Salve Regina University Pell Center and OSHEAN
RI Cybersecurity Exchange Day
Wednesday, March 13th, 2019 - 9AM-3PM
O'Hare Academic Building
Salve Regina University, Newport, RI
#CybersecurityExchangeDay19

9:00am – 9:30am

Breakfast and Registration and Opening Remarks

9:35am - 10:00am

Opening Remarks

Speaker*:* Dr. James Ludes, Ph.D., VP for Public Research and Initiatives and Executive Director, Pell Center, Salve Regina University

Speaker*:* Dave Marble, President and CEO, OSHEAN

10:05am - 10:40am

Keynote Speaker Presentation I

Speaker*:* Paul Asadoorian, Founder & CTO, Security Weekly

Topic*:* Security Isn't Doomed If We Learn From the Past

Presentation Description: Many of us in security today encounter what we believe are new problems and attempts to come up with brand new solutions. While the threat landscape and how we implement IT systems has evolved, several older tactics and techniques still apply today. In fact, many of the new buzzwords trace their roots back to concepts developed many years ago. In this presentation, we'll discuss how threat hunting is not a new concept (and still very effective). We'll take a look at Paul's enchanting quadrants for network security and how it applies to your security architecture. Finally, we'll look at processes developed years ago, such as OODA loops, and how it can help your security teams be more effective at defending enterprise networks.

10:45am – 11:20am

Keynote Speaker Presentation II

Speaker*:* Dr. Chris Demchak, Ph.D., Professor and RDML Grace Hopper Chair of Cyber Security, United States Naval War College

Topic*:* Defending Whole Nations in the Hostile Rising Global Cybered World: Scale Up, Buy Time, Transform Tech

Presentation Description*:* The scale of the rising authoritarian-led world threatens to overwhelm the cyber defenses of the modern westernized democracies, with an ambitious, cyber competent, determined China at the helm. Civil societies now need a collective effective shared cyber defense of their private as well as public sectors as a way to prevent irremediable hollowing of their economies and stability. This collective response is critically needed to integrate the telecommunications and IT capital goods sectors with public defense assets across allied states in order to buy time for this minority community of societies to adapt to the new global circumstances. In particular, the time allows the democracies to transform their shared shoddy cyberspace into a technologically advanced, securable, generative, allied substrate with democratic values to assure their long-term wellbeing and security.

11:25am – 11:30am

BREAK

11:30am – 12:00pm

Breakout Session I

Speaker: Francesca Spidalieri, Senior Fellow for Cyber Leadership, Pell Center, Salve Regina University

Topic: A Practical Approach to Managing and Reducing Cyber Risks

Presentation Description: Cyber risk is an underrated but all too real threat to organizations of every size, industry, and sector. Whatever your place of business, creating a culture of cybersecurity is an essential shared responsibility among leadership and all employees. Organizations must view cybersecurity as an enterprise-wide risk issue and devise plans for employee education, training, and awareness that emphasize risk management, security, and resilience. This session will provide an overview of both the opportunities and threats of doing business online, discuss compliance and regulatory issues, and address different approaches to improve the overall security posture of any organization operating in the digital age.

Speaker: Jesse Roberts, Professor, Security and Network Engineering, New England Institute of Technology

Topic: Dealing with DOS (Denial of Service Attack)

Presentation Description: Participants will be able to see the effects of a DOS attack on a web server. They will then take steps to mitigate the attack. All of this will be done in a simulated environment using RI State Police Cyber Range.

Speaker: Tamara Elliott, Account Executive, Duo Security

Topic: Trust Not, Fear Not (Multi-Factor Authentication)

Presentation Description: When terms like "Zero-Trust" and "Secure Endpoint Policy" get introduced to public organizations, sometimes panic ensues. It's easy for security professionals to understand the importance of Multi Factor Authentication (and other common security practices), but the thought of introducing technologies that require change from end users can sometimes be scarier than the thought of a breach itself. In this session, we'll cover common myths and misperceptions about modern security efforts- and ease concerns about angry mobs forming outside your office. Whether you fear faculty or first-responders, you'll leave with practical strategies to help find that ever-elusive balance between security and usability.

Speaker: Jeff Bain, Solutions Engineer, OSHEAN

Topic: Cyber Security Capture the Flag Series

Presentation Description*:* During this session (which will be run from breakout session I thru breakout session III), participants will compete in a Q&A style format Capture the Flag competition. The goal of this CTF exercise is to show IT generalist how to secure your organizations environments. All levels in IT are invited to compete.

**A pre-registration link will be provided in advance to the event.*
*Top two players will compete in the final round, during closing remarks, in the main auditorium**

12:00pm - 1:00pm

LUNCH

1:05pm – 1:35pm

Breakout Session II

Speaker: Brian Lamoureux, Esq., Partner, Pannone Lopes Devereaux & O’Gara, LLC, Practitioner Faculty, Providence College

Topic: Big Tech and Big Tobacco: Is History Repeating Itself?

