

CYBERSECURITY READINESS PODCAST SERIES

Episode 116

Passwordless at Enterprise Scale: Bridging Technology and Organizational Readiness

with Jim Taylor, President and Chief Product and Strategy Officer, RSA, and Andrew Shikiar, Chief Executive Officer and Executive Director, FIDO Alliance

Host	Dr. Dave Chatterjee, Duke University
Guests	Jim Taylor, President and Chief Product and Strategy Officer, RSA Andrew Shikiar, Chief Executive Officer and Executive Director, FIDO Alliance
Topic Focus	Passwordless Authentication at Enterprise Scale — Passkeys and FIDO Standards, RSA's Internal Deployment, Change Management, Organizational Readiness, and Governance-Driven Adoption
Podcast Portal	https://www.cybersecurityreadinesspodcast.com/

Summary

In Episode 116 of the Cybersecurity Readiness Podcast Series, Dr. Dave Chatterjee is joined by two leaders at the front line of the effort to retire the password: Jim Taylor, President and Chief Product and Strategy Officer at RSA, and Andrew Shikiar, Chief Executive Officer and Executive Director of the FIDO Alliance. The pairing is distinctive: a solutions provider that rolled out passwordless authentication across its own workforce, and the open, cross-industry standards body whose specifications make such rollouts possible. Dr. Chatterjee cites research reports showing that RSA's deployment reached roughly 1,000 employees, eliminated about 260,000 password-based logins, and cut password-related help desk costs by 90 percent. Taylor explains that RSA, whose customers include governments and banks, set out to prove the approach on itself: as Taylor puts it, "If we can do it, anybody can do it."

Taylor reports that RSA is now at roughly 98 percent passwordless, with the remainder tied to legacy systems and unusual use cases, and that the hardest part was not the technology but the people. Registration experiences that users abandoned, behavior that differed from what engineers expected, and the need for flexible authenticators all demanded attention. RSA responded with an enable, default, and require sequence, starting with its own CISO and CIO as the first users. Shikiar describes how FIDO's open standards, certification programs, usability testing, and deployment guidance support this work, and shares that more than 7 billion passkeys are now in use. Dr. Chatterjee defines the key terms for listeners: every passkey is passwordless, but not every passwordless method is a passkey.

The episode's central lesson is that passwordless success depends on bridging technology and organizational readiness: the cryptography is well understood, but adoption succeeds or fails on people, process, and preparation. Viewed through Dr. Chatterjee's Commitment–Preparedness–Discipline (CPD) Framework, passwordless adoption is a leadership and change-management challenge as much as a technology one: executives commit by going first, the organization prepares through education, communication, and flexibility, and discipline institutionalizes use until it is no longer a choice. Both guests affirm that passwordless is real and that organizations should start now. Shikiar adds a pragmatic caveat: the near-term goal is "less passwords, not passwordless," beginning with the most targeted users, making any remaining password use anomalous, and securing account recovery, since a password fallback can still be exploited.

Discussion Highlights

Why RSA Went Passwordless Itself: Proving It at a Highly Security-Conscious Company

Asked why RSA deployed passwordless authentication across its own workforce rather than treating it purely as a product to sell, Taylor traces his nearly 30 years in cybersecurity, always in identity, with earlier stops at Oracle, Symantec, and Novell. As RSA's chief product and technology leader, he describes himself as the "chef in the kitchen." RSA has been a known

name in authentication for close to 45 years, and he has long believed that passwords are expensive, complicated, and insecure. Making them longer and more complex, he says, mostly drove up the stock of Post-it notes.

Taylor's deeper point is that stronger security has always been possible but inconvenient: put a thousand locks on a door and people will use one and leave the rest unlocked. RSA, a long-time FIDO Alliance member and supporter of open standards even when they do not advantage a vendor, saw that FIDO was designed with consumers in mind and wanted it to work in the enterprise. To be believable, the company decided to live the journey itself; as a high-security firm serving governments and banks, it reasoned that if it could succeed, others could. Dr. Chatterjee notes that it is always valuable to hear from a solutions provider that has implemented its own solution.

