ACP

ASSOCIATION OF CONTINUITY PROFESSIONALS

North Texas Chapter

April 2019
Newsletter

Our Mission: Everything we do professionally and as an organization is dedicated to protecting lives, safeguarding businesses, and fostering

President's Comments

Greetings North Texas Chapter Members.

Isn't it great to have spring arrive again? The only exception to the greatness is hailstones from North Texas spring showers. My purple and yellow pansies are blooming and beaming their cute little faces. My dog is back on track now that the time is back on daylight savings time. His hunger pangs never did get on normal time since November! I'll take spring for a while before the heat of summer arrives.

I have some exciting news to share! I have been chosen for a new role as the IT Risk Manager for my business unit at Raytheon! There is a downside however; it means I will be transitioning out of my current IT continuity position and my involvement with ACP. While I've functionally served as the risk manager for a number of years, there was not much traction in the area of risk management. Of course, continuity is closely related, since managing risk as continuity reduces a company's risk exposure.

There are two frameworks we're looking to facilitate:
      1) a sound IT risk management program – COBIT (Control Objectives for Information Technology)
      2) FAIR (Factory Analysis of Information Risk).

It's likely you've heard of one or both of these frameworks. I recommend to those of you in the IT continuity discipline to review the process (with 8 practices) in COBIT *DSS04 Manage Continuity,* and do a quick maturity assessment of your program. I would bet most of your companies have an ISACA license to pull the Practice-Process-Activities for DSS04.

FAIR has a fresh way of looking at IT Security and Operational risk. If you are unfamiliar with the framework, you can learn more at http://fairinstitute.org/. The model is about 10 years old and the fair institute is a young 3 years old. FAIR is changing the way risk analyses are performed. The FAIR Institute is working with NIST to require the use the FAIR risk analytic framework as the default for identifying cyber risks.

One of the books recommended by the FAIR Institute is THINKING, FAST and SLOW by Daniel Kahneman. This book should be required reading for anyone in a continuity discipline as it explains the mechanics of the brain when it comes to rating/ranking risk. You know, the simple quick High, Medium, or Low. Many cognitive studies have explained the errors in judgement with "feelings", "biases", and "influences" which take away from systematic rationalization. There are distinctive patterns and predictable biases in judgements that permeate our decision-making. EVERYONE'S DECISION making, that is, if you're human. I'm only about half way through the book and I sure hope Daniel Kahneman will provide some techniques for ferreting out bad judgements. While he didn't really call it a technique, he did recommend to discuss the set of assumptions someone made on ranking it 'high' or 'very likely.' Then a discussion can occur to determine if the rank is really from more than one person's quick judgement.

The next book in my reading queue is How to Measure Anything, Finding the Value of "Intangibles" in Business by Douglas W. Hubbard. Just reading the back cover of this book highlighting the contents makes me want to read it. It's a marvelous tutorial on how to define sound metrics to justify and manage complex programs. Darn, could someone add at least an hour to every day so I have more time to read?

Wishing you a superb April.
At your service, Wendy

Program Updates by Chet Bojarski

We greatly appreciated the presentation in March that featured our own **Mr. Luis Tapia**, CBCP. Luis provided our members with a unique presentation that covered "Business continuity and crisis management considerations from the Oct. 1, 2017 shooting in Las Vegas". Over and above the content that drove many questions and follow-ups, it gave all of us an insider's look into the incident we remember seeing on the news. Special thanks to Luis for his time and talents, along with **Fannie Mae** who both hosted our March ACP meeting in their conference center and also provided us a great lunch.

I mentioned the After Action Report produced by FEMA on the Las Vegas Shooting. That can be found here: https://www.hsdl.org/?abstract&did=814668

Looking ahead to April 2nd, (remember we head to a different location for this month). We are happy to be hosted by:

SIRIUS Computer Solutions
12801 North Central Expressway #300
Dallas, TX 75243 (near 75 & 635)

SIRIUS Computer Solutions (**Mr. Tony Tomasi**) will be both hosting and providing lunch for those who register in advance for the session (please update your RSVP if your plans change as we use the RSVP to order lunch, and we do not want to ask any lunch sponsor to over spend). When you arrive, staff and signage will be in the lobby to direct you to our conference room on the 1st floor.

At our April ACP North Texas Chapter meeting, we are pleased to announce our guest speaker will be **Special Agent Laird Hightower** of the Dallas FBI Domestic Terrorism Unit. He will be presenting on "Active Shooter Emergency Action Planning for Critical Incident Leadership". We are privileged to have the FBI join our ACP – North Texas monthly meeting to both present and share their knowledge with our members. We continue our commitment to expand our members experiences and industry contacts throughout our region. We look forward to seeing you on Tuesday April 2nd.

