

**15th Annual**

**ContinuityInsights**

**2017 MANAGEMENT  
CONFERENCE**



**April 24-26, 2017**

**Marriott Denver City Center  
Denver, Colorado**

# 2017 Conference Session Guide



Join us in Denver, Colorado  
– The Mile High City –  
for the industry's leading conference  
for strategic business continuity  
management.

**REGISTER AT:  
[www.CIManagementConference.Com](http://www.CIManagementConference.Com)**

---



## 2017 Conference Session Guide

### Conference Tracks

- |  |                               |
|--|-------------------------------|
| A. Case Studies                        | E. Emerging Technology        |
| B. Trending                            | F. Professional Development   |
| C. Program Development and Advancement | G. SME (i.e. ask the experts) |
| D. Measurement, Metrics and Maturity   | P. Plenary                    |

**MONDAY, APRIL 24, 2017**

**8:00 a.m. to 9:30 a.m.**

**Plenary Session**

#### **P1: Institutional Knowledge! When Good Employees Leave, What Do We Really Lose and How Do We Retain It?**

*Dr. Andrew Pena, New Mexico State University*

Every day when a good employee leaves their job, they're "walking out the door" with a very valuable asset. They leave with the valuable information they learned about their jobs, or what you trained them on. Whether it be only for a year or so, or if it was for more than twenty years? They leave with their institutional knowledge or memory. This is what happens to an organization loses its best, brightest, most experienced and knowledgeable employees. Keep in mind, that not all employee turnover is "bad" turnover. Sometimes, there are employees that we'd like to leave sooner rather than later. But regardless of the good or bad types of turnover, what we're finding is that these employees are leaving work with a substantial amount of work, business, and operational knowledge that'll be difficult to replace or duplicate if internal systems to retain or document this type of knowledge are non-existent.

**9:45 a.m. to 10:45 a.m.**

**Breakout Sessions**

#### **B1: The Next Generation of Crisis Management and Business Continuity: How Gen X and Millennials Will Change the Landscape**

*Grace Burley, Strategic Crisis Advisors*

As the power base within companies is changing include more to Gen X and Millennials, crisis management and business continuity programs will need to adapt. Our industry must find ways to communicate and implement our programs in better ways. In this presentation, Grace Burley will explore how to best use metrics and the power of a great story to communicate with Gen X and Millennials to get their buy-in and develop plans and tools to support them.

#### **C1: Developing a New Business Continuity Program – What My Program Looked Like One Year After I Started a New Job**

*Ron Kamps, Mutual of Enumclaw*

How much can you expect to create/develop/mature in your first year managing a business continuity program? What is reasonable to promise, what do you prioritize, and how do you gain support? Follow my journey of the first year at a new organization. Each week, I journaled my activities; what worked, what did not, and what I learned. You will hear about my approach to developing a program, how to start fast, how I gained support, how I held people accountable, how I managed a program with no resources and what I worried most about. As a case study, you will see/hear examples, of the various program components, definitions, activities, hierarchy, reporting, tools, task lists and tips. This course is applicable for those who are planning to start something new, recently started something new, or are looking to jumpstart or mature an existing program or program component.

#### **C2: Choosing a Tabletop Scenario for Your Next Exercise**

*Kathy Lee Patterson, Independence Blue Cross, and Melissa Owings, Blue Cross and Blue Shield of Nebraska*

Many Business Continuity professionals regularly exercise their response plans by conducting Tabletop Exercises by simulating different types of disaster scenarios. This presentation is designed to provide many different ideas for disaster scenarios with different impacts to your organization. For example, there will be scenarios for the impacts of shelter-in-place, computer disruptions, leadership vacancies, facility disruptions, etc. Stories will be given to each impact type. There will be a portion of the session dedicated to breaking the group into smaller groups and working through different types of scenarios that will be given to you. The goal is to give each participant some new ideas for disaster scenarios for their exercises.

#### **E1: Management and Prevention of Cyber-attacks in the Real World**

*Frank Buck, Senior Product Manager, Sungard Availability Services, and Doug Sawyer, Disaster Recovery Coordinator – Team Lead, Kroger*

The cybersecurity outlook has never been more dire. State-sponsored data breaches have turned cybercrimes into weaponized attacks, and all companies will have experienced a cybersecurity incident by 2020. Ransomware is currently one of the most devastating and popular attacks that can bring an organization to a standstill. We'll show you how a large enterprise tackles this problem and you'll learn how to weather the inevitable attacks, minimize the damage, and get back to business.

### **G1: Developing a Strategic Training Plan**

*Mike Keating, RGA Reinsurance, moderator (panel TBA)*

Training and awareness is one of the most important activities performed by BC professionals, but it is also a significant challenge. Unfortunately, there is often very little strategic focus and planning when it comes to executing the organization's business continuity planning processes, as well as executing response and recovery strategies. In this session, the panel will share the best of what we receive from the attendees, as well as offer commentary on best practices and solid solutions to build individual competencies and create awareness throughout the organization.

