Highlights of the EC-Council CISO Executive Summit 2011

Top Information Security Professionals Congregate, Connect, and Interact at the Inaugural EC-Council CISO Summit in Las Vegas, NV

The EC-Council CISO Executive Summit 2011 took place from December 5-6th at the M Resort in Las Vegas, NV. Over 40 speakers from the private, public, and government sectors gathered to partake in 13 interactive panel-based discussions. This format allowed for networking, knowledge sharing, and continuous learning. Participants and attendees were able to engage in intimate discussions regarding the topics most relevant to high-level executives including managing insider threats, cloud compliancy, and structuring and managing an infosec workforce. Lasting relationship and business connections were made during the CISO Summit and at networking events. Continue reading for key takeaways, action items, and highlights from the summit.

Jay Bavisi, Co-Founder and President of EC-Council, began the conference with a welcome and opening address.

Day 1 of the CISO Executive Summit consisted of 6 panel discussions. Each panel discussion focused on one topic pertaining to quandaries faced by top-level IS executives, such as implementing high performing IS programs, best practices, cloud compliancy, outsourcing, challenges of managing IS across international borders, and managing insider threats. They were lead by a chair and 4-5 panel speakers. Below are the panel chairs and co-chairs from Day 1 of the CISO Executive Summit.

Angelique Grado

Chair of Panel 1: Best Practices of IS Operation & Maintenance

Jared Pfost

Chair of Panel 2: Implementing a High-Performing IS Program (A)

Inno Eroraha

Chair of Panel 3: The Challenges of Managing IS in a Global Arena

Ben Eu

Co- Chair of Panel 4: Embracing the Cloud & Mitigating Surrounding Threats

Raymond Soriano

Co- Chair of Panel 4: Embracing the Cloud & Mitigating Surrounding Threats

Jeff Tutton

Chair of Panel 5: Outsourcing & IS Management

Ira Winkler

Chair of Panel 6: Managing Insider Threats (A)

Jeffrey Vinson

Kevin McPeak

Jerry Chappee

Mary Siero

Illyas Kolliyankal

"Best Practices of Information Security Operations Maintenance": (From left to right) *Angelique Grado*, Director, Dexa Systems, *Jeffrey Vinson*, Director & CISO, SecureNet Payment Systems, *Kevin McPeak*, Senior Security Systems Engineer, CACI International, Inc, *Jerry Chappee*, Chief Information Assurance & Operations Officer, U.S. Army Reserves/ Disaster Recovery Manager, Blue Cross Blue Shield, *Illyas Kolliyankal*, CISO, Abu Dhabi Securities Exchange, *Mary Siero*, President & CEO, Innovative IT, LLC

"Best Practices of Information Security Operations & Maintenance" Panel Objectives:

The panel focus was on information security (IS) operations and maintenance. It provided enlightened examples, tips, and useable techniques for operations and maintenance of the security landscape. IS in this panel started with a firm understanding that it's Information at its most fundamental that has to be protected.

Operations and Maintenance of IS is broad enough to be subject to the Security Strategies and Governance in practice to develop a security strategy that leverages the multiple facets of information to best secure it. Every course on security starts with the elements of confidentiality, integrity, and availability of information to exemplify its security. Every threat and vulnerability evaluation considers the ability to trash, tramper, or take critical information. The best IS operations and maintenance professionals meld an approach that includes the security strategy, elements, possible results of a threat exploiting a vulnerability and the information environment to determine the best practices for their operations and maintenance.

"Implementing a High-Performing Information Security Program": (From left to right) *Jared Pfost*, CEO, Third Defense Inc, *Todd Bell*, Executive IT Security Advisor, ConnectTech LLC, *Mike Dahn*, Director, PricewaterhouseCoopers/ Founder, Security B-Side, *Raymond Soriano*, Director, Deloitte & Touche, *Vincent Grimard*, Director, Nelnet, *Michael Rushinsky*, Director, Sallie Mae

Todd Bell

Mike Dahn

Raymond Soriano

Vincent Grimard

Michael Rushinsky

"The Challenges of Managing Information Security in a Global Arena" Panel Objectives:

This panel session discussed specific challenges in managing information security in the global digital arena and solutions to these challenges.

