

On Guard: Why IT Security Remains a Business Priority



Gene Marks

CPA, Columnist, and Host



Lily Hay Newman

Senior writer, *Wired* magazine

Announcer:

Welcome to Thrive, a Paychex business podcast where you'll hear timely insights to help you navigate marketplace dynamics and propel your business forward. Here's your host, Gene Marks.

Gene Marks:

Hey everybody, it's Gene Marks. Thanks for tuning in. You're about to hear a conversation that I had with Lily Hay Newman, who is a senior writer for WIRED Magazine. Lily has been writing in technology for a long time and she covers security, that is like, what she does. I joked around in our interview, considering what she covers, does she live in a cave in Montana, doesn't all this stuff terrify her? It was interesting to hear what her response was and you can listen to it because, although some of the stuff we talked about is terrifying, both personally and for our businesses, she still lives her life and she has a rationale for what she does to make sure that she stays sane. I think you'll find that interesting.

Gene Marks:

Also interesting is that we talked really about two main things that affect our businesses. There are many things, but in the short time we had, we focused on two. Number one is passwords. Are they still relevant? Where are passwords going? Are you using the right passwords? What is she seeing out there, in the world of security, where passwords are going, and will they be replaced by authentication applications, or multi-factor authentication or biometrics? So we talk about that a little bit, so you know, running your own business, what to expect in the days to come, because password as a secure measure, that's changing and that's going to have an impact on you.

Gene Marks:

Secondly, we also talked about ransomware. How can you not talk about ransomware in this day and age? It's a multi-billion dollar business for hackers and criminals that are passing down malware onto people's computers, infecting and encrypting files then asking for money to give their key to release these ransomware files. It's a big issue. So Lily and I talked a little bit about that, as well, so that you can understand the extent that it's out there. And also, what people are doing to prevent against it, if they can do anything and just her thoughts on what she's seeing and where things are going.

Gene Marks:

Again, overall security, passwords, ransomware, these are things that impact your business and we're hearing the advice from somebody that covers this for a living, for WIRED Magazine. Her name is Lily Hay Newman and we'll be back with her in just a minute.

Gene Marks:

All right everybody, we're back with Lily Hay Newman. Again, Lily is a senior writer for WIRED. Lily, thank you so much for joining us.

Lily Hay Newman:

Thanks for having me.

Gene Marks:

So you're a senior writer for WIRED, I want to hear the whole history. How did you make it to where you are now? Start with the seventh grade and just move up from there — I'm just kidding. How long have you been writing for WIRED and where were you in a previous life?

Lily Hay Newman:

I've been at WIRED for about five years, so that's how long I've been dedicated on the cybersecurity beat. Before that, I was a tech reporter at Slate. More general interest, tech policy, emerging tech and also covered a little bit of cybersecurity there but it was a much broader focus.

Gene Marks:

Got it. How did you get into technology?

Lily Hay Newman:

Yeah. I actually was talking to someone about this the other day and they said a similar, "Let's go all the way back to the beginning." I went a little too far back, so now I know how to answer this a little better.

Gene Marks:

Okay.

Lily Hay Newman:

Originally, I was, and still am, interested in science reporting. I did a Masters specializing in that. But, there's a lot more jobs in tech reporting.

Gene Marks:

Right.

Lily Hay Newman:

Because there's a lot more money in tech, and just these huge, huge societal forces, of course. I got into tech reporting that way.

Lily Hay Newman:

But what ended up happening, moving into cybersecurity, is that I found that covering cybersecurity really gives me all the things that I liked about science reporting. I think they're all on a continuum because it's engineering-based computer science, computer engineering. Hacking has this incredible hands-on, or sort of putting-your-brains-together type of collaboration, for better or worse-

Gene Marks:

Sure.

Lily Hay Newman:

- that was really similar to what appealed to me about covering science topics and it has the same variety, emerging research, totally out-of-the-box, mind blowing stuff. And also, really complicated, esoteric aspects to it, and that's something else I really like to delve into, and try to take something just totally subtle and impossible, to understand and try to give a flavor of that to a layperson.

Gene Marks:

It's funny, security itself, it overlaps in so many different areas. It's privacy, and confidentiality, and that's such a big issue for so many of us nowadays. And then, plus it's software, it's hardware, it's various devices, it's the internet, it's, you know, plugins to the internet.

Lily Hay Newman:

And, it's personal life and professional life.

Gene Marks:

Yes, that's exactly right. It is that much of an overlap.