**11:00 a.m. to 12:00 p.m.**

**Breakout Sessions**

### **A1: Cyber Incident Response: It's Not Just for Techies!**

*Tracy Judge, Trans Union and Peter Laz, Fusion*

As continuity professionals, we make sure we have plans in place to handle just about anything. We are well prepared for many types of physical disruptive events. However, data incidents are the threats that keep CEOs up at night! Cyber-attacks and data breaches are the top threats perceived by businesses; and can easily have a catastrophic effect on your business and even the safety and livelihood of your customers and employees. We need to leverage the knowledge and experience we have for plan building, resource coordination and response management to build holistic data incident response plans that enable our company's to face these top threats with confidence. This session will present proven ideas and tips for you to maximize the effectiveness and efficiency of managing cyber-related events within your overall BCM program.

### **C3: The Evolution to Building Effective, Resilient & Compliant Plans**

*Christopher Duffy, Strategic BCP*

Building both business continuity and disaster recovery plans can be onerous for the owner of the plans. Most plan owners don't have the time to focus on building an effective plan. Instead they just add or update the one they inherited. This session will provide a correlation between the intersection of continuity plans, brain functions, and human nature to provide the basis to create and build resilient and easy-to-maintain BC/DR plans that the entire organization can embrace.

### **D1: Regional FIRST Coalitions & New Critical Infrastructure Info Sharing – Panel Discussion**

*Panel Leader: Susan Rogers, FS-ISAC Director of Business Resiliency*

*Panelists: Brian Tishuk, RPCfirst, Greg Gist, Northeast FIRST Executive Director, Monika Stoeffl, California FIRST Executive Director, Robin Remines, Mid-Atlantic FIRST Executive Director*

Learn about development underway for public/private partnerships known as the regional FIRST Coalitions, including: Mid-Atlantic FIRST, Northeast FIRST, and California FIRST and how you can get involved. The FIRST coalitions formed organically in various cities or states, originally within the banking/finance sector, but several have developed into multi-sector coalitions. Regional coalitions build local crisis response relationships that can bring ground-truth information sharing to their members. Because of the importance of ground-truth situational awareness to protect critical infrastructure, the private sector, Financial Sector Information Sharing and Analysis Center (FS-ISAC) is supporting Coalition growth efforts. The panel discussion format will debate information sharing challenges and how these are overcome by building trusted peer relationships between members to benefit their organization's situational awareness needs. Coalitions are also positioned to connect their members with national, critical infrastructure info sharing and critical-sector crisis response activities. Conference participants will speak directly with FS-ISAC resiliency leaders and the executive directors of Mid-Atlantic FIRST, Northeast FIRST, and California FIRST regional coalitions to learn how to join in these new FIRST coalition efforts.

### **E2: Top Five Things You Can Do Right Now to Modernize Your Business Continuity Program**

*Tejas Katwala, Continuity Logic*

As the pace of change in business and technology accelerates, business continuity management (BCM) continues to evolve rapidly within enterprises to meet increased market and regulatory demands. New strategies need to be assessed by the enterprise from many perspectives, including impact on existing processes, associated risk, and how emerging approaches to resiliency can be leveraged to improve continuity capabilities. In this session, Tejas Katwala, CEO of Continuity Logic shares his top five transformational things you can do right now to modernize your business continuity program.

Participate in this session to hear Katwala discuss how to:

- Reposition and restructure a BCM department to be positioned as a revenue center
- Break down silos and provide meaningful insights to other functions
- Improve program adoption
- Track performance and maturity

### **F1: BCM Trends – Understand the Impact to Your Program and Career**

*Cheyene Marling, BC Management*

The Business Continuity profession has and will continue to evolve. With the convergence of risk management, security and cyber security, it's important to understand the current trends and the potential impact to the visibility of your program and your career growth. During this session, we'll assess data trends going back 10 years. How are these trends impacting the visibility of Business Continuity and what steps should you take to better position your future career and marketability?

**1:00 p.m. to 2:15 p.m.**

**Breakout Sessions**

### **A2: Turn Up the Volume: Building a Global BCM Training Program in a Busy, Distracted World**

*Lisa Trousdale, Ernst & Young, and David Mack, Ripcord Solutions*

Are you challenged by the daunting task of training your organization in BCM when everyone (including you!) is stretched thin and pressed for time? Explore emerging trends, how adults learn, and ways to leverage technology to stretch your training budget. Hear how a large multinational company, with over 200,000 employees in 120 countries, developed and implemented a business continuity management training framework that includes short videos, facilitated sessions and virtual instructor-led exercises. Takeaways include ideas for how to focus your training objectives and turn up the volume on your own program.

