­­

|  |  |
| --- | --- |
| **AGENDA** | **ATTENDEES** |
| 1. Call to Order President 2. Welcome/Announcements President 3. Program Speaker 4. Wrap Up Board 5. Meeting Close President | **BOARD MEMBERS**:  Membership – Joanne Storbeck  Web Resources Director – Monique Hafler  Absent:  President\* – Ed Simko - Absent  Treasurer\* – Susan Czarnowski - Absent  Information Director – Grainne McClorey-Mitchell - Absent  President Elect – ***Open***  Secretary\* – Jill Titzer - Absent  Public Relations Director – Keith Berthiaume - Absent  Past President – Cheri Umlauf - Absent  Program Director – Liz Brainard - Absent  \*Executive Committee |

| **Discussion Threads** | |
| --- | --- |
| Call to Order | * + While Joanne worked with Early Warning to get the chapter slides up and running, Monique opened the meeting at 9:02AM. She apologized for the difficulty and explained that she and Joanne would be tag teaming to run the meeting. Not in your typical order of events, Monique welcomed attendees. Talked about the next meeting following DRJ, November being a virtual meeting and the December appreciation luncheon. She explained there would not be 50/50 since there were no tickets. Joanne had attendees introduce themselves and asked who was attending the DRJ conference by a show of hands. Monique reminded folks that the website has different information than the newsletter so encouraged all to visit it. A member mentioned that 2020 Board elections are coming up. Monique stated all positions except Past President are open. Joanne encouraged anyone interested to contact a Board member via email. |
| Local Sponsors | * Fusion Risk Management * BC in the Cloud |
| Meeting Host | * Host: Early Warning. Art MacFarland from Early Warning welcomed all and provided the customary logistics. Debbie DeVries gave an overview of Early Warning. It is owned by several large banks and is best known for its Zelle Network, a first time payment service. Early Warning has about 1,000 employees and her team is responsible for BCM, DR, Risk and Crisis Management. * Breakfast sponsor: Early Warning. |
| Welcome | * Meeting Attendance-   + Guests – 8   + Central Arizona Members – 6   + Member-at-Large - 1   + Total- including speaker 15 |
| Reports from your Board of Director | * Due to the absence of all directors except Membership and Web, there were no reports. * President\* – Ed Simko - Absent * Secretary\* – Jill Titzer - Absent * Treasurer\* – Susan Czarnowski - Absent * Information Director – Grainne McClorey-Mitchell - Absent * Membership – Joanne Storbeck * President Elect – Vacant * Program Director – Liz Brainard - Absent * Public Relations Director – Keith Berthiaume - Absent * Web Resources Director – Monique Hafler * Past President – Cheri Umlauf - Absent   \*Executive Committee |
| Get Connected | * National’s site   + [www.acp-international.com](http://www.acp-international.com)   + Has a lot of good information and webinars * AZ’s site   + <http://chapters.acp-international.com/centralarizona> * LinkedIn   + Arizona ACP Chapter * Continuity Counts newsletter * Arizona Chapter Email address   + [Arizona@acp-chapters.com](mailto:Arizona@acp-chapters.com) |
| Today’s Event | Speaker: Mike Burg is the Director of Strategic Advisory at security services firm Alagen and contributing author to “IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data.” With over 20 years of security experience, he has served as acting CISO across several industries including medical, financial, and transportation.  Breaches, Distributed Denial of Service (DDoS) attacks, and unexpected IT outages are common. Worse yet, they not only impact business operations, but also can cause lasting and costly damage to reputation and bottom line. It's increasingly critical that organizations appropriately assess and account for this difficult-to-quantify risk. Mike Burg, Director of Strategic Advisory for security services firm Alagen, shares an approach that not only supports better structure, reporting, and analysis of cybersecurity risks to business continuity, but also contributes to a culture that positions executive leadership to more efficiently prioritize and address all enterprise risks.  Mike discussed:   * What is enterprise risk management (ERM) * Why incorporating cybersecurity risk is important * Best practices for assessing cybersecurity and other risks * How to measure cybersecurity risk * How to quantify the risk to business operations   ERM runs across the full organization. Risk components are Financial, Employee, Litigation, Economic, Regulatory, Strategic, Operational that generally includes IT/Cybersecurity Risk, and Reputational, which is hard to quantify since it is often so large. Each has their own components and compliance playbook.  Top 20 Risks for 2019:  1. Existing operations meeting performance expectations, competing  against “born-digital” firms.  2. Succession challenges and ability to attract and retain top talent.  3. Regulatory changes and regulatory scrutiny.  4. Cyber threats.  5. Resistance to change operations.  6. Rapid speed of disruptive innovations and new technologies.  7. Privacy/identity management and information security.  8. Inability to use analytics and big data.  9. Organization’s culture may not sufficiently encourage timely identification and escalation of risk issues.  