# The Cybersecurity Readiness Podcast Series

| | |
|---|---|
| **Episode Title** | Building a resilient disaster recovery infrastructure |
| **Podcast Series** | The Cybersecurity Readiness Podcast Series<br><br>https://www.dchatte.com/podcast/<br><br>https://the-cybersecurity-readi.captivate.fm/ |
| **Host and Producer** | Dave Chatterjee, Ph.D.<br><br>https://dchatte.com |
| **Guest** | Sagi Brody, Co-Founder and CTO at Opti9 |
| **Summary Pitch** | The latest disaster recovery statistics reveal that modern businesses still face costly interruptions due to a variety of threats, ranging from ransomware attacks to sudden hardware failures. The monetary costs of disasters and outages can be significant. According to results from Uptime Institute's "Annual Outage Analysis 2023" survey, 25% of respondents reported in 2022 that their latest outage incurred more than $1 million in direct and indirect costs, a consistent upward trend in expenses. In addition, 45% reported that the cost of their most recent outage ranged between $100,000 and $1 million. Another research report reveals that just over half of organizations have disaster recover plans and around 7% of organizations never test their disaster recovery plans. It was a real pleasure having **Sagi Brody, Co-Founder and CTO at Opti9** on the podcast to shed light on the various aspects of disaster recovery and how to do it well. |
| **Time Stamps** | 00:02 -- Introduction<br><br>00:54 -- Disaster Recovery Statistics and Guest Introduction |

| | |
|---|---|
| | 03:08 -- Guest's Professional Highlights<br><br>04:40 -- Overview of Disaster Recovery<br><br>09:12 -- How do you ensure that the disaster recovery infrastructure does not become the next security incident?<br><br>11:51 -- Disaster Recovery Best Practices<br><br>15:23 -- Around 7% of organizations never test their disaster recovery plan. Why is that the case? Why wouldn't organizations want to ensure that whatever they have documented whatever they have planned actually works?<br><br>19:49 -- How effective are tabletop exercises in the context of rehearsing for disaster recovery? Should organizations be doing more than tabletop exercises?<br><br>22:09 -- Disaster Recovery and Outsourcing<br><br>25:09 -- Final Thoughts |
| **Memorable Sagi Brody Quotes/Statements** | "When you think of backups, I like to think of the word RECOVER. When you think of disaster recovery, I like to think of the word RESUME, you're not restoring data, you're resuming your business operations after a disruption."<br><br>"I think one of the biggest mistakes that people make is they sort of build their entire production infrastructure, or their application, get it all up and running, make it perfect. And then later on, they want to focus on disaster recovery."<br><br>"Imposing disaster recovery strategy on an already built, let's say, application is much more difficult than having resilience be part of |

| | |
|---|---|
| | your thought process as you go along building your production environment."<br><br>"We need Runbooks (or Playbooks) for what we do during a disaster. Not only that, but we need Runbooks for different types of disasters. If we need to fail over one application versus our entire environment, we need a separate Runbook for testing."<br><br>"Today, a lot of people have their applications highly integrated with third party SaaS platforms. So let's be sure that when we test our disaster recovery infrastructure, we're testing the applications, we're not poisoning our production data sitting somewhere else inadvertently."<br><br>"You have to be super careful when making decisions on what platforms, what vendors, what software you're using to build your applications and your infrastructure. When you make those decisions, you have to weigh them against your resilience framework and your security framework." |