North Texas ACP Chapter Meetings

Meetings are generally held the first Tuesday of every month from 12:00 noon to 2:00 pm. The location varies, so check the Chapter Newsletter or Website for location information. If you have a topic you would like discussed or presented, please contact any of our board members (Sidebar on page 3).

Next Meeting

Date	April 2, 2019
Time	12:00 pm – 2:00 pm
Location	Sirius Computer Solutions
	12801 North Central Expressway #300
	Dallas, TX 75243 Map
Lunch	Sponsored by Sirius Computer Solutions

Agenda

Call to Order/Welcome	Wendy Nelson
Upcoming Events	Wendy Nelson
Featured Speaker	FBI Special Agent Laird Hightower
Program	Active Shooter Emergency Action Planning for Critical Incident Leadership

ACP News

As Cybersecurity Challenges Climb, Can Training Lower Risk?

by Zvi Guterman on March 14, 2019 (located on Security Boulevard website)

The right training for employees can have a huge impact on a company's security posture

In 2017, a study by analysts at Enterprise Strategy Group (ESG) noted more than a quarter of cybersecurity pros felt a skills shortage was having a significant impact on their organizations. By the end of that same year, additional ESG/ISAA research put the figure at 70 percent.

That's a dramatic rise, but it's just one example of how threats are increasingly impacting businesses. Breaches lead to costly downtime, damaged reputations, fines, lost customers and partners. According to Ponemon Institute's "2018 Cost of a Data Breach Study," the average financial toll of a breach to an organization is $3.86 million. That is also a figure that has climbed, growing 6.4 percent since last year. For some companies, such a setback is not just damaging, it could mean the end.

By 2021 there will be an estimated 3.5 million unfilled security positions. This has made training of IT staff crucial, not just for staying up-to-speed on emerging threats, but for enabling fewer personnel to do more. But it's not just IT that needs educating. In Ponemon Institute's report, "Managing Insider Risk through Training & Culture," 66 percent felt employees were the weakest link in security.

All employees, to varying degrees, need some type of security training. Unfortunately, the ESG/ISAA study points out that 62 percent of organizations fail to provide the training needed to keep up with business and IT risks.

The following tips can help chief information security officers (CISOs), IT leaders and top executives understand risks and fortify their company's security position, particularly with security training.

Get Everyone Onboard

It's widely felt that training is one of the most cost-effective ways to mitigate security risks. In fact, in the 2018 Ponemon study, 22 meaningful factors that decrease or increase the expense of a data breach were identified. The third best way to decrease costs was training, only behind an organization's incident response team and use of encryption, and tied with business continuity management. Read More

BCI News

Adam's Law? Vulnerability to disruption increases with development

By Paul Barry-Walsh
Chairman of Fortress Availability Services Ltd

There is a characteristic which is self-evident to the professionals in this field, that is, as we develop as a Society, we become increasingly reliant on more and more suppliers delivering products or services. Should just one component of the supply chain be disrupted then this service or product cannot be delivered. This can result in chaos. This is simply a manifestation of Adam Smith's contention that the increased division of labour allows increasing output. However, with ever more suppliers, and the implementation of just in time production, the loss of just one small component disrupts the entire chain. This is as true for services as it is for manufacturing and after Adam Smith we should perhaps refer to this as Adam's Law.

To illustrate this, imagine yourself to be a Venetian banker in the 16th century. He would need ledges quills and ink say possibly a desk and to operate in a secure environment, under the rule of law, but that's about it. Now consider his modern counterpart. Just providing the most basic of modern day services the Banker needs to operate both within and under the rule of law, he needs sophisticated computers, he needs a base to operate from, he needs communication devices and he needs an army of people to run this, accountants, data entry, lawyers, compliance people and then HR to manage them.

That's a complex web of people and products just to do the simplest banking operation. This complexity brings with it vulnerability; if they are denied access to the office, if there is no electricity, (or water) then the organisation cannot function. If you cannot function, there will be a knock-on effect for the counterparties, due to the interconnectedness of our society. If just one bank fails, this has a domino effect on other financial institutions and counterparties.

So, how on earth, given this hugely complex environment, can we assure continuity of service?

The answer is firewalls. Firewalls, not in the IT professional's sense, but rather used in their original sense, to stop fires spreading to other parts of a building. Whilst we cannot stop disasters, we can, through planning and risk assessment reduce the chance of them happening. What we need to do is insert a firebreak, preventing a disaster spreading from one institution to another. [Read more](#)

2019 MEETING SCHEDULE

Schedule and Locations are Subject to Change!

