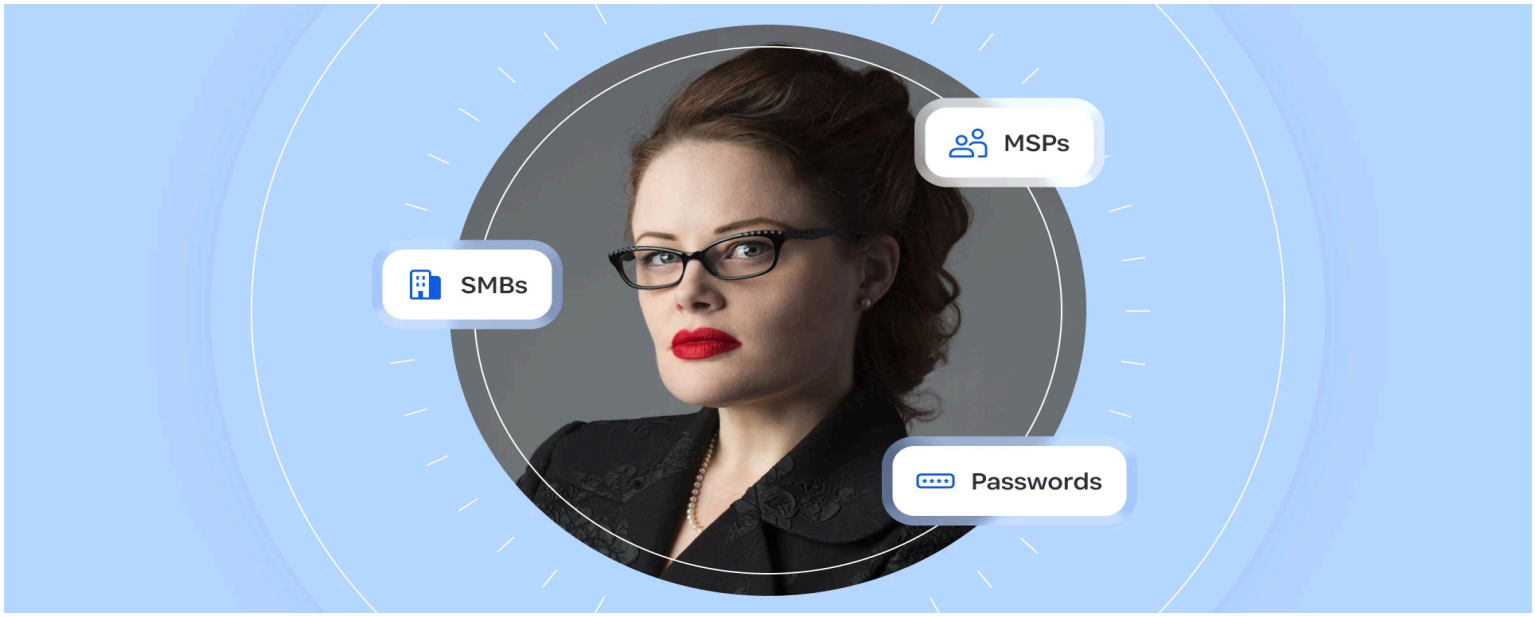
1P_jess
1Password Employee • 1 year ago

Tarah Wheeler on helping small businesses boost their security and choose the right MSP

Last edited: 4 months ago



Tarah Wheeler is passionate about helping small businesses protect themselves against cyber attacks. Her decades-long career in the security industry has revealed a simple truth: small businesses often can't access the same tooling and resources as their enterprise counterparts.

This is where her company, Red Queen Dynamics, comes in. As CEO, Tarah helps managed service providers (MSPs) streamline cybersecurity and compliance for their clients – smaller [illegible] that typically don't have their own IT department or security specialists.

Chat

In the latest episode of 1Password's Random But Memorable podcast, Tarah and 1Password's Michael "Roo" Fey discuss the importance of small businesses taking incremental steps to protect their data. Tarah later explains why it can be so challenging to find a reputable MSP and shares some simple tricks for auditing MSPs so small businesses can feel confident picking one to represent their company.

