

The Cybersecurity Readiness Podcast Series

Episode Title	Thinking Like A Hacker
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	Ted Harrington, author of Hackable: How To Do Application Security Right, and Executive Partner at Independent Security Evaluators
Summary Pitch	Using compelling stories and metaphors, Ted Harrington, author of Hackable: How To Do Application Security Right, and Executive Partner at Independent Security Evaluators , explains the process of hacking and the importance of being able to think like a hacker. He encourages leaders to get excited about information security investments and look for ways of gaining a competitive edge from those investments.
Time Stamps	01:59 -- So let's talk about hacking. For the benefit of the listeners, provide an overview of hacking like hacking 101, what is it? What are the many consequences? 04:30 -- Shed some light on why hackers might be interested in breaching the systems of certain types of organizations over others. And related to that, are any organization types more vulnerable than others? 08:18 -- We hear the phrase 'thinking like a hacker' a lot. The ability to think like a hacker is considered a best practice in cybersecurity governance. I'd like to probe a little deeper into it. Can you shed some light on that?

	<p>11:32 -- What are your thoughts and perspectives on the other group, the folks who are not very security savvy and generally get compromised. You would not recommend or expect them to think like a hacker. What advice do you have for them?</p> <p>15:55 -- Maybe we need the media to help popularize thinking like a hacker, so literally everyone on the street has some sense of what these guys are up to, how they are thinking, how they try to attack. Not to suggest that this exposure would make everyone an expert. But at least it whets the appetite, it gives them a basic understanding. And that would help mobilize organization-wide support. Thoughts, reactions?</p> <p>22:09 -- Let's talk about security assessments. It's reasonable to assume that most organizations are engaging in security assessments. But the more nuanced question is, are they engaging in the right kinds of security assessments, with methodologies that best align with their desired outcomes? What are your thoughts?</p> <p>32:40 -- What are you seeing out there in terms of top management commitment to information security?</p> <p>37:37 -- What is so difficult or challenging about patch management, vulnerability management?</p> <p>42:10 -- What lessons do organizations refuse to learn?</p>
<p>Memorable Ted Harrington Quotes/Statements</p>	<p>"The term hacker is neutral. It's neither good nor bad.</p> <p>"A hacker is someone who is a problem solver. They're creative. They're someone who looks at the way a system works and says, you know, can it behave differently than what it was intended to do?"</p> <p>"To defend against an attacker, we need to think like an attacker."</p> <p>"Most people think about security as avoiding a bad thing. Let's not get hacked. That is a good way to think about security, but it's incomplete. We need to think about not just how do we avoid a bad thing, but also how do we get a good thing? Not just how we do not get hacked, but how can we gain an advantage?"</p>