#### **C4: Business Continuity Exercises: Creating Scenarios to Achieve Goals**

*Laurie Wonders, TriZetto*

Do you set exercise goals you want your teams to achieve, or practice, before defining your exercise scenarios? Are you more likely to create an exercise and then guide your team through it, hoping they learn something along the way? The scenario itself should be less important than the impact it has on your team's ability to conduct business and follow their contingency plan. It's important to start with a goal for your team and then decide how to best create an exercise which will help them learn and meet those goals. During this workshop, you can practice identifying exercise scenarios and injects to achieve your recovery goals. We'll start with a basic plan, then look at creating an exercise for a more advanced team, and finally, we will look at a specialized plan and recovery goals with some more creative injects and challenges.

#### **C5: Everything You're Doing is Wrong! (and Other Helpful Hints from the Continuity 2.0 Manifesto)**

*David Lindstedt, Readiness Analytics*

A BIA? Don't do it. Risk Assessment? Skip, it. Documentation? Eliminate most of it. For 20 years or more, we practitioners have followed the same best practices. But are they "proven practices"? Could there be a reason that our skills are undervalued by our organizations and leaders? Is there a better way? This session will discuss the emergence of a new, exciting, "Lean" alternative to traditional preparedness planning practices; starting with the drivers behind the need for a sea change and the nine principles of the Continuity 2.0 Manifesto. This is no mere theoretical discussion – attendees will be challenged to change the way they do planning and given the framework and justifications to get more recognition for their efforts. Attendees will be able to begin to put these principles into practice they day they leave the conference.

#### **C6: Rapid Continuity: Can We Recover**

*Phil Lambert, Ripcord Solutions*

Planning as it should be: smart, systematic, practical, and functional. The Rapid Continuity program represents a major breakthrough in the design and approach to the strategic and tactical implementation of the resiliency planning process. These components are innovative and unique in their ability to establish buy-in, ownership and participation.

**1:00 p.m. to 3:45 p.m.**

**Workshop (A 2-hour, 45-minute session)**

#### **B2: Cybersecurity Update for Business Continuity Community**

*Dr. Nader Mehravari, Axio*

A day rarely goes by where we don't hear about a multitude of cybersecurity events adversely affecting public and private organizations, communities, and even nations. It is, therefore, critical for business continuity, incident management, disaster recovery, and emergency management professionals and practitioners to continually stay abreast of the latest and ongoing developments in the cybersecurity arena. This workshop is intended to provide an overarching update on the cybersecurity landscape focusing on the needs of business continuity community.

**2:30 p.m. to 3:45 p.m.**

**Breakout Sessions**

#### **A3: Case Study: Workplace Violence Awareness and Prevention Training –How UPS Improved Its Workplace Violence Program**

*Chris Summerrow, UPS, and Randy Spivey, Center of Personal Protection and Safety (CPPS)*

The likelihood of violence, threats and injuries in our workplace seems much more probable today than in preceding times. Are you and your employees prepared to identify, assess and respond to threatening situations in workplace? Have you assessed your workplace violence (WPV) program against the ANSI, SHRM or ASIS standards? Do you have Threat Assessment Teams set up in your operations? Have you considered multi-media training solutions to enhance your program? If you answered NO to anyone of these questions, join us in this session. UPS and CPPS will review a case study on how workplace violence awareness and prevention programs were assessed, improved and deployed across a large organization with success.

#### **C7: Is Your Company Prepared for a Catastrophic Data Breach?**

*Suzanne Hartin, Early Warning, and Chris Belt, PNC*

Given the escalating trend of data breaches across all industries, no one can assume they are immune. Having a strong information security program, a strong incident management program and a strong service continuity program is not sufficient. If it happens to you and you want to save your company's reputation, you need to have practiced this scenario in all its complexities, engaging stakeholders that might not be engaged in other scenarios. Join this session to learn how to plan and execute an effective cyber breach tabletop, the broad range of people that need to be engaged, and considerations that are imperative but have nuances that might not be obvious. Take away specific approaches to planning and tips and tricks to help you prepare your team and company for a catastrophic data breach.

#### **D2: Capturing, Consolidating and Communicating Critical Continuity Data in a Concise, Electronic Way**

*Jeremy Gudgeon and Rebecca Harding, Vanguard*

The goal of this presentation is to create awareness around how to build a basic, electronic repository of business continuity information. The document will not supersede or replace a business area's continuity plan, rather it provides the user a place to "capture, consolidate, and communicate critical continuity data in a concise, electronic way." The session will focus on the concepts to source and document (People, Process, Technology, Suppliers and Workspace), and ways in which that data can be populated in easy-to-reference ways. Finally, the presenters will discuss the idea of creating metrics and reporting basic findings into a dashboard embedded within the document.