Read the interview highlights below or check out the full episode in your podcast player of choice. When you've finished, join the conversation in our episode discussion thread!

Can't see the video? ***Watch on YouTube***

Editor's note: This interview has been lightly edited for clarity and brevity. The views and opinions expressed by the interviewee don't represent the opinions of 1Password.

Michael Fey: Are there any common cybersecurity mistakes that make small businesses easier targets? Are there things they don't know that are making them more vulnerable?

Tarah Wheeler: I don't think [any mistakes are] necessarily unique to small businesses. I think a lot of the training – the TTPs [tactics, techniques, and procedures] – we deal with in enterprise security just hasn't migrated down to that level.

I will give you a couple of great examples. Red Queen Dynamics helps small businesses by [drafting questions for them to answer every so often]. And they will be simple questions that help them understand what's going on with security. That reports up to their managed service provider so they can get help with security.

The way we might phrase a question about account takeover and controls of NIST 800-171 [compliance] or something like that might be as simple as, "Are your home and work email passwords different?" They may not understand that they need to have unique passwords. They might change all their passwords at the same time to one password – no joke intended here!

They know they're supposed to change their password, but they don't know they're supposed to have different passwords for different accounts. I feel like you all at 1Password might have a good answer for that question, but they don't know that!

Here's another great one for you. Small businesses inveterately use personal devices to conduct business. They either don't know any better or they can't afford separate devices. It

doesn't matter anyway. It's not like they're issuing corporate devices. So no, [mistakes] aren't unique to small businesses, but it's the economic constraints of cybersecurity to the level that we're talking about here.

MF: What are the key steps that small businesses should take to prevent breaches and ransomware attacks?

TW: Basic security hygiene is incredibly important. What we've learned at this point is that there are about six to 12 important questions and tactics that small businesses can engage in to make sure they're going to be as safe as possible. Basically, [to ensure] they're not the slowest gazelle at the watering hole, and one of those incredibly important elements is ensuring there are strong, unique passwords for different accounts – shared appropriately.

I'm not even selling your product, Roo. I don't have to. I do that because we use 1Password internally at Red Queen Dynamics. We find that that is one of the strongest predictors of ensuring that businesses don't experience breaches.

One, do not permit any employee to disable multi-factor authentication on any account. Two, don't permit the sharing of passwords of an account across employees.

There are a couple of other key elements, as well. Training everybody not to plug strange USB devices into their laptops is still an incredibly important one. There are still large companies getting popped this way – so you know small businesses are, too.

> *"There's no magic. It's not AI, offensive security, or high tech platforms. It's literally just steps like multi-factor authentication and different passwords."*

If you can do wire transfers from your company bank accounts, ensure that for transactions over $25,000 – I actually like to make it $5,000 – that there's a second person required with multi-factor authentication to authorize wire transfers.

The reason is that wire fraud is the most common way that a small business is going to be targeted by attacks.

There's no magic. It's not AI, offensive security, or high tech platforms. It's literally just steps like multi-factor authentication and different passwords. And don't let people use your badge to get into the company.

MF: We've had a few folks on the podcast who do physical penetration testing. Their stance is that you can do as much on the technical side as you want, but that person at the front door is still going to let in the pizza guy. So, you need pretty comprehensive training.

TW: It's got to be comprehensive, but also it has to be multi-layered. It's the Swiss cheese model of defense. It's just true that somebody who's good at conning people is probably going to be pretty good at conning your people. That's the real challenge, right?

I'm married to a physical security specialist, Deviant Ollam. He can walk into any building, look like he belongs there, and walk out. He doesn't walk out with one computer. He walks out with 50 of them and everybody just thinks he's the maintenance guy.

So, how do you protect against an experienced security specialist or con artist? There's usually very little difference between the two of them other than a vague sense of morality. The answer is: defense and depth. You have to make sure that each layer of security is there. It's not just comprehensive training. It's really making sure that those controls, both technical and policy-based, are everywhere they possibly can be.

MF: You've spoken about how you can get a bad MSP in the same way you can get a bad lawyer. How do small businesses balance cost against effectiveness in this realm?

