50 YEARS OF ISACA: NORTH AMERICA CACS HONORS OUR PAST WHILE INNOVATING OUR FUTURE

ISACA's CACS conferences bring together audit, assurance, compliance, risk, privacy, security, governance and information technology professionals from across finance, technology services, insurance, government, military, healthcare and other sectors.

More than 1,700 attendees were welcomed to the North America CACS 2019 conference: ISACA members, volunteers, speakers, sponsors, exhibitors and staff gathered in Anaheim, California, USA, 13-15 May — a 50th anniversary celebration in southern California, where ISACA began in 1969.

With more than 100 sessions and topics—ranging from transformative technologies, to IT governance, to risk-based approaches to security—attendees engaged with experts, networked with colleagues, and gained valuable education.

Read on for quick takeaways from the event.

SPEAKER INSIGHTS

"Have a retainer with a reputable incident response organization. Not having one makes you run the risk of an attack or malware outbreak response only after you have negotiated contracts and performed your due diligence.”

Sushila Nair, senior director, security portfolio at NTT Data, from the "Cyber Incident Response Planning" session

"Let’s be at the forefront of these new frameworks, processes and technologies, making them standard in our daily operations and lives, so that we can provide more value to the enterprises which we serve.”

Brennan P. Baybeck, ISACA board chair, from the "Brick by Brick: Future-Proofing your Career” closing leadership brief

"In preparation for the Tokyo 2020 Olympic games, the government is running pen tests against 20 million IoT devices.”

Data shared at the "Security and the Internet of Everything” panel
From the days of determining how to secure and derive value from early computers to today’s challenges as organizations navigate digital transformation, it has been a remarkable 50 years for ISACA.

North America CACS was the perfect location to mark this milestone; ISACA was founded as the Electronic Data Processing Auditors Association in southern California in 1969.

North America CACS began with the 50th Anniversary Opening Platform, which followed the anniversary theme of “Honoring Our Past, Innovating Our Future” by welcoming ISACA founders and past leadership, discussing ISACA’s evolution, and looking to the future. Special anniversary-themed panels allowed for industry experts to discuss ISACA’s impact and the disruptive technologies that are changing the landscape. And attendees were able to celebrate in style during the “Surfin’ Through the Decades” social event, with 50th-anniversary-themed drinks, food trucks and activities.

**50TH ANNIVERSARY PANELS**

**A SPECTRUM OF PROFESSIONS: ‘THE WORLD NEEDS US’**
Moderator Marios Damianides, 2003-2005 ISACA board chair and partner at Ernst & Young, led a panel representing the breadth and depth of the ISACA professions to discuss the pioneers of the association and the evolutions that have led to our current innovative landscape.

A common theme throughout the discussion was that foundational skills and challenges will remain constant even as technologies change. “There’s always going to be change, whether it’s a new topic, a new tool, a regulation, whatever it may be,” said Paul Regopoulos, senior manager, information security audit, with The Walt Disney Company. “The fundamentals are always going to be: what are the risks associated with them, and how do we respond?”

READ THE ISACA NOW BLOG POST ABOUT “THE SPECTRUM OF PROFESSIONS” PANEL FOR KEY TAKEAWAYS.

**PANELISTS:**
- Dean Kingsley, Principal, Deloitte & Touche
- Kelly Lin, Assistant Vice President, IT Audit Lead, East West Bank
- Jenai Marinkovic, Chief Technology & Security Officer, Beyond
- Paul Regopoulos, Senior Manager, Information Security Audit, The Walt Disney Company
- Andrew Tinseth, Associate Senior Vice President, Audit Services, University of Southern California

**THE EVOLUTION AND POWER OF DISRUPTIVE TECHNOLOGY**
Led by moderator Thomas Phelps, VP of corporate strategy and CIO at Laserfiche, panelists reviewed the disruptive technologies that have changed how we live and work, and discussed the changing landscape of ever-accelerating disruption. The conversation led to not only the topic of the need to secure AI, but what to do if the data is laden in bias. The panel also discussed retail disruption, blockchain, quantum computing, and enterprises’ need to shift to being data-centric.

READ THE ISACA NOW BLOG POST ABOUT THE “FROM DISRUPTIVE TO DAILY DEPENDENCE: 50 YEARS AND FUTURE TECH” PANEL FOR KEY TAKEAWAYS.