#### **E3: Information Technology Risk: What You Need to Know**

*Michael Herrera, MHA Consulting, Inc.*

In today's business environment, the great risk to organizations is technology. Reputation risk, complexity risk, cyber security risk, cloud-computing risk... practitioners must refocus on these daily occurrences. Technology risk is not an isolated IT problem, there is a responsibility to help the organization overcome these challenges, regardless of your specific role. In this "non-traditional IT recovery" discussion, attendees will engage with a panel of experts to better understand the risks, its challenges, and recommendations.

4:00 p.m. to 5:00 p.m.

Breakout Sessions

#### **A4: Lessons Learned from History Past**

*Joe Flach, Safe Harbor Consulting*

From the First Interstate Bank fire disaster in 1988 to the disastrous West Coast forest fires in the summer of 2016; from the Oklahoma City bombing to the World Trade Center attacks; from Hurricane Katrina to Superstorm Sandy; crisis management, business continuity, disaster recovery, and emergency preparedness planners have had ample opportunity to learn lessons from historical business interruption events. But are the lessons really being learned? Are we leveraging these experiences to improve our preparedness posture or do we keep repeating our mistakes? This session will identify challenges that seem to recur in each event, as if the lessons were never really learned, as well as those that we seem to have remedied in maturing programs and associated plans. We will take a look at a number of real life disasters to examine similarities and differences in responding to crises and explore opportunities to not repeat our mistakes.

#### **C8: Continuity Confessions**

*Howard Mannella, Alternative Resiliency Services*

Learn from others' mistakes! This is a pivot from 'best practices' and 'how to do it right' - this is a highlight of errors and wrong turns organizations have made, so you do not make the same ones yourself. This session will feature a senior panel showcasing and discussing one-slides featuring wrong decisions taken, missteps in recoveries and other "could have done it differently" examples, collected anonymously via survey of attendees and presented without identifying information. You will gain key takeaways that will help you avoid the pitfalls others have encountered.

#### **D3: What Is Your Risk Appetite?**

*Lynnda Nelson, ICOR*

ISO 22301 requires that the organization define its risk appetite as part of its business continuity program. This is a new program requirement for many business continuity practitioners. A clearly understood and articulated statement of risk appetite provides the direction needed to identify acceptable risk treatments and implement business continuity strategies. When risk appetite is properly understood and clearly defined, it becomes a powerful tool for managing risk. However, thinking about risk appetite is often unclear, definitions can be vague, and the gap between theory and practice can be wide. This presentation will help you to understand the purpose and importance of the risk appetite statement(s) and provide guidance on how to document your organization's risk appetite as it relates to business continuity management.

#### **D4: Why Your Vendors' Subcontractors Are Putting You at Risk**

*Brandon Tanner, Rentsys*

Transcription vendor. Payment card processor. Cloud services provider. These are just a few examples of the growing number of vendors that have been responsible for breaches of their clients' data. You won't see their names in the spotlight, though. Instead, the businesses who hired them shoulder the blame. The reason? Clients, business contracts and federal regulations alike hold businesses responsible for making sure third-party technology service providers are able to ensure the availability and privacy of data. If so, how do you address fourth-party risk? In this presentation, the presenter will discuss best practices for selecting third-party providers and for maintaining ongoing oversight of third parties and their subcontractors.

#### **F2: BCI Global Research Summary – Key Trends, Influences and Conclusions Affecting the Profession**

*John Jackson, BCI USA Chapter*

On a global scale, the BCI performs considerable research and creates dozens of original publications summarizing industry trends, emerging threats and other topics influencing the way in which organizations prepare for disruptive events. This presentation will highlight a number of key conclusions, as well as the implications for business continuity and organizational resilience professionals. Join us for this interactive session where John Jackson, USA Chapter Board Member, will summarize this research and invite audience reaction to key conclusions.

TUESDAY, APRIL 25, 2017

8:00 a.m. to 9:30 a.m.

Plenary Session

#### **P2: Legal Aspects of Corporate Crisis Management**

*Stephen Williger, Esq., Thompson Hine LLP*

Your company may have considered the operational aspects of a crisis. But, has it considered how to handle the legal consequences that could include waiver of the attorney-client privilege, government or regulatory oversight, sentencing of the company or other wrongdoers, the possible need for an internal investigation and significant litigation? Has your company considered the urgent need for truth in a crisis in the age of "alternative facts?" Will your company be the target of Presidential tweets in a badly handled crisis? The legal aspects of pre-crisis planning, mitigation, remediation, and recovery will be explained in clear language.

9:45 a.m. to 11:00 a.m.

Breakout Sessions

#### **A5: If BC/DR is the Heart of Your Program – Collaborative Recovery is the Life Blood**

*Stuart Murray, Jabil Circuits, and Aaron Callaway, Fairchild Consulting*

Collaborative recovery enables an operationalized approach to business continuity and disaster recovery that facilitates a resilient organizational culture. By managing BC/DR on an enterprise platform, Jabil Circuits, a global US-based manufacturing services company, is able to work where the business works, unifying business continuity and disaster recovery with normal IT operations. In addition, having a platform-based BC/DR tool means doing more with the applications you already own. Does your organization really need another application? Jabil Circuits recognized the power of leveraging one of their existing enterprise platforms and how it was able to naturally from bridges across the organization.