Presentation Description*:* Are smartphones the new smoking? Is Big Tech anything like Big Tobacco, but in sleeker packaging? This session will explore some of the parallels and key differences between Big Tech and Big Tobacco through the lens of marketing, social impact, and provide some food for thought on the impacts that social and digital media are having on us.

Speaker: Jesse Roberts, Professor, Security and Network Engineering, New England Institute of Technology

Topic: Dealing with DOS (Denial of Service Attack)

Presentation Description: Participants will be able to see the effects of a DOS attack on a web server. They will then take steps to mitigate the attack. All of this will be done in a simulated environment using RI State Police Cyber Range.

Speaker: Craig Sandman, President and Co-Founder, Symbol Security

Topic: Phishing and the Disruption in Traditional Cyber Security

Presentation Description*:* Traditional IT Security and Cyber Security practices are predicated on prevention. Shoring up leaks, holes, potential vulnerabilities…preventing the bad guys from getting in. However, with the pervasion of email and the ease at which Cyber Criminals can leverage email to get direct access to our employees, Cyber Security practices need a new trick. We'll look at how Phishing has emerged and what businesses, hospitals, universities, and all entities can combat this highly successful form of Cyber Crime.

Speaker: Dr. Mark Arnold, Ph.D. Senior Director, Security and Compliance, Navisite

Topic: Vulnerability Wrangling in the Current Threat Landscape

Presentation Description*:* Vulnerabilities have been overwhelming security practitioners for years. Currently an average of 19 CVEs are published every day. The exponential rise in vulnerabilities has scaled at a rate greater than our ability to manage them. As the number of vulnerabilities continues to scale upwards, the task to wrangle them has becomes more complex and difficult possibly at the risk of overlooking important issues - losing them in the noise and chaos. To that end, through collaboration with some of the best vulnerability wranglers in the security community, we have generated content to help us become better vulnerability wranglers and leverage best practices to that end. In this session, we will review perspectives on the current vulnerability landscape and associated risk, understand abstraction, and prioritize remediation. We will examine areas in vulnerability management that give we as wranglers the most angst: vulnerability coverage, the common vulnerabilities and exposures (CVE), the common vulnerability scoring system (CVSS), prioritization, and more. Attendees will learn from insights and mistakes, drawing upon our collective experiences to avoid common pitfalls encountered when wrangling vulnerabilities.

1:40pm – 2:10pm

Breakout Session III

Speaker: Patrick Laverty, Pentester, Rapid7

Topic: Social Engineering Awareness: Explanations and Stories from the Field

Presentation Description*:* Let's talk about social engineering. What is it, what types are there, how can you be more aware of these types and better protect against them. We'll talk about real world examples where we'll see how the psychology works, how confidence and being persistent comes in to play. We'll also look at pretexts that social engineers use and look at why they work. We'll look at phishing, vishing, smishing, and any other types of *ishing that we can think of.

Speaker: Jesse Roberts, Professor, Security and Network Engineering, New England Institute of Technology

Topic: Dealing with DOS (Denial of Service Attack)

Presentation Description: Participants will be able to see the effects of a DOS attack on a web server. They will then take steps to mitigate the attack. All of this will be done in a simulated environment using RI State Police Cyber Range.

Speaker: Todd Knapp, CEO, Envision Technology Advisors

Topic: How the Digital Transformation Mandate Drives Cyber Strategy and Employee Training

Presentation Description: Digital Transformation isn't a choice. It's an unstoppable force of evolution that will touch every aspect of your business, including the people your company is hiring. These new hires include a generation of professionals who have grown up trading privacy for convenience and who communicate and collaborate using a completely new set of tools. This poses a number of challenges for how you train your team members, and for the first time it makes organizational change an imperative if you want to have a comprehensive cybersecurity strategy.

In this session, Envision Technology Advisor's Founder and CEO, Todd Knapp, will discuss how to manage the impact of Digital Transformation initiatives, including new imperatives for collaboration between InfoSec and other areas of IT. Included in this discussion will be a focus on Employee Security Posture Training and how you can develop a curriculum that will bridge generational gaps and help keep your company and your people better protected.

Speaker: Rohit Madhok, Systems Engineer, Palo Alto Networks

Topic: How to Create a Modern Ransomware Strategy

Presentation Description: Government agencies and education institutions are under attack. And ransomware is the weapon of choice. So, phishing prevention and education have become top of mind across the globe. Security teams and organizations are constantly working to upgrade their systems and provide better protection to their networks. However, the 'bad guys' – threat actors, are also constantly developing new techniques. There is an entire dark market associated with the threat landscape that is automated, scalable and profitable. Developing new threats takes time and expense and so those looking to get around network security measures often target the weakest link in the security chain – the user. Join Rohit Madhok, Systems Engineer from Palo Alto Networks to learn about how building a solid prevention strategy, so your organization doesn't become the next Ransomware victim.

2:15pm – 3:00pm

Capture the Flag Game Finals and Closing