Transcript:

John Dodds: Data governance and regulatory frameworks are creating the impetus to involve ransomware. It's like creating the external factor.

Tuhina Goel: Today it has really evolved into pure data destruction, data exfiltration. So that's one major difference we've seen in the last couple of years.

Jason Lopez: On this edition of Tech Barometer, ransomware. The latest trends and developments from two people behind the scenes working on technologies to keep data protected.

John Dodds: Every new cool technology comes out and solves an amazing problem immediately makes security more difficult because it's new.

Jason Lopez: In 2023, the costs of cybersecurity and the payouts to ransomware criminal organizations rose to unprecedented levels. Businesses lost over a billion dollars in payouts. Hospitals, school systems, public utilities have been prime targets.

John Dodds: How can we go from detecting as fast as possible to closing the risk holes before they even become exploitable? That's where AI is going to be a big deal because we have the power at the edge now to make it a reality.

John Dodds: The privacy thing has really created a big problem because it's not just a matter of, oh, I can ignore the ransom and maybe I had good backup hygiene and things like that.

Jason Lopez: John Dodds is a cybersecurity expert who's part of the product management team at Nutanix. In the interview we did with him, he cited multiple factors which explain the rise of ransomware.

John Dodds: The data itself creates a problem because with all the different privacy regulations and data sovereignty rules and regulatory frameworks, it started with GDPR, moved into California Consumer Privacy Act. And now we have regulations in the European Union like DORA. All of these regulations are putting an emphasis on the data custodian's responsibility to protect that data. Everyone knows that these companies could be held liable.

Jason Lopez: One kind of organization is especially vulnerable… health care companies. And they are increasingly vulnerable when hackers don't just lock down data but steal it.

John Dodds: That information is so sensitive and so protected. When they get attacked and there's any chance of exfiltration, they almost have to pay the ransom in some cases because penalties for violating HIPAA and violating all these other things, not just monetary, but also the human damage is getting very, very, very severe.

Jason Lopez: Many organizations are legally responsible for keeping the data on their platforms secure. But this exists, he says, within a compute environment that gives hackers numerous entryways. Dodds points out that, as users, we have more data freedom than ever before.

John Dodds: We have hybrid workforces coming in and VPN aggregators. We have people allowed to access corporate data on mobile devices like iPhones and Android devices. Security teams 20 years ago would have never have let that unrestricted, multidimensional access happen on corporate data that was considered sensitive. The reason why we have this power and flexibility of the modern hybrid workforce and the hybrid cloud environments out there is because these technologies have gotten much more seamless and much better.

Jason Lopez: In the past many organizations might ignore a ransomware attack. But lately, more are paying the ransom. When you add up all the variables from sensitive information, data freedom and liability, the world which organizations operate in has become far more complicated.

John Dodds: Complicated is the right word. The ransomware attacks aren't going to stop, but how we react to them is continuously complicated by everything that's going on in the data governance world at the same time.

Jason Lopez: In this simple hypothetical, Dodds illustrates how, along with threats from hackers, IT departments have to deal with regulators.

John Dodds: There's one thing that I could say that could probably scare you. Do you process credit card data? If we were in a legal case and someone comes up and says, show me every single file that this person touched because I need to know if they had access to insider data or something like that, we were finding a lot of IT administrators sitting around with those kind of, I don't know what to say because you're not going to like the answer type of face.

Jason Lopez: Increased entry points for hackers, more data governance… those help explain the rise of ransomware attacks. There's also been a change in the extortion itself.

Tuhina Goel: There are chances that you will be asked for additional ransom before you can eventually get access to your data.

Jason Lopez: Tuhina Goel is the director of product marketing at Nutanix

Tuhina Goel: So there has been instances where corporations, they were asked to pay ransom, then they were asked to pay additional ransom. And in some cases, they still did not get back access to the data.

John Dodds: That secondary ask is absolutely diabolical because once you've made that threshold where you said your best business decision is to pay the ransom and you have that sunk cost, I hope I never end in a situation where I have to make that sort of decision.

Jason Lopez: If Dodds is right, if ransomware isn't going to be stopped in its tracks anytime soon, what can an organization do?

John Dodds: The best way to protect yourself is to assume you're going to get attacked and make sure that you're doing everything to prevent it at the very beginning on the clients and on the front end, and then ensuring that you have those immutable air-gapped backup copies and snapshots somewhere so that if it does happen to you, it's an inconvenience that you can recover from. That's the best way to make it worthless to a hacker.

Jason Lopez: He says practices like using strong algorithms and salting of keys helps to make data useless.

John Dodds: The way that you devalue the data to a hacker is by proper cyber resiliency built in with many layers of defense, including air-gapped backup copies. So the reason why that data will no longer be valuable to the hacker is if they can't get into it and it's properly encrypted, it's only valuable to a hacker if they have your only good copy of the data.

Jason Lopez: Tech innovation since the rise of the Internet, such as mobility or the cloud, have certainly given companies more tools. But with that, more to protect.