### **B3: Maximizing Millennials in BCM**

*Margaret Millett, MetLife and Joanna D'Aquanni, SAS*

By 2020, almost half of the workforce will be millennials and more Baby Boomers will be looking to enter retirement. Millennials are taking a risk by entering the Business Continuity profession since most of them have not studied the subject at university. Attend this session to learn first-hand insights to maximize the value of millennials in your BCM Program. Special attention will be given to the nuances of hiring, training, managing, growing and retaining millennial talent. Tips will also be shared on creating an environment where millennial employees feel supported and valued by the leadership will lead to increased productivity and valuable relationships. Attendees are asked to bring their experiences for a best practice discussion.

### **D5: Process Maturity vs. Program Capabilities – Resilience Strategy and Operating Effectiveness (RSOE)**

*Dave Sarabacha, Deloitte*

BCM program assessments generally focus on the identification of program gaps, including inadequate program documentation, incomplete process and procedures, and level of adherence to industry standards and best practices. However these assessment seldom fail to provide executives with the answer to most important questions – ‘Can we recover? How confident are we? Can we recover efficiently and effectively?’. The RSOE concept focuses on determining the operating effectiveness of your program processes and the level of recoverability it has created for your mission critical functions. It helps with the discovery of recoverability gaps, including business readiness, validation of recovery resource priorities, vetting of documented strategies and project assumptions, and evaluation of recovery capabilities.

### **E4: People: The Missing Ingredient in IT Recovery**

*Steve Ross, Risk Masters International*

You’ve got the DR site. Your data is backed up. But when the time comes that you need to recover – FAST – you find that IT recovery is still labor-intensive and costly. Huge enterprises are in a better position to deploy technical specialists and facilitate rapid recovery, but small and medium size businesses (SMB) are often much more constrained. Moreover, businesses of all sizes have outsourced many technical functions overseas, where personnel might not be able to communicate with the systems they support until after they are recovered. This presentation is directed to the Business Continuity and IT Disaster Recovery personnel who often find advanced IT recovery beyond their reach and their budget. It addresses techniques including broad cross-training, contingent outsourcing and Disaster Recovery as a Service (DRaaS). The session points to the problems faced by small (even one-person) Business Continuity Management functions that are concerned that their organizations’ IT recovery capabilities do not align with their Recovery Time Objectives.

### **G2: Exercise Facilitation Techniques**

*John Jackson, Fusion Risk Management, moderator (panel TBA)*

Exercises are an excellent tool to develop competencies, create organizational awareness, identify opportunities for improvement, engage management, and prove that response and recovery capabilities work. Our panel is highly experienced in developing and facilitating exercise sessions that dramatically improve preparedness and management buy-in. This session will be a highly interactive discussion of ideas and techniques, ensuring that attendees leave with relevant and usable takeaways.

**2:00 p.m. to 3:15 p.m.**

**Breakout Sessions**

### **A6: You're Having a Disaster, Now What?**

*Tom Serio, Verizon Wireless*

The presenter will walk you through a real disaster that impacted a large business and forced them to enact ALL of their business continuity plans. What's the reality of the situation? What's were upper management thinking? How do quickly and successfully did employees get back to work? Learn from some very valuable and real lessons learned while recovering a corporate campus from a nine-day outage.

### **A7: Setting a New Standard for Integrated IT Recovery Orchestration**

*John Steffen, Charter Communications and Bob Sibik, Fusion*

Flexibly integrating your IT Disaster Recovery & Crisis/Incident Management program with ServiceNow and other ITSM systems can deliver the right combination of strategy, processes and technologies to minimize recovery times and reduce execution risk. This session presents a case study addressing the approaches, program frameworks, and benefits of achieving efficient and seamless collaboration among all teams involved in IT DR testing and recovery events. You will learn strategies, tips and techniques to prepare for tests more efficiently; conduct complex simulations more effectively; respond more quickly to IT disruptions; achieve command & control at every stage; and organize your program for accurate and up-to-the-minute reporting.

### **C9: Major Challenges to Implementing an Effective Business Continuity (BC) Program and How to Overcome Them**

*Mike Janko, Goodyear Tire & Rubber Company, and Chris Summerrow, UPS*

There are many textbook definitions and opinions as to what makes your BC program a success, yet many believe an effective BC program is one that is recognized as having business value. How do you accomplish this? What are some of the many obstacles you will likely face on getting personnel at all levels and job functions to “buy into your BC process”? Join us for this session which will include an overview of many key techniques relating to implementing your BC process for the right reasons, who you should engage, what are the most common issues that could stall your progress and the impact of human element factors as a key contributor to your program’s continued success.