**PANELISTS:**
- Kim Bollin, Vice President, Internal Audit, Workday, Inc.
- Jenai Marinkovic, Chief Technology & Security Officer, Beyond
- Ken Venner, Former CIO, SpaceX
- Jedidiah Yeuh, Founder and Chairman, Delphix
10 STEPS TO BETTER INNOVATION FROM GUY KAWASAKI

He rose to fame as Apple's chief evangelist and is now chief innovation officer of Canva. Guy Kawasaki offered 10 critical steps for better innovation in his opening keynote session:

1. Define your business.
Many businesses make the mistake of defining their business related to what they already do. Think about what your customers actually GET from you—not in terms of your specific product or service, but the BENEFIT.

2. Jump to the next curve.
How do we make the benefit to our customers even better, and adapt to serve them well? Consider ice harvesting: it evolved from saws and sleighs to ice factories that froze water centrally. Then came Ice 3.0: the refrigerator. But ice harvesters defined their business as harvesting ice, and ice factories defined their business as freezing and delivering ice, so both became irrelevant. The trick is to get to the next curve to stay relevant and innovative.

3. Don't worry, be crappy.
When you have jumped to the next curve, your elements of evolution can have "aspects of crappiness to them. Apple produced some pieces of crap, but they were revolutionary pieces of crap." The market is remarkably forgiving.

4. Polarize people.
Great products and services polarize people. Some people love you, and some people hate you—and that's okay. Take TiVo, as an example. People loved it, but large brands and their ad agencies hated it.

5. Ignore naysayers.
They are negative people, often resistant to change. A Western Union internal memo from 1876 states, "This telephone has too many shortcomings to be seriously considered as a means of communication." If you listen to the people who crush your dreams, you will never try and you will never know. And that is the worst outcome of all.

6. Change your mind.
People think, "If I change my mind, I'm going to look weak and stupid." Quite the contrary. In 2007, Steve Jobs said the iPhone was a closed system. In 2008, he completely reversed the direction and went to an open iPhone, and the rest is history. Without that, we wouldn't have these millions of apps. Changing your mind is a sign of intelligence and strength.

7. Get high and right.
Consider a graph with "Unique" on one axis and "Value" on the other. To succeed, you need to be in the upper-right quadrant.

8. "Let 100 flowers blossom."
Take your best shot in positioning and branding your project, and people you never anticipated might buy your product. A lot of companies freak out when this happens, but if it does, take the money.

9. Churn, baby, churn.
Ignore what rich and famous (and supposedly "smart") people say when creating your product. Once it ships, switch gears and start listening. 1.0 must quickly become 1.1, 1.2, 1.3, 2.0.

To be successful innovators, you must be able to pitch today. Pitch for capital, for approval, for permission, for partnership, for recruiting, for sale. It is an essential skill for everyone.
THE WISDOM AND POETIC INSPIRATION OF SEKOU ANDREWS

This schoolteacher turned national poetry slam champion has become the world’s leading “Poetic Voice” – a new type of speaker and artist who blends inspirational speaking with spoken word poetry. Some memorable takeaways from Andrews’ closing keynote session:

“You win some. You learn some.”

“There’s always a risk in innovation. Be okay with your discomfort.”

“Disrupt yourself. Interrupt yourself.”

“The greatest resource each of you has is Each of You.”

“How many of you have ever had a ‘Why Didn’t I Think of That?’ moment?”

“It’s time to DIY your innovation like it’s HGTV. IKEA your innovation. Lay out all the screws and shelves, and sit surrounded by it until you figure out how to do it yourself. Otherwise, someone will figure out how to do it for you.”

“Disruption is kind of a jerk. It is rude and relentless. It doesn’t raise its hand. It doesn’t say, ‘Excuse me.’ Disruption does not RSVP. You may not even know it has come with you until it is done with you.”

“You are both the source of your solutions and the source of your problems. This is our duality.”

“Just as important as knowing where you CAN’T fail is identifying where you CAN fail. Embrace failure in your mindset....I’m not going to stick my head in the sand and hope for the best. Failure, let me dance with you.”

“Transform yourself from a what to a why—from a service to an experience.”

“Homogeneous teams lead to homogeneous cultures that lead to homogeneous decisions. Train yourself to become a leader who seeks out diverse perspectives.”

“ROI: Return on Innovation.”

“Can’t blaze the trail if you’re afraid to fail.”
SECURITY AND THE INTERNET OF EVERYTHING PANEL: KEY TAKEAWAYS

Moderator Sushila Nair, senior director, security portfolio at NTT Data, led a discussion on the Internet of Things (IoT), noting that IoT includes any physical object with an Internet connection. This includes anything connected to a phone, such as door systems, thermostats and other devices. With an increasing number of devices, companies and consumers must start building an approach to securing them. This includes:

1. Creating Policy: Enact a policy that purchased IoT devices meet security requirements; include supply chain requirements.