Corporations today are doing business globally, forcing them to disseminate information to customer service representatives, outsourcing partners, development teams, sales, and so forth. Connectivity, communication and collaboration tools to access this information are more ubiquitous than ever before. Emerging technologies like outsourcing and cloud computing are relied upon because they offer cost-effective alternatives to information access but pose hindrances to security/privacy. Lack of knowledge and/or expertise in monitoring data breaches poses grave risks to information. Moreover, the sophistication on cyber attacks against confidential information continues to remain on the rise.

"The Challenges of Managing Information Security in a Global Arena": (From left to right) *Inno Eroraha*, Founder & CEO, NetSecurity Corporation, *Dave Anders*, Director, Orange Parachute, *Illyas Kooliyankal*, CISO, Abu Dhabi Securities Exchange, *Andrew Sispoidis*, Executive Director, The Center for Global Information Security, *Robert Hotaling*, Chief Security Officer, Cengage Learning

Dave Anders

Andrew Sispoidis

Robert Hotaling

Illyas Kolliyankal

"Embracing the Cloud & Mitigating Surrounding Threats": (From left to right) *Ben Eu*, CISO, IBM, *Raymond Soriano*, Director, Deloitte & Touche, *Michael Berman*, Chief Technology Officer, Catbird Networks, *John Lamboy*, Director of IT Security, eGlobalTech/ AVP, MedeAnalytics Inc, *Eric Svetcov*, Evangelist, TrustInMotion & SV Technology Ltd, *My-Ngoc Nguyen*, Vice President, Link Technologies

"Embracing the Cloud & Mitigating Surrounding Threats" Panel Objective:

The objective of the panel was to discuss experiences in threat mitigation efforts in Cloud implementations. The co-chairs presented questions to guide discussion amongst the panelist to provide insights and experiences on Cloud computing, its characteristics, service models and deployment models. The discussion investigated areas of risk analysis of data, regulatory requirements, security requirements, cloud model selection and cloud service providers selection. The panelists openly shared their personal and practical perspectives regarding cloud deployments and their threat mitigations experiences as part of their respective industries.

(From left to right) Jeffrey Vlnson, Kevin McPeak

(From left to right) Jerry Chappee, Illyas Kooliyankal

Top 3 Takeaways from "Embracing the Cloud and Mitigating Surrounding Threats":

By: Raymond Soriano (Director, Deloitte & Touche) & Ben Eu (CISO, IBM)

1. Regulation has an influence on the type of cloud deployments and solutions that organizations must consider.

2. Subscribers of cloud services need to perform sufficient level of due diligence and development of Service Level Agreements with potential cloud providers.

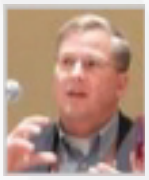
3. Cloud computing contracts should have appropriate provisions for accountability and auditability within service contracts.

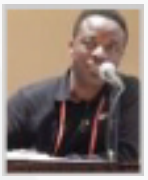

Michael Berman


John Lamboy

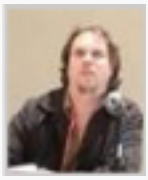

Eric Svetcov


My-Ngoc Nguyen


Todd Bell


Inno Eroraha


Chris Oglesby


Edward Ray

Top 3 Action Items for CISOs to Explore/ Implement from "Embracing the Cloud and Mitigating Surrounding Threats":

By: Raymond Soriano (Director, Deloitte & Touche) & Ben Eu (CISO, IBM)

1. Perform due diligence and consider satisfactory levels of Right to Audit and other measures within contracts.

2. Consult with business to understand requirements and risk tolerance for cloud solutions.

3. Engage with Internal Audit to help support and drive additional control with cloud solutions applied for the organization.