### **C10: Crisis Management Simulation**

*Frank Shultz and Stephanie Marjoram, BC in the Cloud*

The first several hours following an incident are critical and it’s within this time period that we will be conducting our simulation. After dividing into teams, we will engage in a live, interactive simulation in which each team will coordinate responses as the situation unfolds. We will review several scenarios of varying difficulty and complexity and will discuss all aspects of communications relevant today including social media. By the end of the session, you will be able to assess if your organization is prepared for the next event and you will have additional tools in your belt with which to build out a successful crisis

### **G3: The Case for Developing Organizational Resilience Capability**

*Mark Carroll, Income Research, moderator (panel TBA)*

Out of the box thinking and taking creative, innovative actions to address those ideas are a few of the keys to developing the capability for organizational resilience. Attendees will learn of and discuss examples of creative and innovative actions taken to improve the resilience capability of the organizations profiled. This session will consist of a series of five- to seven-minute presentations by various practitioners on innovative approaches that have been taken to enhance organizational resilience capability that were neither intuitive nor obvious and the capabilities that have been put in place. The session will include a brief Q&A with the practitioners profiled.

**3:30 p.m. to 4:30 p.m.**

**Breakout Sessions**

### **A8: A History of Tabletops**

*Blaise D'Ambrosio, T. Rowe Price*

Over the past 10 years, T. Rowe Business Continuity has gone from doing one executive level tabletop exercise a year to at least five. In this session, the presenter will review how his firm develops, prepares, and delivers tabletop exercises, producing successful outcomes, leading to internal demand for more. This interactive discussion will cover past mistakes and current good practices. Topics will include how to choose appropriate scenarios, how to use tabletops to further the expansion into organizational resilience, and the takeaway: a packet list of tabletops, the scenarios, objectives, and lessons learned.

### **B4: How to Control the Message in Today's Connected World: Social Media and Crisis Management**

*Ted Brown, KETCHConsulting*

Social media has become a major channel for connecting with customers, but businesses are wary because ultimately it is harder to control the message on social than on other media. During a crisis, the stakes are even larger. Social media is only part of a greater crisis communications system, but in the moment, it may be your quickest and first method to react to a situation. In this session you will learn how social media can be a powerful tool for crisis management. The session will look at the different procedures and philosophies with using social media when handling internal and external incidents. Also discussed will be the role of an Incident Command team in using social media.

### **E5: Doing What Technology Can't: The Use of Risk Transfer in Managing Resilience and Cyber Risk**

*Dr. Nader Mehravari and David White, Axio Inc.*

We now live in a world that has experienced cyber induced physical damage, blackouts, hacking of medical devices, automobile recalls, fraudulent funds transfers, and resulting implications to board of directors and officers. Company executives face tough decisions on how much to spend and what investments to make to improve their organization's operational resilience and cybersecurity posture. Business continuity and cybersecurity programs and associated investments are a means to reduce the potential impact from operational and cyber risk. Organizations' initial cybersecurity investments should be, and often is, focused on capability development; i.e., the implementation of controls to protect and sustain business operations that depend on information and operational technology. However, as the organizations' cybersecurity capability increases, additional capability investments produce diminishing returns. At that point, utilization of modern risk transfer and cyber insurance instruments becomes an effective and economical means to further reduce risk. This presentation will provide a comprehensive overview and the current state of this important emerging field.

### **D6: Executive Buy-in of Your Business Continuity Management Program**

*Lance Stange, Virtual Corporation*

Let's face it. Executive buy-in is not easy to get. Business continuity, disaster recovery, & organization resilience management requires buy-in from the entire organization, from the top down, across all departments & across external service partners & providers. This session will discuss five steps for building executive buy-in of your organizational resilience management program:

- Step 1: Define Organizational Resilience or Business Continuity as it best relates to your organization or industry.
- Step 2: Determine a baseline by measuring your company's continuity maturity
- Step 3: Regulatory & government compliance – know the laws
- Step 4: Conduct a business impact analysis
- Step 5: Share the financial impact with executives to justify resources for program

### **C11: Resiliency Meets New Complexities of a Hybrid World: The Need to Bring a Paradigm Shift in Business Resiliency**

*BJ Klingenberg, IBM, and Vinod Kuppasamy, Sanovi, an IBM Company*

Disruptions in business are daily occurrences. How you prepare for those disruptions will make the difference in whether your Resiliency strategy will cost you money, or save you money. With cloud-enabled Resiliency as a Service delivered through IBM's Software Defined Resiliency Framework you can maximize the value and flexibility of your existing disaster recovery assets as well as ensure enterprise-wide DR and availability management across physical, virtual and cloud IT environments supporting lower RTO for hybrid environments. This session will feature a newly published global study on Disaster Recovery Orchestration which enables best practice adherence, enhanced readiness, and automated validation for Hybrid IT environments.