2. Policy and Vulnerabilities Check: Ensure IoT devices meet all current security policy requirements; check for and change default passwords. Understand device vulnerabilities and how they can be patched.

3. Classification: Classify IoT devices; put the appropriate security measures around these devices, such as network segmentation. Check out the draft publication NISTIR 8228, “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks” and the discussion draft on IoT baselines.

4. Device Inventory: Organizations do not know what IoT devices they have. Many of these devices are very expensive, so maximizing their use and preventing them from being stolen or hacked is critical. You can’t secure something you don’t know that you have. Leverage experts who can use tools to perform assessments to create and maintain a device inventory.

ATTENDEE POLL:

What are the biggest tech or business challenges keeping you up at night?

“No, it’s not because they lack knowledge. It’s the complexity of compliance issues, the way that regulations are changing regularly, and the variety of regulations that we have to follow. It’s not just the United States, it’s all the different countries. It’s the number of different countries and the number of different regulations that we have to follow.”

Jim DeDad, CISA, CTPRP
Lead IT Risk Management & Compliance Analyst
Erie Insurance IT Strategic Integrated Services
Erie, PA, USA

“There is a lot and increasing involvement of top management, and too many issues to communicate back to the top levels of management. We need to focus and reduce the scope of information, taking a look at security and technology risk, and IT management needs to talk the language of business more.”

Jesus Ariel Moreno Camacho, PCSI
IT Compliance COPPEL
Culiacan, Sinaloa, Mexico

“Basically, it’s the people who have access to our data and our systems, whether they’re internal or external, and whether the controls are solid in terms of keeping the people that are supposed to be kept out, out, and for those that are allowed in, limiting it to what they’re supposed to be able to access to get whatever they need while they are connected.”

Addie Lui, CISA, CISM
VP & Corporate Security Officer
Hawaii National Bank
Honolulu, HI, USA
THE NEW PRIVACY: GDPR, CALIFORNIA CONSUMER PRIVACY ACT, AND THE FUTURE OF DATA REGULATION PANEL

A panel moderated by Rob Clyde, 2018-2019 ISACA board chair, explored the ways in which GDPR and other recent privacy-related measures are changing the enterprise landscape. The consensus: virtually all organizations still have progress to make on the data privacy front, but at least now they understand the importance of doing so, not only to meet compliance requirements, but to establish stronger relationships with customers.

The panel agreed that methods such as data encryption and maintaining a minimum amount of needed data can be useful, but there is no single magic bullet – a holistic, enterprise-wide strategy is needed.

Clyde recommended “stopping the bleeding” by figuring out how new data will be processed and stored, and then circling back to deal with existing data.

Panelist Bill Bonney, information security professional & virtual CISO at Cyber Advisory Group, said he expects the changing attitudes of the public will have a major impact on future data privacy policy in the US. “I think the court of public opinion is going to overrule even the Supreme Court,” he said.

5 THINGS YOU NEED TO DO NOW FOR BETTER IT RECRUITING AND RETENTION

Sandy Silk, director of information security education and consulting at Harvard University, shared five steps for building a new rubric for IT hiring:

1. Remove unconscious gender bias from job descriptions. Tools exist to help you do this, including this one.

2. Resist assumptions about technical degrees and certifications. Technology can be taught; soft skills and other key attributes can come from a variety of backgrounds.

3. Focus on core skills, knowledge and aptitudes crucial to success. Leave out what isn’t needed to avoid missing out on candidates you may wish to attract. Research shows men are more likely than women to apply if they don’t meet all the job requirements.

4. Build an interview plan that provides a positive experience for everyone. Interview questions should refer back directly to the necessary qualifications in the job description.

5. Develop and leverage a recruiting network that reaches a broader pool of potential applicants than what your HR team can provide. Reach out to these connections when you’re about to post a job and ask them to help you share it widely with their networks.

Listen to the “Off Stage and Off Script” ISACA podcast interview with Sandy Silk, recorded onsite at North America CACS.
“BRICK BY BRICK: FUTURE-PROOFING YOUR CAREER” LEADERSHIP BRIEF

Although the closing session audience initially may have wondered about the title, “Brick by Brick,” and the brick technology metaphor explored in Brennan P. Baybeck’s leadership brief, the 2019-2020 ISACA board chair used the analogy well in calling audit and security professionals to action—for themselves and their organizations.