If the most secure security company out there can be fully adopted as passwordless, everybody can do it.
— Jim Taylor

Two Careers, One Mission: From Identity Management to Open Standards

Shikar describes a career that has mixed private-company work with leading industry consortia, always around emerging technology: Sun Microsystems during the early days of Java, a streaming media software start-up, the launch of the Liberty Alliance, and then FIDO, where he first ran marketing. He believes this background brings a more entrepreneurial, outcome-oriented lens than a typical standards body, one that treats standards as products to be shipped rather than lab projects.

What keeps him motivated, he says, is that the people contributing to FIDO's more than 300 members, including companies such as RSA, Google, and Apple, are the product and user experience leads who actually ship the technology. When a use case needs a specification or a user experience problem needs fixing, the right experts are in the room. The stubborn entrenchment of passwords, he adds, is precisely why the whole ecosystem had to come together to solve the problem.

Passwordless, Passkeys, and How FIDO Brought Convenience to the Masses

Dr. Chatterjee offers a plain-language primer. Passwordless is the goal: you no longer prove who you are with a password. A passkey is a specific FIDO credential, a cryptographic key pair in which the private key stays on your device and the service holds only the public key. It is tied to the website, so it cannot be phished or reused, and no shared secret sits on a server for attackers to steal. Hardware security keys are another route to passwordless, so every passkey is passwordless, but not every passwordless method is a passkey.

Taylor adds that many approaches to going passwordless existed, using hardware devices or biometrics, but FIDO made it convenient. He compares the challenge to replacing every brass washer in New York City with a plastic one: it only works if the whole community, including vendors and platforms, joins the effort. Shikar explains that FIDO protocols were on the market for about eight years before the term passkeys was introduced four years ago, along with the option to securely synchronize the private key across a credential manager cloud, so a credential registered on one device is available on another. Together with built-in support in every major web browser and platform, achieved through W3C and members such as Apple, Google, and Microsoft, this has driven more than 7 billion passkeys into use and roughly 85 to 90 percent consumer recognition. Because employees are also consumers, that familiarity carries into the workplace.

Inside RSA's Rollout: 98 Percent Passwordless and the People Problem

Taylor reports that RSA is in the high 90s, roughly 98 percent passwordless, and still working toward 100 percent. The holdouts are legacy technologies, such as an old door badging system, a remote console, or a mainframe-era system that does not support modern authentication. He considers the two best decisions of the rollout to be making the CISO and the CIO users number one and two: if it did not work for them, it would get fixed, and executive adoption built momentum.

The main snags were not technical. Registration was a change-management problem: browser and operating system dialog boxes made the process confusing, and users abandoned it much like shoppers abandoning a cart before checkout. RSA studied the behavior it expected against the behavior it observed, then reworked registration, login, and the overall user experience to close the gap. Taylor stresses that the technology, built on cryptographic key pairs used for decades, is the easy part; the packaging around it, the registration, and making the experience compelling are the secret to success. Dr. Chatterjee relates this to his own research on technology implementation, which finds three requirements for success: creating awareness, mobilizing support, and institutionalizing use.

People don't behave the way engineers think.
— Jim Taylor

Standards, Certification, and Deployment Guidance: What the FIDO Alliance Contributes

Responding to Dr. Chatterjee’s request to go deeper on how the Alliance helps companies like RSA, Shikiar describes standardization as a collective choice to commoditize technology up to a certain value line, freeing research and development investment for areas where companies truly differentiate. For that to matter, he says, it needs the right breadth of stakeholders and certification. FIDO certifies servers for the FIDO2 protocols and certifies authenticators, so businesses can avoid vendor lock-in, future-proof their build-outs, and run hybrid environments, for example after acquiring another company.

