaterhouseCoopers Audit OOD, Bulgaria
In an edutaining session on when and how to embed cybersecurity in software, CSX North America Conference speaker Anna Murray, president of tmg-e media, inc., described the development process as a familiar journey fraught with emotional baggage.

Murray said cybersecurity features and functions can—and should—be successfully integrated into software, with best results achieved through active communications and cooperation by the security team, the development team, business analysts, program managers and “the business” throughout the development lifecycle.

Using “A Different Chart for Software Development” [see accompanying PowerPoint graphic to the right], Murray said software development typically begins in a “euphoric” state, progressing from “dreamy-dream mode to the murky muck.”

Murray said that embedding cybersecurity “must happen in the muck” of the feature-set and requirements stages, and that “almost no one is comfortable with the mid-level – the muck.” Requirements are produced from a successful journey through the muck, but there is a time of “Pain and Loss of Hope” right after going live. After that comes Stability and Steady State; Murray says that requirements exist in a continuum of “understanding, re-understanding, and re-re-understanding.”

CSX EUROPE 2018

CYBER CRISIS TABLETOP SIMULATION

At one of CSX Europe’s top-rated sessions, “Cyber Crisis Management Tabletop Simulation for Senior Management and Board of Directors,” speakers Guy Dagan, CAO at Consienta, and Oren Elimelech, Founder & CISO at CyberTeam 360, led attendees through an exercise in which they needed to decide how to engage with cyber criminals who have attacked their organization, a global bank based in England with 50,000 employees in Europe and the United States. Each team of eight selected participants to act in the roles of CEO, CFO, CIO, COO, CISO, Legal, PR and DPO to determine the best course of action, including whether to pay the cryptocurrency ransom and/or alert law enforcement. External stakeholders, such as a bank regulator, insurance representatives, and a GDPR supervisory authority, also weighed in on the cyber breach.

SOME CONSIDERATIONS:

• Assume that internal communications are compromised as well; distribute new cellphones to management and be prepared to work offline without computers.

• What is your crisis plan, especially if your CEO is on a 12-hour flight?

• Do you have the appropriate leaders’ contact information, including personal email addresses, when they are out of the office?

• Even if you want to negotiate with the cybercriminals, it’s highly unlikely that you can meet a ransom demand in 72 hours; a large amount of bitcoin for sale is difficult to find.

CSX NORTH AMERICA 2018

EMBEDDING CYBERSECURITY INTO SOFTWARE DEVELOPMENT

In an edutaining session on when and how to embed cybersecurity in software, CSX North America Conference speaker Anna Murray, president of tmg-e media, inc., described the development process as a familiar journey fraught with emotional baggage.

Murray said cybersecurity features and functions can—and should—be successfully integrated into software, with best results achieved through active communications and cooperation by the security team, the development team, business analysts, program managers and “the business” throughout the development lifecycle.

Using “A Different Chart for Software Development” [see accompanying PowerPoint graphic to the right], Murray said software development typically begins in a “euphoric” state, progressing from “dreamy-dream mode to the murky muck.”

Murray said that embedding cybersecurity “must happen in the muck” of the feature-set and requirements stages, and that “almost no one is comfortable with the mid-level – the muck.” Requirements are produced from a successful journey through the muck, but there is a time of “Pain and Loss of Hope” right after going live. After that comes Stability and Steady State; Murray says that requirements exist in a continuum of “understanding, re-understanding, and re-re-understanding.”
TACKLING RISK AND COMPLIANCE IN A GLOBAL CONTEXT PANEL

Challenges — such as differences in cultures, regulations, risk tolerance and compliance behavior — are a constant as security leaders attempt to develop and deploy information security programs worldwide, according to an expert panel at CSX North America. Among the challenges, however, are clear paths for program success.

Cybersecurity leaders must balance proactive and reactive activity, considering applicable information security regulations and the many regulatory changes around the world, noted panelist Doug Grindstaff. “Security leaders must first keep the strategic focus on their cyber program, and not play ‘whack-a-mole’ with local regulations,” he said.

Aaron Pritz used another game analogy — American football — in calling on security leaders to “be a quarterback, to have some regulatory and compliance issues managed centrally, and some in a more decentralized and local” way for best results.

Brennan P. Baybeck listed several challenges for security professionals, including differing opinions on what’s right or wrong, what’s acceptable, what’s urgent or important, and what levels of security are necessary, good, or good enough. Baybeck emphasized the importance of international standards and frameworks to guide alignment, policy and behavior. “Use a framework: pick one and drive to it,” he said.

In addition to underlining the importance of standards and framework use in assessing risk, Pritz said security leaders should evaluate and convey risk in the context of the overall business and industry. “Focus on helping business leaders understand the [security] risk issues in the context of the business. You don’t have to boil the ocean,” he said. “I use this analogy all the time: we don’t all need to be meteorologists to know how to prepare for a hurricane. The same applies to security.”