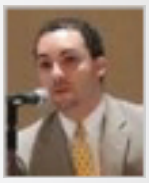
"Outsourcing and Information Security Management":
(From left to right) *Jeff Tutton*, President, Intersec Worldwide/ AVP, MedeAnalytics, *Todd Bell*, Executive IT Security Advisor, ConnectTech, LCC, *Inno Eroraha*, Founder & CEO, NetSecurity Corporation, *Chris Oglesby,* Senior VP, Knowledge Consulting Group, *Edward Ray*, CISO, MMICMAN, LLC,

"Outsourcing and Information Security Management" Panel Objectives:

This panel discussion focused on the challenges and benefits of outsourcing with respect to Information Security. It reviewed the definitions and the concepts behind understanding the full impact of security involved with outsourcing. The panel discussed the challenges of managing risk and monitoring the outsourcing company's performance when it comes to IT Security as well as the requirements to be considered before outsourcing. It explored industry cases, both success stories and failures that were lessons learned. The panel closed by giving an overview of recent industry changes that may impact outsource management, including SAS70 and PCI changes.

"Managing Insider Threats": (From left to right): *Ira Winkler*, Chief Security Strategist, Codenomicon/ President, Internet Security Advisors Group, *Eric McKim*, Senior VP, Cybersecurity/ CISO, Business Integra, *Steven Fox*, Security Architecture & Engineer Advisor, U.S. Department of Treasury, *Rick Moy*, President & CEO, NSS Labs, Inc, *Anthony Meholic*, CISO, Republic Bank, *Joe McCray*, Founder & CEO, Strategic Security LLC

"Managing Insider Threats" Panel Objectives:

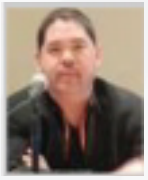


Eric McKim

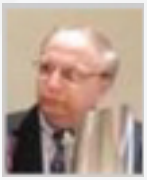
The panel addressed the most common underlying vulnerabilities that enable the losses incurred due to insider actions (both malignant and malicious). The discussion explored lessons learned and best practices when attempting to mitigate losses.

Despite the hype of malicious hackers, APT, etc., the insider threat is the most costly to organizations. Insiders can cause losses to the organization through malicious or malignant actions. The damages from malignant actions far outweigh those from malicious activities.

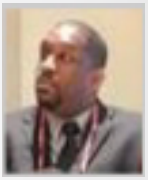
Steven Fox



Rick Moy



Anthony Meholic



Joe McCray

The panel-only discussion format enabled participants and attendees to steer the conversation to the most pressing and important issues. Those present at the summit were able to ask questions and gather feedback from the panel chairs and speakers. The atmosphere encouraged the opportunity for networking, knowledge sharing, and continuous learning.

Day 1 concluded with a networking event in The Wine Cellar of the M Resort. Speakers and attendees were given the opportunity to connect and forge new business relationships.

The panel discussions on Day 2 were centered on information security strategies and methodologies. The topics featured a variety of issues related to the technical and organizational roles of a top executive in information security. Management concerns were discussed in depth, such as structuring and managing an infosec workplace, monitoring and evaluating IT security policies, and managing insider threats. Technical and industry concerns, such as achieving PCI DSS compliance in the cloud and the factors that have the greatest impact on the IS profession, were explored and debated. The day ended with a discussion on preparing for future challenges.

Panel chairs and co-chairs are shown below:

Kevin McPeak

Chair of Panel 7: Implementing a High-Performing IS Program (B)

Jeffrey Vinson

Co-Chair of Panel 8: Structuring and Managing Your Infosec Workforce

Jerry Chappee

Co-Chair of Panel 8: Structuring and Managing Your Infosec Workforce

Mike Dahn

Co-Chair of Panel 9: Achieving PCI DSS Compliance in the Cloud

Michael Berman

Co-Chair of Panel 9: Achieving PCI DSS Compliance in the Cloud

David Simpson

Co-Chair of Panel 10: Monitoring and Evaluating Your IT Security Policies

Mary Siero

Co-Chair of Panel 10: Monitoring and Evaluating Your IT Security Policies

Jared Pfost

Chair of Panel 11: Factors with Greatest Impact on the IS Profession

Illyas Kooliyankal

Co-Chair of Panel 12: Managing Insider Threats (B)

