



## A Discussion of Risk; CPI Global Summit 2017

06 September 2017 By: Sean Sposito

There's a knee-jerk reaction among bank executives to large security incidents – like the WannaCryptor or SWIFT attacks – in the news. “How do we solve our ransomware problem?” they may ask. Or, “how can we address our data breach issues?”

Without victim blaming, I think the much more important question to ask: What can we all do to lessen the bank's risk?

At the [CPI Global Payment Summit](#) in New York City, next week, I'll moderate a conversation between cybersecurity executives and threat intelligence researchers on the most pressing security issues facing the commercial payments organizations inside FIs.

**Our focus:** To determine how can the vast security teams inside FIs and the non-technical payment executives who want to better understand their customers' and their firm's risk can come closer together. The conversation is high-level and general. The audience will mostly be made up of non-technical executives. **Here are the types of questions I'm hoping we can begin to answer for them:**

- What are the largest systemic issues -- the Internet of Things, think, CCTV cameras, and unencrypted data -- inside FIs that lead to larger security incidents?
- What resources can bankers depend on -- government, industry, or academic -- to gain intelligence on emerging threats? And, does threat intelligence matter in a landscape that's always shifting?
- How do non-technical executives start having conversations about security with their larger teams?
- What kinds of services can nontechnical executives recommend to their clients to cut down on their risk?

**So, what's my ask of you:** Tell me how you, given the audience, think I should frame the discussion?

As always, I'm available over Signal, Wickr, LinkedIn, Twitter (@seansposito), or, yes, email – [Sean.Sposito@javelinstrategy.com](mailto:Sean.Sposito@javelinstrategy.com). I look forward to hearing from you.

---

Copyright ©2020 Escalent and/or its affiliates. All rights reserved. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of Escalent.