After tracing both the evolution of brickmaking and bricklaying to today’s Semi-Automated Mason, a robotic bricklayer that increases productivity yet is managed by humans, Baybeck turned more broadly to the implications of industry shifts for IT professionals. “Industry 4.0 isn’t just about improving speed and ability, it’s about exponential change: turning everything upside down and inside out,” he said. Likewise, professional careers “start from the ground up…We add, brick by brick, skills, experience, knowledge,” Baybeck conveyed. Yet, because of the pace of technology and business, and specifically because Industry 4.0 “is about change and transformation,” he said “those of us in this room [and the ISACA professional community at large] must do the same to remain relevant” and valuable to their organizations.

“Brick by brick, we need to work with the tech that is driving change, and we need to learn and train in areas in which we may not have realized we would need to gain expertise when we entered the field,” he said.

Citing just one example, Baybeck said that “traditionally, audit professionals are on the tail end of technology adoption, spending more time auditing it than using it.”

“But I challenge every one of us to change that model…let’s be at the forefront of these new frameworks, processes and technologies, making them standard in our daily operations and lives, so that we can provide more value to the enterprises which we serve,” he said. “We should be the leaders helping our boards and executive management understand the importance of concepts such as IT and data governance and information protection.”
DON’T PANIC! RESPONDING TO A SECURITY INCIDENT

A common first step after a security incident is to panic—but with proper training and preparation on the front end, you can skip that step and go straight to the investigation, according to Alex Holden, CISO of Hold Security LLC.

It is essential to ensure your teams are being properly trained—do they know what they need to do when? Are scenario plans in place? Has it been defined when law enforcement should be notified and who should make that call?

Additionally, organizations must not overlook the importance of policies. Many make the mistake in thinking that they are not needed because there is an incident response plan in place—but not everyone gets a copy of the incident response plan. HR policies outlining rules such as “No employees are authorized to speak to media about the company without permission from the communications team” can help ensure that no unauthorized staff members talk to a reporter after an incident is discovered.

It is also important to put in writing exactly how you’ll respond to certain scenarios. Do you have written guidelines on what questions you should ask when you receive notification of a breach? What information do you obtain to help verify that the notification is legitimate? Once you’re notified, who do you call and when? Make sure you have a plan for how and when to notify IT, legal, the C-suite, HR, partners, law enforcement, insurance and others.

Many organizations resolve an incident but neglect to identify the root cause. As a result, they find themselves in the same place, facing a similar incident that could have been avoided. As an example, one organization was attacked by ransomware three times in a single month.

ATTENDEE POLL:

What are the most important skills for young professionals to acquire for career success?

“Young professionals need soft skills, communications skills; everything we do is communications, and in our jobs, people must trust us and the information we communicate. Young professionals need communications and emotional intelligence skills to build and maintain credibility. The ability to understand business needs and communications skills will set you apart.”

Mary Breslin, CIA, CFE
President
Verracy
Austin, TX, USA

“All young professionals need to understand audit, privacy, security and risk foundational skills because they are important; not just in their careers and their professions, but in their personal lives. We use all kinds of technology every day—cellphones, wearables, everything for convenience. Young professionals need to think about their personal data, where it goes, how it’s used, not just by other individuals but by companies. There are potential issues and there can be great risk.”

Yesenia Delgado Naranjo, CISA, CGEIT, CRISC, MBA
Administrator
Servicio de Administracion Tributaria
Mexico City, Mexico
THE DARK WEB: SIMULATE A DIGITAL ATTACK AND REHEARSE YOUR INCIDENT RESPONSE

In order to be prepared for breaches using information gleaned from the Dark Web, said Cindy Boyle, partner at BKD, and Rex Johnson, director at BKD, in their presentation “The Dark Web: The Myths, Reality & The Risks,” it is essential to educate your team—and that includes the board, executives and vendors.

Boyle and Johnson educated attendees on what the Dark Web is and how cybercriminals share and sell information. Less than 10 percent of the Internet is accessible through typical search engines; the other 90 percent is known as the Deep Web—and the Dark Web is a part of the Deep Web that is intentionally hidden and requires an anonymizer to access (e.g., Tor). On the Dark Web, you can find credit cards for sale for US$1, or full identification records (Social Security numbers, date of birth, account numbers, etc.) for US$30. Encourage reporting, even if you’re getting many false positives.

Steps for combating the criminal activity stemming from the Dark Web are to document and distribute security policies, and be sure to develop and rehearse a robust incident response program.