Gene Marks:

I've got to imagine, when you first started writing about security itself not just technology, some people I talk to in the media, it's like they never expected to be there but you probably got drawn in to write something in the field and then because of that, you became a little bit of an expert in it, just to know what you're writing about. And all of a sudden, that mushrooms from there. Is that kind of right?

Lily Hay Newman:

Yeah, definitely. I don't want — the experts are the people I talk to for my stories — I don't want to overstate it. But yeah, I just really ... What I love about beat reporting and choosing one thing is that you get to meet more and more people in that field over time, and just get a sense of a broader and broader community, and its failings and its problems. And also, the amazing things about it. That's what I really enjoy.

Lily Hay Newman:

Yeah, I got really into security and the intellectual topics behind it. But also, just getting to meet more and more people who work on the same thing, or the same type of thing.

Gene Marks:

Right.

Lily Hay Newman:

Obviously, it's a diverse field. But yeah, there's just something very rewarding and fascinating about building out your own mental picture of a community over time.

Gene Marks:

Yeah. No, I agree. I agree.

Gene Marks:

All right, let's talk about some specific security stuff. Like I told you before we started recording, our audience are small business owners, so there are some specific issues that are facing small business owners. I'm going to get to ransomware soon because that's obviously ...

Lily Hay Newman:

Right.

Gene Marks:

But, let's talk about passwords first because you've been doing some writing about passwords and the fact that passwords are not yet dead. Microsoft, as we're talking here, just very recently have come out with ways to avoid using passwords forever on some of their products.

Gene Marks:

So for starters, talk to me about where you see the state of passwords right now and where you see this going. From the aspect of a business owner, will we still be using passwords a few years from now?

Lily Hay Newman:

Yeah. It's such a huge topic, I'm just trying to think of how to distill down.

Lily Hay Newman:

But basically, I think one of the key issues with passwords is they've ... Well, okay. So, first of all, just to quickly recap, we all know the issue with passwords is that it's something -

Gene Marks:

One, two, three, four, five.

Lily Hay Newman:

Right. It's something you know and that means it's something that somebody else could know.

Gene Marks:

Right.

Lily Hay Newman:

As you're saying, a lot of us set them to be easily guessable and all of these, sort of, flubs that we have. And, you know, passwords — it's just so hard to manage them, and remember them that you make them really easy.

Lily Hay Newman:

But at the core, the issue is if it's something you could know, it's something somebody else could know, and that becomes a problem, right?

Gene Marks:

Right.

Lily Hay Newman:

So, in thinking about this, though, because they've been around for so long and it was just the only option that was being presented, maybe there were other options out there, but it wasn't available to regular people. There's all these systems to make passwords better and make it work. So I think that's part of what's been so complicated in trying to transition away.

Lily Hay Newman:

It's very obvious or clear, like I was saying, what the problem is with passwords and why we need to do something else. But, societally, globally, we're so entrenched with this technology. There are some solutions, namely multi-factor authentication, two-factor authentication and password managers, where when used in combination, they're very effective. They really do "improve passwords" a lot.

Gene Marks:

Right.

Lily Hay Newman:

I think that has been — that's the big hump. When you're saying, "Are small and medium businesses still going to be using passwords 10 years from now?" Probably yes, at least in a lot of environments and situations. I think it's precisely because of that combination of there's a lot of unaddressed, unresolved, insecure use of passwords. But then, also, people have invested a lot to improve the security of how they're managing passwords so everybody's all in. So, to migrate everyone somewhere else, I just think that's where the inertia is and that's why it's going to take time.

Gene Marks:

I hear you, with multi-factor authentication. And guys, for those listening just, still not familiar with that, again, that's just you try to log into your bank's website and you get a text message, you know, that you have to put in a PIN.

Lily Hay Newman:

Right, or a code from ...

Gene Marks:

Or, a code that you get, or a text.

Lily Hay Newman:

From an app.

Gene Marks:

Right. I've been reading ... I listened to an episode recently of "Reply All," which is a great podcast by the way, on technology. They were talking with like, a hacker who was voice disguised, the whole thing. The guy was saying how it's very easy to get around multi-factor authentication, it's very easy to dupe a phone company into transferring over a number into another phone, and then the text message comes to the hacker's phone, and then they get access into your ... You know, it terrifies me that people, if they really want to, they can get access to our information, the way that they are.

Gene Marks:

So multi-factor authentication combined with passwords, you're finding in your reporting that it's a good thing, it's taken passwords far along, but it's certainly not the be-all-and-end-all, right? It's not a guarantee that you're secure.