Karthik Swarnam

Co-Chair of Panel 12: Managing Insider Threats (B)

Michael Rushinsky

Chair of Panel 13: Preparing for Future Challenges

Audience participation and engagement on Day 2

"Implementing a High-Performing Information Security Program" Panel Objectives:

This panel discussion addressed the development of high-performing information security policies, processes, and technologies that address all facets of the new IT environment. In addition, the panel identified the measurements and metrics that a CISO should use to effectively quantify improvements of their information security program.

CISOs are faced with a rapidly evolving threat landscape, where the infusion of diverse mobility devices, the acceleration of cloud computing, and the exponential growth of business related social media have essentially obliterated the legacy concept of perimeter network security. In order to implement a high-performing IS program, today's CISO must proactively develop "defend, detect and react in real-time" strategies that robustly address threats emanating from across the spectrum. A key component for success will be the CISO's ability to convince C-suite and Boardroom leaders to wholeheartedly endorse and fund existing security program changes. To obtain such a high-level of executive sponsor buy-in, the CISO must be able to demonstrate that developing a high-performing information security program will further protect sensitive organizational data, adhere to regulatory and legally mandated privacy requirements, while simultaneously not hampering business processes; all with an eye on reducing the TCO for the IT infrastructure.

"Implementing a High-Performing Information Security Program": (From left to right) *Kevin McPeak*, Senior Systems Engineer, CACI International Inc, *Nitin Kumar*, Interim CISO, *Zachery Mitcham*, CISO, University of North Carolina Wilmington, *Richard Rushing*, Senior Director of IS, Motorola, *Karthik Swarnam*, CISO, Transunion

"Structuring and Managing Your Infosec Workforce": (From left to right) *Jeffery Vinson*, Director & CISO, SecureNet Payment Systems, *Jerry Chappee*, Chief Information Assurance & Operations Officer, U.S. Army Reserves/ Disaster Recovery Manager, Blue Cross Blue Shield, *David Simpson*, CSO, Cyber Security Forum Initiative, *Steven Fox*, Security Architect & Engineering Advisor, U.S. Department of Treasury, *Nitin Kumar*, Interim CIS, Jim Wiggins, Executive Director, Federal IT Security Institute, *Michael Rushinsky*, Director, Sallie Mae

"Structuring and Managing Your Infosec Workplace" Panel Objectives:

This panel concentrated on the importance of getting management's approval and creating a highly-skilled and agile security team that is laser-focused on stopping the cyber threats and educating the entire workforce on their role in information security.

In this rapidly changing security and threat landscape it is important to be able to adapt and overcome the challenges on a daily basis. Security executives must be able to defend and protect their organizations from cyber criminals and insiders that pose significant risk to the business.

"Achieving PCI DSS Compliance in Cloud": (From left to right) *Michael Berman* (not pictured), CTO, Catbird Networks, *Mike Dahn*, Director, PricewaterhouseCooper/Founder, Security B-Side, *Eric Svetcov*, Evangelist, TrustInMotion & SV Technology Ltd, *John Lamboy*, Director, eGlobalTech, *Jeff Tutton*, President, Intersec Worldwide/ AVP, MedeAnalytics, *Juan Gomez-Sanchez*, Principal/Founder, Optima Consulting Inc

Top 3 Takeaways from "Structuring and Managing Your Infosec Workforce":

By: Jeffrey Vinson (Director & CISO, SecureNet Payment Systems) & Jerry Chappee (Chief IA & Operations Officer, U.S. Army Reserves/Disaster Recovery Manager, Blue Cross, Blue Shield)

1. There is not a perfect reporting structure; all of them have strengths and challenges.

2. Certifications are very helpful in creating a baseline level of understanding, but there has to be experience to support the certification.