Date	Location
May 7	Toyota North American Headquarters, Plano
June 4	Boy Scouts of America, Irving
July 9	Boy Scouts of America, Irving
August 6	Boy Scouts of America, Irving
September 10	Site Visit (TBD)
October 1	Federal Reserve Bank, Dallas
November 1	Mary Kay Headquarters, Addison
December 3	Maggiano's Little Italy (Willow Bend), Plano

Check here for most current topic, speaker, and meeting location updates

Please contact a board member if there is a topic that you would like discussed, if interested in presenting, or know of others who would be willing to present an upcoming meeting.

DRJ Article

An Introduction to Adaptive Business Continuity

by Mark Armour on February 6, 2019

If you have been in the business continuity profession for any length of time, then you are certainly familiar with the laundry list of standards that already exist. This includes BCI's Good Practice Guidelines, ISO 22301, and NFPA 1600, to name a few. If you have familiarized yourself with the guidance of these standards, you probably also know they are all predicated on the same basic methodology. They all define the same sets of deliverables. Also, they all have the same means of measuring the effectiveness of an organization's business continuity program: its conformity to these same standards.

There is a new kid on the block that is challenging traditional perceptions of business continuity and shattering assumptions about how best to be effective in this discipline. This method is called adaptive business continuity (or merely "adaptive" from this point forward). Adaptive lays out an entirely new approach to the profession; an approach which is simple, straightforward and delivers significantly better value. Most importantly, one of the key components actually defines a means by which to determine the ability of an entity to recover following a disruption. Using this model, the principles can be applied to discern the specific actions that can improve an organization's recovery capabilities. Ongoing measurement and improvement provide long-term benefits while delivering value, all for considerably less effort than following traditional methodologies.

The Adaptive Business Continuity Manifesto

The original manifesto, published in September 2015, outlined a set of principles applicable to business continuity practices. While the document is a rather brief 15 pages, including a summary matrix and postscript, it covers a lot of territory. This starts with a new definition of business continuity and justifies the need for radical new approaches to the discipline. It then goes on to firmly establish the scope of the business continuity practice before providing a detailed list of its 10 principles.

Read more Need to log-in to DRJ to read article.

TRAINING OPPORTUNITIES

Upcoming Conferences

Resilience Day with South Texas ACP
April 18, 2019 – Texas Medical Center Innovative Institute, Houston, TX
Approx. $100 (Free to ACP Members—Promo Code: WeSaluteTheLoneStarState) Conference Link

Continuity Insights Management Conference 2019
April 15-17, 2019 – Hilton New Orleans Riverside, New Orleans, LA
Approx. $1595 ($100 ACP Discount—Promo Code: ACP)
Conference Link

Business Resilience Conference
April 25, 2019 – Grand Hyatt DFW, Dallas, TX 75261
Approx. $795 Conference link

RIMS2019
April 28-May 1, 2019 – Boston, MA
Approx. $1165 (Certified Individual Discount)
Conference link

Gartner Security & Risk Management Summit 2019
June 17-20, 2019 – National Harbor, MD
Approx. $3350 ($350 Discount until 4/19/19)
Conference link

DRJ Fall 2019
September 29-October 2, 2019 – Phoenix, AZ
Approx. $1395 Conference link

Local Certification Classes

DRI
ABCP Certification Class - BCLE 2000 Dallas 7/15/19 – 7/19/2019, $2750 Does not include lodging/transportation. Class link
ACRP Certification Class - CRLE 2000 Dallas 12/9/2019 to 12/13/2019, $2750 Does not include lodging/transportation. Class link

BCI
CBCI Certification Course
No local classes scheduled for 2019
Class listings

Ongoing Webinars

Federal Government
Webinar link Held on the **1st Wednesday of every month at 1 P.M. Central Time.**
ACP International
Webinar link Held monthly. Check website for details.

Firestorm
Webinar link Held monthly. Check website for details, scroll down and look under Events
Bright Talk
Webinar link Random scheduling.

Courses Beyond Conferences/Webinars

Business Continuity Institute www.thebci.org

Disaster Recovery Institute International www.drii.org

InfraGard (Partnership between FBI and Public Sector www.infragard.org

TEEX www.teex.org

ISO Based Training Website link

National Initiative for Cybersecurity Careers and Studies (NICCS) Training More info

Here are a more ways to find out what we have planned:

Our web site: http://northtx.acp-international.com

Join our LinkedIn Group for the latest updates