Cyber Security and Privacy Research Institute (CSPRI)
presents

# The Journey to Rational Cybersecurity

**Dan Blum**
Security Architects Partners

Thursday October 17, 2019
12:00 noon
SEH-B1220
(An informal lunch will be served)
*Please RSVP to cspri@gwu.edu*

Cybersecurity is in chaos. Despite increased spending, organizations keep exposing known vulnerabilities. Attackers keep penetrating defenses all too easily. Regulations such as the GDPR for privacy and DFARS for Defense contractors' cybersecurity are ratcheting requirements tighter, but compliance doesn't always meaningfully increase security. Despite general agreement that cybersecurity programs need to be better aligned with the business, why do we continue to struggle? What should we do differently?

The intent of this and future Cyber Security and Privacy Research Institute (CSPRI) lunches is to provide glimpses of the vibrant security and privacy private sector in the Washington region to GW faculty and students and to promote dialog and debate regarding breakthrough initiatives. The potential of support for research or conference papers on related topics will be part of the discussion.

**Speaker: Dan Blum**

Security Architects Partners

## The Journey to Rational Cybersecurity

Cybersecurity is in chaos. Despite increased spending, organizations keep exposing known vulnerabilities. Attackers keep penetrating defenses all too easily. Regulations such as the GDPR for privacy and DFARS for Defense contractors' cybersecurity are ratcheting requirements tighter, but compliance doesn't always meaningfully increase security. Despite general agreement that cybersecurity programs need to be better aligned with the business, why do we continue to struggle? What should we do differently?

Please attend our CSPRI lunch event to hear how cybersecurity expert Dan Blum's upcoming book - Rational Cybersecurity for the Business - will address these questions to provide guidance for security leaders and staff on how to:

- Apply the Cybersecurity Pareto Principle (80-20 rule) to the security program
- Identify the optimal security governance structure and drive security culture change in alignment with the business culture
- Coordinate and implement security initiatives with business engagement at the Executive, Line of Business, IT, Development, and End User levels
- Manage risk in the language of the business - use risk to prioritize controls, and use architecture to arrange controls
- Institute resilience, detection, and response to minimize impacts from threats, breaches, and outages
- Scale "best practices" to a business's size, complexity, and security pressure level

## Biography

An internationally-recognized expert in security, privacy, cloud computing and identity management **Dan Blum l**eads and delivers consulting projects spanning multiple industries. Formerly a Golden Quill award-winning VP and Distinguished Analyst at Gartner, he has led or contributed to projects such as: cloud security and privacy assessments, security organization and risk management framework development, and identity management architectures. He's also consulted on technical security engagements in all areas of data protection domains including enterprise authorization, DLP, privileged access management, and encryption/key management.

Mr. Blum holds CISSP and Open FAIR certifications. He is a frequent speaker at industry events and participates in industry groups such as ISACA, FAIR Institute, IDPro, ISSA, CSA, Kantara Initiative, Open ID Foundation, OASIS, and others.

Finally, Mr. Blum is writing the book “Rational Cybersecurity for the Business.” This book is addressed to security leadership and staff requiring guidance on how to coordinate, architect, and implement security initiatives with business engagement at the Executive, Line of Business, IT, Development, and End User levels. As part of the book project, he is in the process of interview over 100 CISOs, Board Members, and other business or security leaders.