The Alliance also invests in usability and enablement. Deployment working groups issue best practice guidance; RSA co-chairs the enterprise deployment effort, which recently produced guidance on rolling out passkeys to the workforce. A site called Passkey Central serves product leads who want to get started. Extensive usability testing even examines the words on a screen, and the consistent finding from case studies and conferences is that investing in education to prepare employees is time and money well spent. Dr. Chatterjee notes that this peer sharing is exactly why organizations adopting passwordless should learn from those, like RSA, who have already done it.

Standardization without certification is like one hand clapping.
— Andrew Shikiar

Enable, Default, Require: Changing Behavior in Stages

At Dr. Chatterjee’s request, Taylor explains RSA’s three-stage methodology. First, enable: make passwordless available, build champions among early adopters who can show that it is easier, and learn from user interviews which approaches work. Second, default: passwordless became the easy option on every drop-down, and not using it required deliberate extra clicks, which brought another wave of advocates. Third, require: passwordless became the only choice. The point, he says, was retraining behavior over time, for a workforce that includes HR, finance, logistics, and manufacturing as well as technologists, through guidance, reinforcement, and reward.

Flexibility was essential. RSA has manufacturing facilities where employees may not be allowed to carry phones, so a passkey on a phone does not work for them; a biometric that unlocks a passkey or a physical hardware token may. Shikiar agrees, adding that the larger the enterprise, the more diverse its users, and that settings such as clean rooms may rule out biometrics altogether, which is why a flexible protocol matters. His shorthand for rollout: test, educate, test, educate, roll out.

You have to fit the solution to the users, not fit the users to the solution.
— Jim Taylor

Is Passwordless Real? Start Now, but Aim for Less Passwords First

Asked whether he can tell listeners that passwordless authentication is a reality, Taylor answers with a resounding yes. On the consumer side the technology has long been in browsers and devices; on the enterprise side, RSA has shown it can be done under demanding circumstances and shared the details in case studies. His message to enterprises is that there is no reason not to start today, with help available from the FIDO community and from RSA.

Shikiar agrees that passwordless is in our future but offers a pragmatic framing: the short-term objective should be less passwords, not passwordless. Organizations should start with the most vulnerable people, such as IT workers targeted by social engineers and groups like Scattered Spider, and with the C-suite, and make remaining password use anomalous, so that a password sign-in by someone who has a passkey triggers red flags. He notes that the workforce may have a shorter path than consumer services because recovery, the biggest challenge in passwordless, can be managed with more control in an enterprise. A remaining password fallback can still be exploited for an account recovery attack, which is why the end goal is to remove passwords entirely. Dr. Chatterjee closes by reminding listeners that multi-factor authentication is built into passwordless authentication, so nothing is given up.

...our short-term objective needs to be less passwords, not passwordless.
— Andrew Shikiar

The CPD Framework Applied to Passwordless Adoption

Dr. Chatterjee maps his Commitment–Preparedness–Discipline (CPD) Framework onto the implementation approach Taylor described, which mirrors three decades of research on how organizations assimilate technological innovations. Preparedness is where the bridge between technology and organizational readiness is built.

CPD PILLAR	APPLICATION TO PASSWORDLESS ADOPTION
------------	--------------------------------------

COMMITMENT	Top management support drives adoption throughout the organization. RSA secured it by making its CISO and CIO the first users, so that problems affecting executives got fixed quickly. Leaders also commit to the goal of eliminating passwords, including the remaining legacy exceptions, rather than settling for partial adoption.
PREPAREDNESS	Prepare the organization and its culture. Educate users, communicate what is in it for them and who is speaking to them, study how people actually behave during registration and login, and offer flexible authenticators such as phone passkeys, biometrics, and hardware tokens to fit different roles and work environments. Learn from peers through certified standards, case studies, and deployment guidance.
DISCIPLINE	Institutionalize use so passwordless is part of everyday work processes and no longer ad hoc. RSA moved from enabling to defaulting to requiring passwordless, reinforcing and rewarding behavior along the way, while treating any remaining password use as anomalous and continuing toward 100 percent.