10.Sustaining customer loyalty and retention  *Source: Executive Perspectives on Top Risks 2019, Protiviti and North Carolina State University Poole College of*  *Management’s ERM Initiative*  He referred to CIS 20, a set of security (20) controls, which Mike stated the top 6 are mandatory for a successful cybersecurity program. They are collaborative, and provide the framework for easy to understand and prescriptive controls. #2 risk issue is there is not much cybersecurity talent available, Crooks are staying ahead of controls put in place for cyber threats. #8 haven’t figured out how to collect and move it forward. Mike stated it would be nice if companies could make decisions, strategies, etc. to figure out how to make a Really Secure Company, (1% likelihood of breach in next 5 years) and if Money Went To Marketing Company  (30% likelihood of breach )in next 5 years. The challenge is Cybersecurity risks are notoriously hard to quantify  Breaches: Not if, but *when* Average cost of a breach is $148 per capita. Challenge is Doom and Gloom. How do business’ stay in business with these controls.  Two types of analysis – Qualitative (Supports quantitative facts, Useful as guideposts, Accurately describes situation (human factor) and Quantitative (Tells part of the story, Difficult to identify, Devil is in the details of assumptions.) You need to have both. One is not better than the other. Impact and likelihood are most important, the rest just fall in to place.  Risk Appetite – For companies with zero tolerance, they will probably go out of business. A member commented that if people were looking at silos but not looking at all the risk appetite factors, they have to be looked at as one component.  The ERM processes is generally what’s used. Not many companies go into the How. Mike is a big fan of the ISO standards and follows the Deming model of Plan-Do-Check-Act and repeat.  A team approach is better as more than one head is better – but be careful to not have too many people. Causes arguments. Address as many silos as possible using repeatable steps.  Different Flavors of Classifications – slide  Threat Modeling is a good way to help numerate risk factors. Put them into real-life scenarios to give context.  Preventative and Detective controls are typically for the technical factors.  Consensus – Everyone looks at it.  Auditors want to look at these. Use scenarios to rate controls. Verizon reports looks at different companies and breaks into categories and looks at them to develop scenarios. You can begin to breakdown and look at controls. Live within real-life scenarios and address the issues. Can concretely measure. Mike aims to bring in at least ¾ of them. Then add them to your incident response plans.  Quantifying is an Art. We tend to assume controls are in place. Need to start at ground zero for effectiveness. Look at them as binary – Yes or No questions on risk. There is a variety of ways of determining security posture. Determined usually be the Risk Committee.  Understand the likelihood and impact. Look at the model and identify how often it happens. Investigate it. Identify the potential impact.  Ratings – fully document assumptions to get away from disagreements on how to rate.  Communication and reporting – Very important. Do ongoing Risk monitoring. Committee best idea. Use the Deming model. Need to understand how the company is doing overall and where do we go from there.  “Risk – Love it, Want to Measure it. Want to Get Rid of it” Mike Burg  In summary, assess mechanisms to measure, report, communicate and train users.  Take different views of risks. Use Scenarios. People understand them vs. making it technical. Qualify and Quantify. Document assumptions.  Contact info:  Mike Burg, Director of Strategic Advisory  [Mike.burg@alagen.com](mailto:Mike.burg@alagen.com)  Questions/Comments:  Q – How are costs derived? Slide  A – Poneman and Verizon reports.  Q- Does the cost of secondary loss really matter?   1. It talks more to if a company has a breach. In general, cost is not representative of each company. There are better views than the secondary cost. They would be mitigated after resolving the breach.   Q – Probability of plugging in to a risk? What is that based on?  A – Combination of indicators like the IT help desk and the subject matter expertise. What’s reasonable? Consider Accuracy vs. Precision based on the data.  Q – Have you read Douglas Hubbard?  A – Yes, he uses Monte Carlo to run scenarios with variables and how to measure things. Also Jack Jones with the Fair Institute. “Those concepts make your eyes glass over.”  Q – ISO vs. COSO (Committee of Sponsoring Organizations). Which fits cyber security better?  A – From a cyber-perspective, ISO 31000 is better as it is non-prescriptive. Both fit. Both state to “do this” and document it.  Q – Is Audit on the team or on the outside?  A – Audit is usually seen as outside of the risk team and is invited in when needed. They may have different perspective and are generally the ones making the recommendations. |
| Next Meeting | Date:  **October 2, 2019 – Following the end of the DRJ conference, 1-3pm**  Location:  **JW Marriott, Desert Ridge Resort**  Speaker: TBA  Topic:TBA |
| Program Outlook |  |
| Events | * DRJ conference, Sept 30-Oct 3, Desert Ridge JW Marriott, Scottsdale * October AZ ACP Meeting October 3 following DRJ conference * December Member Appreciation luncheon, December 5, 11-1pm, Desert Willow Conference Center, John Iannerali speaking |
| Wrap Up | * Steve O’Neal with Agility asked what topics attendees were interested in since he is the November speaker. He also said he had invited Deb Roepke to attend and suggested our chapter get with her to do something with the Coyote Crisis group. Steve also asked about our membership with Infraguard. I told him some ACP members belonged and that is has been several years since we had a joint meeting with them. |
| Adjourn | Meeting adjourned at 10:40 am |