**WEDNESDAY, APRIL 26, 2017**

**9:00 a.m. to 10:00 a.m.**

**Plenary Session**

### **A9: Lessons Learned from the 2016 Flood in Louisiana**

*Bonnie Canal, The Resiliency Institute*

This presentation will focus on the causes, effects and long term challenges faced by the public and private sectors after the catastrophic flooding in Louisiana. We will focus on the lessons learned by all parties involved with special attention paid to the recovery efforts of the business community. We will offer real, tangible takeaways for all participants on how to be prepared for these types of events and the opportunities for businesses to (be)come more resilient.

### **C12: Streamline Your Risk Assessment in Four-Steps and Learn How-To Attract BCM Investment to Your Recommendations!**

*Shane Mathew, DaVita Rx, and Christopher Rivera, Lootok*

In this session the presenters will share the secret behind their risk assessment that helped to secure funding from executives. If you've experienced difficulty making the transition from your BIA's to a business case, this session is for you. The end result of the four-stage process is a risk-focused analysis that gives your leaders the necessary information to justify their involvement and investment of resources.

### **D7: Measuring Preparedness and Predicting Recoverability Using Metrics and Maturity Models**

*Sudhir Gadepalli, Enterprise Resiliency Services*

This presentation will provide an overview of the "Enterprise Resiliency Planning Reference Model" and use the "Enterprise Resiliency Planning Maturity Model" to outline a new approach to measuring BCDR preparedness and predicting the likelihood of success. Traditional BC & DR metrics and reporting models tend to focus on measuring compliance with existing BC & DR plans and policies. Relevant BCDR metrics are often reported "after the fact" – for example, the number of plans for each business process/application, the number of plans tested and the outcome of testing, amongst others. This presentation will outline a new methodology to measure enterprise resiliency preparedness and provide stakeholders and executive sponsors a proactive "what can we see in front of the windshield" view rather than "what do we see in the rear view mirror" view.

### **E6: Cyber Resilience – A Comprehensive Approach to Cyber Attack Protection and Response**

*Allan Cyntryn, Risk Masters International*

Cyber Resilience addresses the unique and complex challenges posed by cyber-attack. By incorporating cyber-security, business continuity, disaster recovery, and operational risk management into a common response framework, it provides a unique comprehensive solution to the problems of securing your infrastructure from cyber attack, mitigating the risks, and maximizing your ability to overcome the threats and consequences.

### **F3: The FIS Global BCMS – Centralizing a Global Program for Certification**

*Jim Nelson, Business Continuity Services*

Learn from an FIS BC Professional and an ISO 22301 Lead Auditor as they tell the certification story from the point of view of the company and the third-party certification body auditor. FIS has a global business continuity program. Learn how they took a decentralized program and built a global business continuity management system that has obtained ISO 22301 certification. Case study will include lessons learned from FIS in centralizing the BCMS globally, managing the global certification process, and demonstrating continual improvement. The case study will also include the perspective of the third-party certification body auditor on what is looked for during a certification audit.

**10:15 a.m. to 11:15 a.m.**

**Breakout Sessions**

### **C13: Innovations in Business Continuity Planning**

*Mark Armour, Brinks, Inc.*

Business Continuity should be considered more than just a series of sequential steps. There are ways of better preparing organizations for disruption that don't follow the traditional, linear path. From exercising first to building ground support, your colleagues are blazing trails you may not even be aware of. Even if you have been exposed to many of these concepts there is bound to be something new to learn here. Whether you are new to the field and looking for a wide spectrum of ideas or you've been doing this for a while and want to kick your program out of autopilot, come to this session and find out what others have been doing that you may not have been aware of.

### **D8: Third-Party BC Assessment**

*Victoria Kagler, T. Rowe Price*

In a time of static budgets, the need to perform extensive assessments of vendor's BC/DR capabilities has stretched BC staffs to the limit. The typical BC due diligence questionnaire is bloated with ineffectual and redundant questions that ultimately fail to provide the information your staff needs to properly perform an assessment. Furthermore, Programs need an internal mechanism to understand the context of the vendor's impact to the firm. Learn how T. Rowe Price's BC Program worked with their Vendor Management Office to institute a concise, smart set of questions that provide the basis of an effective vendor BC/DR assessment.

### **D9: Outside the Box Thinking – Data Driven Decision Engine**

*Scott Staiton and Mitesh Shetty, Deloitte*

Risk assessments and business impact analysis often provide static information that does not provide insight into unfolding events. More valuable insights can be brought to bear when we bring a richer set of data together which also provides a common operating picture to drive decisions during a crisis. By leveraging external threat data with internal information systems – clients can make more informed decisions based on richer and more timely information. By synthesizing the data into a visual format that summarizes the organization's recovery status, executives can make the rapid decisions needed to effectively respond to catastrophic events.