John Dodds: It's a cloud adoption question. Every new cool technology comes out and solves an amazing problem immediately makes security more difficult because it's new. I hate that that's the way it usually ebbs and flows. But generally, there's a reason why cloud was slowly adopted by financial services companies and healthcare companies. They were very conservative on the security side, and they were like, let's wait and see before we bless this stuff.

Tuhina Goel: We talk about cloud native applications and how everything's going to be born in the cloud. And we ourselves as Nutanix, we support hybrid cloud, right? So we are more than an on-prem company. But there are industries whose first preference is to keep their most coveted asset on-prem because the control measures are much more in control, right? So it's just easier to manage that.

Jason Lopez: Since the advent of the Internet, and by extension the cloud, it’s not as if cybersecurity has been after thought. Technologists have been working on it all along. Nutanix’s cybersecurity journey began with storage.

John Dodds: As storage got bigger, as audit logs became bigger, as threats became more diverse, permission structures are inherently super complex, we found out that we needed to move to cloud scale. So that was kind of the evolution of data lens, which was let's do everything we can to make NUS as easy to use to its highest degree for our customers as possible. Because we didn't just want NUS to be a great tool, we wanted our customers to be able to use what made it great. Then we ran into some scale limits, and that's kind of how data lens was evolved.

Jason Lopez: Data Lens is designed to give ransomware resilience to unstructured data on the Nutanix Cloud Platform. It focuses on proactive detection and rapid containment to prevent security breaches before they can cause significant harm. It uses one click recovery and offers tools for compliance and risk analysis. The precursor to Data Lens was a free tool called file analytics, which was essential intelligence for managing data and storage.

John Dodds: Everyone was playing catch up on ransomware on files-based storage systems. We're trying to learn from that and stay ahead of ransomware on object storage systems.

Tuhina Goel: One of their recent emerging technologies is cyber storage, where the expectation is the storage systems will be able to defend themselves against ransomware, especially the unstructured storage, which is files and objects. So the idea is that inherently the storage system should have capabilities to defend itself against ransomware.

John Dodds: It was much more complex to defend security threats on objects because they're the current state of the art in terms of sophistication in a lot of cases, and there's no established kit for object-based ransomware. So we saw the benefit that we had on files, and we didn't want object storage systems to be left out. They are a core source of unstructured data now. So at the same time we did this ransomware containment window, we added support for NUS objects auditing and data lifecycle reporting and anomaly detection.

John Dodds: We're legitimately investigating uses for real AI models now. We're starting to see that the chips have become powerful enough. The models have become sophisticated enough for these multi-ontology LLMs to really start to do some really cool things for security and we're actively researching, how can we take our ML-ish types of things that are more statistical? How can we use AI to push that to the appliances themselves? Security is actually a really good place for it because it is a complex layer of permission structures that were human designed constructs that were put on top of a file system, constructs that were put on top of a directory services infrastructure, data that's being managed by thousands of individual little unique humans. We can't set one policy that everyone will adhere to. That's where we're actually pushing the boundaries with AI. We're taking a lot of our machine learning and basic AI stuff and saying, we have the data, we have to compute. We can now not just proactively monitor for threats, we can proactively identify the risk before it becomes exploited.

Jason Lopez: Dodds essentially says that everything is on the table to not only help protect against ransomware, but to stay ahead of it. So, AI is one tool. What are the others?.

John Dodds: The real answer is we need to already be thinking about adopting the post-quantum cryptography.

Jason Lopez: His team is already looking at three algorithms approved by the National Institute of Standards and Technology.

John Dodds: We're already evaluating how we can implement Crystals Kyber and Crystals Dilithium, which are two of the NIST approved quantum resistant algorithms. The problem is always going to be, it's all theoretical.

Jason Lopez: That's a key concept in the discussion. As much as technologies and cutting edge advancements have a major role to play in protecting against ransomware, both Dodds and Goel place the factor of human nature prominently in the conversation about cybersecurity.

John Dodds: You want to know why I love hackers? Because I feel like they're my people. If there's something that I can find that defines a hacker, the attribute that first comes to mind is laziness. The laziness is winning because there's easier targets. Ransomware hackers can go out there and try to reverse engineer and circumvent all these protections. But why do that when it's still easy to check out someone's LinkedIn profile and find someone at the end of the day who's thinking about what they're going to make for dinner that night, call them up on a phone and try to socially engineer them?

Tuhina Goel: There's no silver bullet when it comes to ransomware or protection against ransomware. People and processes play an as important role as technology does. It's a people problem. It's a people loophole. So it's very important to also pay attention and time and energy budget towards prioritizing employee training and awareness, because that goes hand in hand with what technology can do.

Jason Lopez: Tuhina Goel is director of product marketing at Nutanix. John Dodds is a cybersecurity technologist at Nutanix working in security and data governance product management. This episode of Tech Barometer is produced by The Forecast. I'm Jason Lopez. You'll find more podcasts and articles like this one at theforecastbynutanix.com. That's www.the forecastbynutanix.com.