Lily Hay Newman:

Well, the specific example you're talking about, you're absolutely right. If you're relying on getting an SMS text message through the telephony network, the cell network, and to your phone number, that is not a secure way to do two-factor [authentication]. And the security community has known that for a long time because of exactly what you're describing, SIM-swapping attacks where someone, hand of God, reaches in, and grabs your number and takes control of it. And then, the texts are coming to them.

Gene Marks:

Right.

Lily Hay Newman:

Security professionals like to really emphasize using SMS for two-factor [authentication] is better than nothing, people should do it. It will improve their security. But, there are much more secure ways to do two-factor [authentication], such as, like I was saying, there are these authenticator apps that you connect to your accounts and then they'll generate random numbers. It's not related to your phone number. So if your phone is totally compromised with malware, like a targeted attack, attackers may be able to grab those codes, but it's not very scalable.

Gene Marks:

Right.

Lily Hay Newman:

You know, that would be a personal attack on you or your business — that wouldn't be typical. In general, those are a much more secure way to go.

Lily Hay Newman:

You can also get into some of the same technologies that can be used in password-less can also be used as a second factor of authentication with the password. So things like hardware authentication tokens, it's a USB stick essentially, but it's designed especially as an authenticator, and you plug it in. You put your password in, and then you plug in the hardware authentication token, or you, sometimes they could be Bluetooth, and you press a button or whatever it is. And then the account says, "Okay, both of these factors are present, you're authenticated to log in."

Lily Hay Newman:

So those are much more secure ways to do it. But what you're saying, I think, still makes sense which is that, conceptually, it's kind of a way stop on the journey. Like, why don't we just get rid of the password, at that point, and use other factors rather than a password at all?

Gene Marks:

Before we get into the other factors, you mentioned USB sticks, which also seem ... Again, you're physically carrying that around with you, it's like a key.

Lily Hay Newman:

Right.

Gene Marks:

When you plug it in to whatever device that you're in, it's you doing that. My understanding — I don't see a lot of my smaller clients, small companies in general, doing that.

Lily Hay Newman:

Yeah.

Gene Marks:

It seems more like a big company. If you talk to people that work at Google or any big tech, many of them are using those USB sticks, aren't they?

Lily Hay Newman:

Right. Right, these are things like YubiKeys and there are other companies that make them. But, yeah, there's definitely an investment to roll it out. Like we were saying, I think for small and medium business, and big enterprises also, but focusing smaller, the thing is you need to invest where you can. And there's limited resources, a lot of times. You kind of get committed to a path that you're on.

Lily Hay Newman:

So, a small or a medium business that wants to really prioritize doing hardware authentication tokens? That's great, I'm all for — I support it.

Gene Marks:

Sure.

Lily Hay Newman:

They can do it. But, that's really making that a priority one year in the budget, or whatever, because it's also time and expertise of IT professionals or security professionals to get this stuff set up.

Gene Marks:

Yeah.

Lily Hay Newman:

So that's why, probably, you may not have seen it as much and it may not be out there as much. But, it just depends whether there's room to prioritize that and just go all-in on that infrastructure, and then it's there, so it just depends.

Gene Marks:

How about biometrics? We hear about fingerprints, eye scans, even voice recognition, all being used as part of face recognition, as part of security. Do you think that type of technology will ultimately replace passwords? Do you think it will become ubiquitous among particular smaller companies, someday?

Lily Hay Newman:

I have a lot of thoughts here, so again I'm going to try to condense it in.

Gene Marks:

Bring it on. Bring it on. Okay.

Lily Hay Newman:

So that's definitely where things are moving right now, in terms of password-less. Microsoft, for example, it's not the only option for things like "Windows Hello," the Windows no-password authentication. It's not the only option, you can use hardware authentication tokens, you can use other things that we were talking about. But, biometrics really are the first choice, let's say.

Lily Hay Newman:

The reason for that, we were saying passwords are something you know and somebody else could know it, too. Biometrics are something you are. It's not always perfect on the technical systems side, but in terms of you as a human, nobody else can be who you are, like that part is perfect. There can be bugs in the-

Gene Marks:

I keep telling my kids that but they don't buy it.

Lily Hay Newman:

Yeah, there. You're perfect, just the way you are.

Lily Hay Newman:

But so, you can see why it's such an appealing authenticator because it's the essence, right? It's like, that's who you are.

Gene Marks:

Sure.