Actionable Recommendations

RECOMMENDATION	DETAIL
Lead from the Top	Make senior leaders, such as the CISO and CIO, among the first users of passwordless authentication. Their adoption builds momentum, and problems they experience get fixed quickly.
Design for Behavior, Not Just Technology	Treat registration and login as change-management challenges. Compare the behavior you expect with the behavior you observe, simplify confusing steps, and invest in education so users are ready.
Move from Enable to Default to Require	Start by making passwordless available and building champions, then make it the easy default, and finally make it the only option once users have been retrained.
Fit the Authenticator to the User	Offer a choice of passkeys on phones, biometrics, and hardware tokens, since environments such as factories and clean rooms may not allow phones or biometrics. Fit the solution to the users, not the users to the solution.
Build on Open, Certified Standards	Choose FIDO-certified servers and authenticators to avoid vendor lock-in and keep hybrid environments interoperable, and use peer case studies and deployment guidance such as Passkey Central.
Prioritize High-Risk Users and Minimize Passwords	Begin with IT staff and executives, who are prime targets of social engineering, and treat the goal as fewer passwords where full removal is not yet possible. Make any remaining password use anomalous so it triggers red flags.
Secure Recovery and Close the Password Fallback	Recognize that account recovery is the hardest part of passwordless and that a leftover password fallback can be exploited. Manage recovery with tight control, and work toward removing passwords entirely.
Apply the CPD Framework to Sustain Passwordless Adoption	Use Commitment to secure executive sponsorship, Preparedness to educate and equip a diverse workforce, and Discipline to institutionalize passwordless use as the standard way of working.

Time Stamps

TIME	CONTENT
0:02	Introduction — Dr. Chatterjee’s background and credentials
0:49	Host framing: passwordless authentication at enterprise scale; guest introductions
2:47	Jim Taylor’s background and why RSA went passwordless internally

6:44	Andrew Shikiar's background and path to the FIDO Alliance
10:07	Dr. Chatterjee defines passwordless and passkeys
11:43	Taylor on passwords, FIDO, and the need for critical mass
14:08	Shikiar on how FIDO works, synced passkeys, and 7 billion passkeys in use
17:33	RSA's results and how close it is to truly passwordless
18:50	Taylor on the rollout: CISO and CIO first, registration snags, and user behavior
25:00	Dr. Chatterjee on awareness, support, and institutionalizing use
27:00	Shikiar on standardization, certification, and deployment guidance
30:41	Enable, default, and require methodology
35:43	Shikiar on flexibility, testing, and education
36:23	The CPD Framework applied to passwordless implementation
39:11	Is passwordless a reality? Taylor's response
41:13	Shikiar: less passwords, account recovery, and anomalous password use
42:48	Closing remarks: multi-factor authentication is built into passwordless
43:48	Special thanks and episode wrap-up

Memorable Quotes

I can put 1000 locks on a door, give you a ring of 1000 keys, you'll use it once, and then you'll leave 999 locks unlocked.

— **Jim Taylor**

Every passkey is passwordless, but not every passwordless method is a passkey.

— **Dr. Dave Chatterjee**

If the most secure security company out there can be fully adopted as passwordless, everybody can do it.

— **Jim Taylor**

You have to fit the solution to the users, not fit the users to the solution.

— **Jim Taylor**

Standardization without certification is like one hand clapping.

— **Andrew Shikiar**

Our short-term objective needs to be less passwords, not passwordless.

— **Andrew Shikiar**

It's time for passwords to go away.

— **Jim Taylor**

Multi-factor authentication is built into passwordless authentication, so it's not like you're giving up something.

— **Dr. Dave Chatterjee**

Disclaimer

The information contained in this summary is for general guidance only. The discussants assume no responsibility or liability for any errors or omissions in the content of this podcast. The information is provided on an as-is basis with no guarantee of completeness, accuracy, usefulness, or timeliness. The opinions and recommendations expressed are those of the discussants and not of any organization.

Dr. Dave Chatterjee | dchatte.com | dchatte@gmail.com | linkedin.com/in/dchatte

© 2026 Dave Chatterjee. All intellectual property rights reserved. | cybersecurityreadinesspodcast.com