3. The leaders of the organization need to support their people and show them the importance of a certification. More specifically, how the certification directly supports the business and keeps information more secure.


David Simpson


Steven Fox


Jim Wiggins


Michael Rushinsky


John Lamboy


Jeff Tutton


Eric Svetcov


Juan Gomez-Sanchez

Top 3 Action Items for CISOs to Explore/ Implement from "Structuring and Managing Your Infosec Workforce":

By: Jeffrey Vinson (Director & CISO, SecureNet Payment Systems) & Jerry Chappee (Chief IA & Operations Officer, U.S. Army Reserves/Disaster Recovery Manager, Blue Cross, Blue Shield)

1. Improve the certification process for the team.

2. Review the options on the reporting structure. Explore the ideas of collaborating with the auditing department or reporting through the legal department.

3. Lead by example: Ensure that support is given to the team and keep focus on how the overall strategy of IT Security and certifications directly sustains and helps drive business.

"Achieving PCI DSS Compliance in the Cloud" Panel Objectives:

This panel discussed requirements and best practices for attaining and sustaining PCI DSS compliance in the cloud. Topics included CISOs, QSAs, cloud providers, and subject matter experts in cloud security. Leveraging their direct expertise in implementing, testing, and certifying systems for PCI Compliance, the panel speakers discussed risk assessment, mitigation, and the value of moving some or all of the operations to private or public cloud infrastructures. The panel included perspectives on PCI Compliance in Software as a Service (SAAS) and Infrastructure as a service (IAAS) cloud architectures.

"Monitoring and Evaluating Your IT Security" Panel Objectives:

This panel discussed the various methods that organizations use to monitor (assess compliance to policies) and evaluate (assess effectiveness) IT security policies. Among the topics was a discussion of the usage, value and implementations of Governance Risk and Compliance (GRC) software packages.

"Factors with Greatest Impact on the Information Security Profession" Panel Objectives:

This panel session recognized the evolution of the Information Security profession to a business focus and included actionable examples with lively discussion. The goal was to share specific experiences to empower attendees' current direction, challenge it, or disagree with the panel speakers all together. It started with core factors to embed security into business and IT priorities, facilitate evidence-driven risk decisions, and drive incremental execution. Then, addressed factors and skill gaps seen today and in the future (e.g. actionable risk management, consumerization, leadership, social media, etc.)

"Factors with Greatest Impact on the Information Security Profession": (From left to right) *Jared Pfost*, CEO, Third Defense, *Steven Fox*, Security Architect & Engineering Advisor, U.S. Department of Treasury, *Angelique Grado*, Director, Dexa Systems, *James Synovec*, CIO, Aquila Business Services, CISO, Rocky Mountain School of Ministry & Theology, *Ira Winkler*, Chief Security Strategist, Codenomicon/ President, Internet Security Advisors Group, *Juan Gomez-Sanchez*, Principal/Founder, Optima Consulting Inc

"Monitoring and Evaluating Your IT Security Policies": (From left to right) *David Simpson*, CSO, Cyber Security Forum Initiative, (Not pictured) *Mary Siero*, CEO, Innovative IT LLC, (Not pictured) *My-Ngoc Nguyen*, VP, Link Technologies, *Steven Fox*, Security Architect & Engineering Advisor, U.S. Department of Treasury, *James Synovec*, CIO, Aquila Business Services, CISO, Rocky Mountain School of Ministry & Theology

My-Ngoc Nguyen

Steven Fox

James Synovec

"Managing Insider Threats" Panel Objectives:

This panel explored the journey to the insider ally. Who is an insider? What's considered an insider inappropriate activity? What do you do about it? Some of the common culprits include software development, employee portals, firecall tasks, etc.