TW: Well, Roo, they do it poorly. That's the answer. They do a really bad job of it, honestly, because it's very difficult to figure out whether or not someone has expertise in an area you don't have expertise in.

Everybody's got a specialty at this point. I am an extremely qualified chief information security officer, and I'm the CEO of a company now too, but I have been hired before as an information security executive. Do you know how hard it is to tell if somebody's good at that job?

It's impossible for a hiring committee of a CMO, a CEO, and a couple of people from the board to tell whether or not someone's good at their job when it's an area they don't have expertise in. The thing we're often relying on is someone else vouching for a person at almost every level.

> *"These folks inside small businesses just have different skills – not lesser – just different ones. There needs to be some respect around that fact."*

So, small businesses don't necessarily judge that expertise. They're looking for basically the equivalent of Yelp stars and reviews and things like that. And that's a hard thing. They do it badly because people are susceptible to being told things that aren't true. Not knowing how to differentiate between confidence and expertise is a really common one. And technology is already an intimidating area.

I have a lot of people tell me, “Gosh, I could never do what you do”. And I'm like, “You've testified before the Supreme Court. What are you talking about? You just have a different set of skills.” So, these folks inside small businesses just have different skills – not lesser – just different ones. There needs to be some respect around that fact. I don't think there is, frankly, from our industry. There's a lot of contempt from information security towards small businesses. And I'm kind of angry about that too.

MF: Are there ways for small businesses to, for the lack of a better term, find those five star MSPs?

TW: I'm going to give you a couple of secret little heuristic tricks that I use.

When I am evaluating whether or not an MSP that I'm talking to – they could be a potential client or I might be referring people to them – does a good job, one of the very first things I look at is who they're connected to on LinkedIn.

Do they put out content that tells me that they care about their customers? Are they connected to and talking to people that appear good in the industry? It’s one of the quickest ways to tell. It’s not perfect. It's necessary, but not sufficient.

One way to tell that somebody isn't any good at being at MSP is to look them up and determine that they are unconnected to the larger ecosystem of MSPs. It means they're not trying to be part of the community of people that are making this better. They're trying to operate in geographic or subject material isolation.

That's a really good way to tell that somebody is probably not great at their job. If they're not being inundated with information and new TTPs, new opportunities, connected with people, and participating in their community, don't hire them. Don't use them for your business.

MF: That's a really good observation that I don't think many people would reach for. To look for that community connection. It really does tell a story about a person without knowing the person.

TW: And, just to note very quickly, the MSP world is very much like information security. It's tribal in some really interesting ways. There are geographic centers there. You'll find that MSPs often focus on operating in a geographic area or a subject area like healthcare in Minnesota or something like that, and you'll often find that that's the case in a way that's super, super interesting.

They're tribal just like we are in information security and being vouched for matters more than anything else.Because again in technology, it's very difficult to tell if people are good at their jobs. Often the only way to do that is to have a community recommend you.

Like 1 Reply Follow Share

Leave a reply...

Was this helpful?

Related topics

Random but Memorable 14.7: Malicious Pottery Service Provider with Tarah Wheeler
Lounge

15 security takeaways from 150 episodes of Random but Memorable
Industry perspectives

Business product updates: May 2026
Industry perspectives

AI-powered social engineering attacks have arrived. Here's how to spot one.
Industry perspectives

Business product updates: August 2025
Industry perspectives

1Password Products

Extended Access Management

Unified Access

Enterprise Password Manager

Personal Password Manager

Password generator

Username generator

Pricing

Downloads

Features

Autofill

Password sharing

Two-factor authentication

Passkeys

Solutions

Passwordless

Device Security

Compliance and Cyber Insurance

What's new

Community blog

Events

Developers

Discussions

Documentation

Integrations

Slack

Bug bounty

Resources

Guides and toolkits

Help and documentation

1Password blog

1Password Marketplace

Random but Memorable

Community guidelines

Company

About

We're hiring!

1Password

Terms of Service

Your Privacy Choices

Cookie Policy

Privacy Policy

Accessibility

©2026 1Password. All rights reserved.
4711 Yonge St, 10th Floor, Toronto Ontario, M2N 6K8, Canada