### **E7: In a Hybrid World, Automating Discovery of IT Assets Is Essential to IT Projects, Both Large and Small. Can Your Current Tools Keep Up?**

*James Leclair, IBM Resiliency Services*

Experience has shown that client inventories of IT assets are generally 70-90 % accurate. But planning an IT project, such as a data center migration, requires an airtight inventory management approach with repeatable and reliable methods to discover elements of enterprise IT infrastructure. Join this session to learn about new approaches to IT discovery that can equip your organization with the comprehensive understanding of your IT environment needed to seamlessly execute a migration that can help reduce your costs, mitigate risks, and significantly improve your resiliency posture.



#### **G4: Business Resiliency Tool Insides and Outs**

*Tyrone Clark, CNA Insurance*

Attend this where an expert panel would answer questions on business recovery program lifecycles. This vendor-neutral presentation will focus on best practices and lessons learned, as it addresses:

- Program commitment
- Sourcing engagement
- Stakeholder awareness
- Implementation
- Go-Live
- Post-Implementation/Enhancements

**1:00 p.m. to 2:00 p.m.**

**Breakout Sessions**

#### **B5: Preparing for the Worst: Cyber Terrorism and the Human Impact**

*Terri Howard, FEI Behavioral Health*

The phenomenon of cyber terrorism and cyber-attacks is one that businesses continue to underestimate. A cyber-attack does not just mean a blow to the bottom line; it is a traumatic and fear-inducing experience that directly impacts its victims through stolen identities and exploitation of private information. The threat of attack is constant, and businesses must be prepared to protect themselves, their workforces and their clients. The question for employers is no longer "Will I be a target?" but rather "When?" Join us as we discuss the long-lasting and traumatic impact of cyber-attacks on employees, customers, and businesses.

#### **B6: How to Gain Value from Public Private Partnerships to a BCM Program**

*Christopher Sarcletti, BMO Harris*

A great way to expand and enhance your business continuity management program is through engagement with Public Private Partnerships. This presentation will walk you through the key steps involved in engaging with public private partnerships in your area. Additionally, the presentation will include specific details regarding demonstrated real world success that numerous companies have achieved by partnering with Public Private partnerships. BMO Harris Bank has had great success engaging with public private partnerships, including ChicagoFirst and BRPA. We will define what such partnerships entail and discuss our own success, offering tips and best practices we have learned. You will gain a better understanding of the different types of meetings and collaboration opportunities that are available as part of continuous engagement with public private partnerships.

#### **B7: 21<sup>st</sup> Century Technology for Shared Global Resilience**

*Pete O'Dell, Swan Island Networks*

Disasters have always been local. We're moving away from that on the fringes, and remote disaster support will become far more mainstream as the governance and best practices catch up with the technology, eventually moving to a globally shared resilience capability. The list of new options will continue to grow as the IOT, drones, new micro-grid technology, and many other revolutionary technologies become integrated into the toolbox of the people responding to disasters, and those people integrated across silos instead of being ignorant to anything outside their jurisdiction.

#### **C14: Business Resiliency Health Index Implementation**

*Jeremy Adkins and Neeta Adkar, Lockheed Martin*

Evaluating business resiliency posture, highlighting areas of progress or regression, and objectively comparing results across business areas are some of the keys to identifying opportunities to improve preparedness. Lockheed Martin has developed and implemented a model that provides the ability for each of its business areas to self-assess the health of crisis management, business continuity, IT disaster recovery and medical response activities. This presentation will focus on an overview of the project, information about the structure of the model, and how the results are shared.

#### **D10: Let's Measure Our Capability to Recover!**

*Michael Harding, Automotive Resources International*

This session will provide the audience with a real-world method that the presenter implemented to measure business unit recoverability in our organization. It has helped provide senior management with a solid understanding of our capabilities to recover business operations. After you collect the Business Impact Analysis requirements and document the strategies in the Business Continuity plan, it is extremely helpful to understand whether adequate components will be readily available following a disruption to ensure the department can recover within the Recovery Time Objective. The takeaways of the session will include being able to implement a similar measurement within their own environment.

**2:15 p.m. to 3:15 p.m.**

**Plenary Session**

#### **P3: When Doing the Right Thing is the Right Thing to Do: Models of Good Contingency Management Leadership**

*Robert C. Chandler, Ph.D., Professor of Communication, Lipscomb University*

Leadership is the most influential and critical element of successfully managing a contingency or crisis. Despite this seemingly obvious fact – many executives and managers remain ill prepared to function as good leaders during these urgent situations. This session calls our attention to those who choose to do the right things even at the most difficult times. The presentation briefly reviews the marks and traits of positive leadership which apply at the executive level down through localized managers. Several mini-case studies are reviewed that illustrate positive leadership by a focus on doing the right thing despite the challenges of the situation or crisis to be managed.

**3:15 p.m. – CONFERENCE ADJOURNS**

Register for the **2017 Continuity Insights Management Conference** at [www.CIManagementConference.com](http://www.CIManagementConference.com).