People are the key ingredients to an organization's success. In today's world security professionals have a handle on external threats or are prepared to deal with them. Elements to addressing the insider are no different than addressing any business problem (i.e., early detection, confirmation, containment, and eradication). There are frame works available, one such example is the MERIT framework from CERT. Reasons for insider betrayal include theft, fraud, and sabotage resulting in financial gain, revenge urge among others. There is a human element; there is a purpose, and a method. Managing the insider threat includes understanding the threat vector, opportunities, and elevating solutions that span from a deterrent to preventive controls.

(From left to right) Karthik Swarnam, Illyas Kooliyankal

Angelique Grado

James Synovec

Ira Winkler

Juan Gomez-Sanchez

"Managing Insider Threats": (From left to right) *Karthik Swarnam*, CISO, TransUnion, *Illyas Kooliyankal*, CISO, Abu Dhabi Securities Exchange, *Robert Hotaling*, CSO, Cengage Learning, *Ben Eu*, Program CISO, IBM, *Karl Krispert*, VP, Aujas, *Zachery Mitcham*, CISO, University of North Carolina Wiilmington, *Oliver Gruskovnjak*, CTO/ Director Penetration Testing, Portcullis Inc

(From left to right) Karl Krispert, Zachery Mitcham, Oliver Gruskovnjak

Ben Eu

Karl Krispert

Zachery Mitcham

Robert Hotaling

Oliver Gruskovnjak


Eric McKim


Edward Ray


Paul Nguyen


Andrew Sispoidis

"Preparing for Future Challenges" Panel Objectives:

Took a risk-based approach to proactively managing future security challenges over the next few years' horizon.

Key Topics: Risk vs. Reward. Tactical vs. Strategic. Balancing the tradeoffs.

Ever changing technology and paradigm shifts that carry future security challenges: Mobile Computing, WiFi/3G/4G, Multimedia, Cloud Computing, Social Media, personal devices, HTTP tunneling, increasing regulatory governance, etc.

Discussion points: What are the highest risks and threats that are coming down the pike facing all of our market verticals and why? How do we effectively and efficiently manage the ever evolving information security risk landscape and adequately mitigate that which we cannot control?

"Preparing for Future Challenges": (From left to right) *Michael Rushinsky*, Director, Sallie Mae, *Paul Nguyen*, VP, Cyber Solutions, *Eric McKim*, Senior VP/ CISO, Business Integra, *Edward Ray*, CISO, MMICMAN, LLC, Andrew Sispoidis, Executive Director, The Center for Global Information Security

Top 3 Action Items for CISOs to Explore/ Implement from "Preparing for Future Challenges":

By: Michael Rushinsky (Director, Sallie Mae).

1. Research and Pilot: Out-of-Band Authentication - native telephone-based two-factor authentication.

2. Gain an in-depth understanding of Stuxnet and the supply-chain risk and develop a strategy to adequately mitigate the risk.

3. Apply the insider threat philosophy - the goal of an outsider is to first become an insider and then see what they can accomplish - to the International Cyber Warfare issue - the goal of a foreign perpetrator is to first become a domestic perpetrator and then see what they can accomplish.

Top 3 Takeaways "Preparing for Future Challenges":

By: Michael Rushinsky (Director, Sallie Mae)

1. International Cyber Warfare is equivalent to Domestic Cyber Warfare and Organized Crime due to the fact that personal home computers are the weakest link and highly susceptible to compromise. A foreign country could launch a large-scale attack on US Companies that originates domestically.

2. Balance the tradeoffs and enable the mobile workforce and personally-owned devices in the workplace while adequately mitigating the risks through scalable automated policy enforcement technology solutions.

3. Generally accepted professional social media, such as LinkedIn, have significant human intelligence risk. That risk must be adequately mitigated.

Jay Bavisi, President and Co-Founder of EC-Council, closes the summit with closing remarks and a bid farewell

The CISO Executive Summit's 2 day duration and interactive nature provided a great opportunity for networking between panel participants and attendees. The conversations continue of EC-Council's Global Executive CISO Summit LinkedIn page.