REHEARSAL OF A DIGITAL ATTACK SIMULATION CONSISTS OF SIX STEPS:
1. Leadership engages Red Team
2. Red Team hackers break in (infiltrate)
3. Red Team propagates and aggregates
4. Once detected, Red Team shows exfiltration data
5. Red Team provides feedback to security team
6. A report is published

Preparation is key. While some data shows that the number of breaches per year is declining, the impact is soaring. In 2018, the number of exposed records was more than 2.5 times the number in 2017, even though the number of attacks was smaller.

PROTECTING YOUR DATA AGAINST INSIDER THREATS

Insider threats remain a major challenge for enterprises, as emphasized in a session by Thomas Baumann, IT performance architect at Swiss Mobiliar.

To deal with the threats, Baumann recommends defining a rule set to trigger alerts. The rule set can incorporate machine learning techniques and potentially use existing solutions, such as Security Incident and Event Management (SIEM) and Database Activity Monitoring (DAM). Baumann said organizations also should classify their data by importance and utilize encryption for particularly sensitive data.

Listen to the “Off Stage and Off Script” ISACA podcast interview with Thomas Baumann, recorded onsite at North America CACS.
IT AUDIT LEADERS’ SUMMIT

Dozens of IT audit leaders from Fortune 500 companies attended the one-day summit dedicated to current challenges, solutions, and transformative innovations. Presenters focused on auditing in a changing world – companies are changing dramatically, and there’s nothing more dynamic than the IT organization.

TAKEAWAYS: IT AUDIT BEST PRACTICES RESEARCH

• Attendees accessed the executive summary of “A Global Look at IT Audit Best Practices,” released at North America CACS. This IT audit benchmarking study conducted by ISACA and Protiviti notes the growing role and responsibilities of IT audit in digital transformation, partnerships between the IT organization and IT audit function, and differences in how IT audit leaders operate compared to other IT audit professionals.

• The summit included an in-depth discussion of robotic process automation (RPA), including the importance of being deliberate about RPA implementations and that having an RPA strategy is essential to success.

• Audit leaders also discussed the challenge in finding the skill set of data scientists. Many teams find success in bringing professionals from other business areas into audit.

TAKEAWAYS: AUDIT INNOVATION

• Blockchain: It’s not just a buzzword; there are many more use cases for transacting beyond cryptocurrency, such as medical records, retail, processing and manufacturing. Understanding how audit will interact with blockchain is crucial.

• Cyber incident response: Work with the business to be seen as a valued partner in incident response, keep communication channels open and be prepared for “worst case” by running a variety of simulations that involves all necessary parties.

• DevSecOps: There is a culture clash of inserting security into development, and it can be difficult to find enough qualified professionals to build security into the mentality early in development.

TAKEAWAYS: IT AUDIT ROLE IN CYBERATTACK INVESTIGATIONS

• Understand the impact of an attack: Where did attackers go in the environment, but also where could they have gone, and what could they have done given the systems to which they had access?

TAKEAWAYS: AGILE SOFTWARE DEVELOPMENT

• DevOps is about tearing down silos between organizations – it’s a process that never ends, and as such it requires a cultural shift. We have to have the conversations about audit’s role and where we need to be involved, as well as how different areas can advocate for one another in a constantly moving environment.
SECURITY LEADERS’ SUMMIT

CISOs and other senior security leaders covered a panorama of business and technology issues, including data governance and privacy, emerging tech and cyber threats, cybercrime and law enforcement, and leadership culture and characteristics during the inaugural ISACA Security Leaders’ Summit at North America CACS.

Attendees were briefed on a few highlights from ISACA’s 2019 State of Cybersecurity research, then quickly considered observations from veteran ISACA contributor Todd Fitzgerald, managing director, CISO Spotlight. Fitzgerald said that while “CISOs still generally are reporting up through CIOs” in their organizations, he recommends the function be moved out from under the CIO given the strategic priority and importance of security, especially in corporate boardrooms.

Fitzgerald also noted that laws, regulations, policies and procedures represent the “shared values” and “tone” of security leaders throughout their organizations, and “every CISO needs to understand the language of privacy,” which can differ globally.

HE ALSO RECOMMENDED THAT SECURITY LEADERS:

- “Pay attention to differences across generations and personalities” to get the best out of management and teams
- Emphasize the importance of soft skills, for themselves and their teams
- Promote the importance of gaining professional certifications “to get people to understand and get things at a deeper level”

In a panel on data governance and privacy, Billy Spears, senior vice president and CISO, loanDepot, emphasized the importance of a “best friend” relationship with legal teams in organizations, taking proactive steps to ensure compliance in light of GDPR, CCPA and Canada’s Privacy Law, and to tackle reviews, gap analyses and updates to organizational privacy policies now rather than later.