MODERATOR:
Greg Witte
CISM, Senior Security Engineer at G2, Inc

PANELISTS:
Brennan P. Baybeck
CISA, CISM, CRISC, CISSP, Board Vice Chair, ISACA; Vice President of Global IT Risk Management, Oracle Corporation
Doug Grindstaff
Senior Vice President of Cybersecurity Solutions at CMMI Institute
Aaron Pritz
CISA, Advisor at Reveal Risk

NO SILVER BULLETS: CYBERSECURITY IN THE COGNITIVE ERA

Security Operations Center (SOC) staff members “are paid to solve problems, not read blogs, research and look to the future,” said Neil Warburton, Security Architect at IBM, during his CSX Europe presentation on securing new technologies. He warned that when it all goes wrong – and it will – you need a bootstrap process. “Wannacry has taught us to expect a total loss of IT,” he said. “What and who do you recover first? You must restore backups and recredential everyone: admins, users and customers.” He encouraged attendees to keep up with research on AI. “Attackers share intelligence; defenders need to as well.”
SO, YOU REALLY WANT TO BE A CISO?

Dabbling in the good, the bad, and even a horror story or two, Tim Callahan, Aflac senior vice president and CISO, and John Graham, EBSCO CISO, offered insights and encouragement in the panel discussion “The Journey to Become a CISO and Why They Don’t Run with Scissors,” moderated by Tammy Moskites, Accenture managing director and senior security executive, during CSX North America. Some of the questions and responses:

► What levers are important in becoming a CISO?

MOSKITES: Leverage people, mentors, coaches...people I aspire to be like.

Graham: Networking is extremely important, both inside and outside the company.

Callahan: You must see the opportunity and seize the opportunity.

► Have you had any political missteps in your career?

Moskites: A CISO needs political astuteness, in addition to all the technical, soft and leadership skills.

Graham: As a security person, when I enter a room, I have a wake behind me, and it is important to know how that wake is perceived.

Callahan: I want my team to go out and skin their knees. It’s my job to keep them from breaking their necks.

► Do you have any CISO horror stories?

Moskites: When people are asking you to do things that fundamentally go against your integrity, that are fundamentally wrong, it’s time to make a change.

Callahan: In interviews [for a new job] it’s important to get buy-in, and to clearly define roles and responsibilities, especially across the group that will become your peers.

Graham: Relationship-building is more important than achievements, from the start and ongoing. Relationships with peers must be good, so it doesn’t ever become combative.

CSX NORTH AMERICA 2018

CYBERSECURITY JOBS BY THE NUMBERS

From David Foote’s "Analyst View: Cybersecurity Jobs, Skills, Pay Review and Forecast"

780,000 US PROFESSIONALS EMPLOYED IN CYBERSECURITY

350,000 US CYBERSECURITY POSITIONS UNFILLED

1,000 TOP-LEVEL CYBERSECURITY EXPERTS CURRENTLY IN ROLES

10K-30K TOP-LEVEL CYBERSECURITY EXPERTS NEEDED

3.5X CYBERSECURITY POSITIONS GROWING AT 3.5X THE RATE OF THE IT JOB MARKET

12X CYBERSECURITY JOB MARKET GROWING 12X FASTER THAN TOTAL MARKET

3.5 MILLION CYBERSECURITY PROFESSIONALS NEEDED GLOBALLY BY 2021

1 MILLION NEEDED IN INDIA ALONE
Simone Petrella, chief cyberstrategy officer at CyberVista, shared her insights into seven things NOT to do as a CISO.

CISOs often run into numerous challenges—from a culture that doesn’t prioritize cybersecurity, to a budget that doesn’t match the organization’s size and goals—and those factors are among many that lead to an average tenure of only 2.5 years.

But sometimes the reason for a short tenure is the CISO himself or herself. Here are seven mistakes CISOs frequently make—and what they should do instead:

1. **Talk to the C-Suite in technical terms.**
   - **What to do instead:**
     - Know your audience.
     - Tailor your talking points.
     - Get to the bottom line.

2. **Only tell the good news stories.**
   - **What to do instead:**
     - Know that bad news doesn’t get better with age.
     - Be honest—sometimes you have to talk about the ugly baby.
     - Be upfront so the board isn’t shocked when something goes wrong.

3. **Assume third-party providers will effectively handle your security.**
   - **What to do instead:**
     - Recognize there is no magic bullet.
     - Conduct your due diligence.
     - Find the right people to ensure successful implementation.

4. **Think every aspect of security is equally important.**
   - **What to do instead:**
     - Realize that if everything is a priority, then nothing is a priority.
     - Understand your industry’s and organization’s goals.

5. **Expect technology to solve all your problems.**
   - **What to do instead:**
     - It’s a people problem—treat it like one.

6. **Position security as unrelated to business growth.**
   - **What to do instead:**
     - Approach security as an enabler of the business.
     - Think of security like the brakes on your car—your brakes are there to help you go faster.
     - Make friends and influence people.

