The Cybersecurity Readiness Podcast Series

Episode Title	Global Security and Post Breach Management Best Practices
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.dchatte.com/podcast/ https://the-cybersecurity-readi.captivate.fm/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Tim Callahan, Senior Vice President, and Global Chief Information Security Officer, Aflac
Summary Pitch	"If you can plan for the zombie apocalypse, you can probably face just about anything," said Tim Callahan, Senior Vice President, and Global Chief Information Security Officer, Aflac during a talk in my Master's level class on cybersecurity readiness at Duke University. In this podcast, Tim describes the key elements of an effective crisis management framework and shares several best practices. Some of the highlights of a robust business resiliency and recovery posture include -- a) well thought-out and rehearsed plan that takes into consideration different scenarios; b) world-class forensics team; c) strong partnership with Legal, HR, Law Enforcement (local FBI and Secret Service), Department of Treasury, and independent agents; d) highly trained in-house teams focused on response and recovery; e) leveraging open-source and paid intelligence; f) CEO led strong commitment throughout the organization; g) honest and candid communication; h) rewards and incentive programs such as the Global Security Challenge Coin; and j) building a caring and empathetic work culture.

Copyright © 2021 The Cybersecurity Readiness Podcast Series by Dave Chatterjee, Ph.D. All Rights Reserved.

Time Stamps	00:49 -- Please share with listeners some highlights of your professional journey. Share with them how this journey of yours has shaped your views of cybersecurity, and cyber risk management. 05:55 -- So, Tim, during your talk in my Master's level class on cybersecurity readiness at Duke University, you made a very poignant statement, you said, "if you can plan for the zombie apocalypse, you can probably face just about anything." Please share with the listeners the key elements of an effective crisis management framework and related best practices. 11:15 -- As we all know, ransomware attacks are rampant, and many organizations are underprepared to deal with such attacks. Based on your experience, what advice do you have for your peers in other organizations? 17:16 -- It's not good enough to just have backups, and that they're properly secured both offline and online. It is equally important to have read-only backups. Would you like to add anything to that? 19:45 -- Given the variety of ways in which the ransomware attackers put pressure on the organization, and the unfortunate reality, that it is hard to keep up with the evolving attacks and techniques, it must be a very unnerving feeling that if your organization gets attacked, if your organization gets compromised, the battle against the ransomware attackers is hard to win, because they have the data and you have to depend on them live up to their promise that if the ransom is paid, they won't share the stolen data, or they won't do anything more with it. That's a very difficult kind of situation, isn't it? 24:56 -- I'd love to hear your reaction to some of the CPD (Commitment-Preparedness-Discipline) framework success factors. For instance, how does an organization create and sustain a We-Are-In-Together culture? What are some key elements of a best practice to do that?

Copyright © 2021 The Cybersecurity Readiness Podcast Series by Dave Chatterjee, Ph.D. All Rights Reserved.

	34:20 -- I was just speaking with another group before this discussion, and they were talking about how important empathy is when it comes to cybersecurity governance. And I'm sure you will agree that it plays a huge role. Because, unless you're empathetic to people making mistakes, even though they use their good judgment, they trained sincerely, but they can make mistakes. But as long as they're owning up to it, and enabling organizations to react quickly to the consequences of their mistakes, instead of punishing them, be encouraging, and maybe celebrate their candor and honesty. It has been done by some companies. So I'll let you speak to that as well. 38:59 -- We can end on that note unless you have any final thoughts, Tim.
Memorable Tim Callahan Quotes/Statements	"If you plan for the zombie apocalypse, you can handle just about anything." "You can't do a good job in post-recovery if you don't do a good job in the response process, and in those stages leading up to that." "I think it's very important that you exercise with different scenarios before the event happens. And you put yourself in continuous learning and improvement mode. When we generally have our exercise, we bring in third parties, we also call on law enforcement, our intelligence partners, intelligence we paid for, and intelligence through FS-ISAC (Financial Services Information Sharing and Analysis Center). All of these things help us prepare for different attack scenarios." "I mean, when employees enjoy coming to work, or enjoy their workplace, because of empathy, because of humor, because we care, obviously, they're going to do a better job, they're going to feel a sense of ownership to that company. It's not kind of the working in the coal mine attitude, it's, I want to be there, I want to be there. And because I want to be there, I want to protect it." "I think the public and our customers would have a lot of sympathy for a company if we're doing the right thing, we've done the right thing, and we're communicating honestly, openly, and transparently. They'll realize

Copyright © 2021 The Cybersecurity Readiness Podcast Series by Dave Chatterjee, Ph.D. All Rights Reserved.

	and we've seen this in other companies, the customers realize that we're a victim too and we're doing our very best to protect them." "One thing that we do is three or four times a year, we actually host a shred day. So people can bring their personal information that gets piled up in the corner someplace and bring it to the shred they can bring their computer disks, they can bring hard drives, we sponsor that. And we use that opportunity as people bringing things to just reinforce the principles of good sound security."

Copyright © 2021 The Cybersecurity Readiness Podcast Series by Dave Chatterjee, Ph.D. All Rights Reserved.