And, in turning from regulation to technology, a panel gave practical advice to attendees challenged every day by “the 90 percent of vendors at my door who claim to have AI,” as one attendee put it.

Andy De La Cruz, network security at Aruba Networks, said vendors should be able to show their machine learning model, derive valuable analytics from their AI solution, and convey data collection methods.

Rich Lindberg, virtual CISO with Nth Generation, said he would ask vendors if they have data scientists behind their AI solutions, to explain the “core” of their AI engine in two minutes or less, and probe why their offering is meaningful to his business.

Jenai Marinkovic, chief technology and security officer, Beyond, echoed both De La Cruz and Lindberg, adding she challenges suppliers to convey fit. “To me it’s about security, enterprise architecture—does my organization and architecture have a gap, and does what they offer fill it, and does it help my team work better,” she said.
SOCIAL MEDIA ROUNDUP

Allen Steinberg @aksteinberg  ·  May 10
What a privilege to be at ISACA’s 30th Anniversary celebrations at PACACS, a short distance from where it all started in 1990, and to hang out with Chapter leaders and members from the inaugural chapter, @ISACA/CA. Thank you for the memories. ISACA& @ThomasPDtay @ISACA

Laurie Nelson-Rose @lncrmketers  ·  May 14
ISACA Security Leader’s Summit’s Todd Hodgdon talks 5 Stages of COSO @ PACACS

Mish Derryshire  @Oridex  ·  May 10
Brilliant eye-opening few days at PACACS. My first time attending, but there will be many more ahead! @ISACAToday @ISACASummit

Lew Wilf @lew2u  ·  May 15
Surf’ Thru Five Decades at PACACS @Pacancements @ISACA

Chet Saccio 2nd  ·  May 15
Hybrid Lean-Agile Leader and Coach
This morning at PACACS a panel of experts did a deep dive into the 30 years of tech and the future. Interesting takeaways include: - Conflicting predictions don’t come true, often the next big thing is unknown until it’s here, and technology is making innovation and disruption easier.

What does the future hold? Who really knows? What we think is the advancement in broadband paired with AI and quantum computing are going to create opportunities to create new tech beyond our wildest dreams.

Sushila Haer @sushila_uak  ·  May 15
We loved talking about @ConferencesatPACACS, great audience and discussion.

SEE YOU SOON!

North America CACS 2020—12-14 May, Baltimore, Maryland, USA

Visit www.isaca.org/conferences to view all of ISACA’s global CACS, GRC, and Infosecurity ISACA Expo and Conference events.
THANK YOU TO THE NORTH AMERICA CACS SPONSORS

<table>
<thead>
<tr>
<th>DIAMOND SPONSOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlackBerry</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PLATINUM SPONSORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe</td>
</tr>
<tr>
<td>Galvanize</td>
</tr>
<tr>
<td>SecurityScorecard</td>
</tr>
<tr>
<td>VANTAGE</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GOLD SPONSORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>KPMG</td>
</tr>
<tr>
<td>OneTrust</td>
</tr>
<tr>
<td>protiviti</td>
</tr>
<tr>
<td>Qualys</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SILVER SPONSORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
</tr>
<tr>
<td>servicenow</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BRONZE SPONSORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patchworx</td>
</tr>
<tr>
<td>DARKTRACE</td>
</tr>
<tr>
<td>FASTPATH</td>
</tr>
<tr>
<td>LOGICGATE</td>
</tr>
<tr>
<td>netwrix</td>
</tr>
<tr>
<td>TEVORA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SUPPORTING SPONSORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTION SOFTWARE</td>
</tr>
<tr>
<td>ISACA</td>
</tr>
<tr>
<td>Lockpath</td>
</tr>
<tr>
<td>LogicManager</td>
</tr>
<tr>
<td>MIS Training Institute</td>
</tr>
<tr>
<td>Onspring</td>
</tr>
<tr>
<td>ProcessUnity</td>
</tr>
<tr>
<td>Quantivate</td>
</tr>
<tr>
<td>SafePaaS</td>
</tr>
<tr>
<td>The Walt Disney Company</td>
</tr>
<tr>
<td>UCF</td>
</tr>
<tr>
<td>VENAFI</td>
</tr>
</tbody>
</table>