7. **Come from a place of “no.”**
   - **What to do instead:**
     - Invest the time to understand where business peers are coming from.
     - Make sure others see security as a resource that is there to help.
     - Get involved as early as possible.
ISACA’s SheLeadsTech™ program seeks to increase the representation of women in technology leadership roles and the tech workforce. Attendees at CSX North America enjoyed a networking breakfast and panel where women in cybersecurity and tech discussed their career pathways, work/life balance, and how opportunities for women have changed since they embarked on their careers.

As he awarded attendees with goldfish crackers, Swedish fish candy, fish-shaped keychains and even a stuffed fish screen cleaner, Todd Fitzgerald, Managing Director/CISO of CISO Spotlight, LLC, shared that staff members at every level of the organization are vulnerable to falling for phishing emails, and said that “you can’t build a moat around your borders; you need an entire ecosystem of cyber risk.”

Fitzgerald shared research that showed the average mid-sized company lost $3.77 million per year in cyberattacks, mostly due to decreased employee productivity and uncontained credential compromise. However, after undergoing phishing awareness training, companies could save up to $188.40 per employee, as the phishing email click rate improved an average of 64% following training.

He described how to announce a phishing test to employees, and how to properly follow up with the staff who fell for a phishing email, as well as to thank those who correctly identified and reported a suspicious email. He recommends “burying the once-a-year, one-hour training sessions” for more holistic programs that engage staff in being aware that they will be tested, and to educate them on why it is critical that they are always aware of cyber risk as attacks become more sophisticated and easier to fall for.
CSX CONFERENCES 2018

SOCIAL MEDIA

Thoroughly enjoyed ISACA RCSXNA with not only my professional peers but the good folks! / Mark Thomas, CIO/ CREST. CSX. Chris Moshevski and Anna Murray. And I highly recommend Chris Moshevski’s book "Cybersecurity Program Development for Business". - Presenter: Robbi Rosena

The three technologies which will dominate the Digital Transformation in the next year are big data, AI, and public cloud. Cybersecurity professionals need to focus on ensuring how the security controls around these technologies can be defined and implemented. #CSXNA #ISACA

@RogerOfarrill may have given the best presentation at #CSXNA -- proactive threat hunting is doable for almost any security team. Start small, do achievable things, have a plan and a methodology...then grow from there.

#CSXEURO will strong cyber security culture will prevent another leak? No. Can it prevent majority of leaks? Yes.

ISACA international

Former hacker @kpoulson shows his first tool of choice, "possibly the most fearsome cyber weapon of all time." #CSXNA

Angela Darrow @angela_crawley

#CSXEURO first time attendees

Allan Boardman @allanboardman

Nice summary of soft skills required for Tech Professionals from David Foote @dfoote1313 in his session at #ISACA #Cybersecurity conference #CSXNA.

Manoj Agarwal @manojag

#CSXEURO will strong cyber security culture will prevent another leak? No. Can it prevent majority of leaks? Yes.

Tammy Mookites @TammyMookites

Passionate about what I do. Thanks for allowing me to share those passions!

#CSXEURO dowhatyoulove #loveyoulook #Accenture #ISACANews
BIG CHANGES IN 2019

ISACA is thrilled to invite you to join us for CSX education, networking and professional development at two newly-imagined events in North America and Europe in 2019.

Infosecurity ISACA North America Expo & Conference 2019
20-21 NOVEMBER 2019
New York, NY, USA
www.infosecuritynorthamerica.com/2019
ISACA, the leading global association for IT audit, risk, governance and security professionals, and Infosecurity Group, Europe’s leading information security event, are partnering to produce the most progressive information security event in North America.

EuroCACS/CSX
16-18 OCTOBER 2019
Geneva, Switzerland
https://conferences.isaca.org/euro-cacs-csx-2019
ISACA’s first EuroCACS/CSX Conference leverages the best of Europe’s CACS and CSX events to advance attendee knowledge, skills and careers in information systems, cybersecurity, and business.

“What is being CYBER RESILIENT in a phrase? The ability to keep business running.”
- TAMMY MOSKITES, ACCENTURE,
  “GAINING GROUND ON THE CYBER ATTACKER: BUILDING A CYBER RESILIENT BUSINESS" AT CSX EUROPE

THANK YOU TO OUR CSX 2018 CONFERENCE VOLUNTEERS

CSX North America Volunteers
CSX North America Volunteer Lead: Toan Do, MSc, CRISC, CGEIT

CSX Europe Volunteers
CSX North Europe Lead: Garen Melikyan, CISA, CISM, CRISC, CISSP

SPECIAL THANKS TO OUR EMCEES:

CSX North America Emcee: Mark Thomas, CRISC, CGEIT
CSX Europe Emcee: Richard Hollis, CISM, CPP, CRISC