Lily Hay Newman:

There's no proxy.

Gene Marks:

Sure.

Lily Hay Newman:

You want the, the, the account or the device to know it's you, and they are. It's you. It's your heartbeat, or your fingerprint or your eyes.

Gene Marks:

Right. And it seems like the technology is there, you know what I mean? To do eye scans.

Lily Hay Newman:

It's pretty good, yeah.

Gene Marks:

It's pretty good. But I guess, is it the cost? I mean, In your reporting, do you see more and more biometrics there as a security protocol? And I'm assuming if you do, it's more larger companies that you're seeing this at? Is it out there?

Lily Hay Newman:

Well, well, first of all, here's where we get into all of my thoughts. Yeah, it's definitely ubiquitous because it's in consumer devices.

Gene Marks:

Sure.

Lily Hay Newman:

We've got fingerprint scanners on Android phones. Maybe not low end Android phones, but medium and certainly flagship phones, it's very com- standard. Apple famously popularized face ID. It's not the only consumer facial recognition, but it's one of the most prominent.

Lily Hay Newman:

A lot of that, the crucial thing in terms of security is that those systems authenticate, meaning like, check their record of your face, print, or fingerprints or whatever, locally against what the camera is seeing or what the sensor is seeing. Meaning not sending it off to the cloud, not sending to a server somewhere, it all just happens on the device, and it stays on the device. That's the most secure way to implement this, and a lot of ubiquitous tech has it now. Consumers can get it, small and medium businesses, big enterprises, everybody has at least some of this available to them now.

Gene Marks:

Okay.

Lily Hay Newman:

But, you know, the huge hesitation for me — and based on my reporting, I think a lot of other experts feel this way — but there is this question of well, what would be better? It's like passwords 40 years ago, it just happens, you know?

Lily Hay Newman:

The concern is if your fingerprints or a face print is stolen somehow, even though those systems are very well designed and they're very secure, that's it, forever.

Gene Marks:

You are in trouble, yeah.

Lily Hay Newman:

That's it.

Gene Marks:

That's a problem. Right.

Lily Hay Newman:

Because you only have one face, you only have 10 fingerprints, whatever.

Gene Marks:

Right.

Lily Hay Newman:

Certainly, things like you know, heartbeat, or electrical fingerprint of your heart impulses or something, you're not going to be able to change that.

Gene Marks:

Right.

Lily Hay Newman:

There have been, like, already, for years, some very notable situations in which large quantities of biometrics were stolen.

Gene Marks:

Awesome.

Lily Hay Newman:

Cool, right?

Gene Marks:

Yeah.

Lily Hay Newman:

Not from those local, everybody's-stuff-stays-on-their-own-device systems that I was talking about, but from centralized repositories.

Gene Marks:

Yeah.

Lily Hay Newman:

One of the ones that really comes to my mind is the US government Office of Personnel Management breach, back in 2015, I think — 2014 or 2015, that had 10s of millions of passwords in it.

Gene Marks:

Right.

Lily Hay Newman:

Biometrics.

Gene Marks:

Biometrics, like fingerprints I'm sure.

Lily Hay Newman:

It also has passwords. But, 10s of millions of, I think it was around 30 million fingerprints that had been collected, related to background checking candidates and things like that.

Gene Marks:

Right.

Lily Hay Newman:

It's already been six, seven years since that happened and those are just out there forever. It's not like "Well, it took a while to fix it but a couple years later we worked it out." That's just it, that biometric data is just out there forever. And I am wary of that.

Gene Marks:

Right.

Lily Hay Newman:

Yeah.

Gene Marks:

Yeah, so am I. I guess we have to understand that none of this is completely secure. You're terrifying me because I'm thinking of TSA. When I come back, the global entry system, I use my fingerprints.

Lily Hay Newman:

Right.

Gene Marks:

So that's clearly stored by the government, and I'm sure they're doing a wonderful job securing that, and I'm completely fine and don't have to worry about that being hacked. So yeah, it gives a lot of pause to business owners.

Gene Marks:

Okay, so my takeaway is that biometrics are probably more secure, more secure even just passwords, or even multi-factor authentication, but there is still that risk. And there's this giant risk that, if they do get stolen, then that's like a lifelong problem for a human being, and that is a risk that's out there.

Gene Marks:

Okay, Lily, I'm going to now pivot a little bit. We talked about passwords and biometrics.

Lily Hay Newman:

Yeah.

Gene Marks:

I'd love to spend even more time on this, but let's talk about ransomware.

Lily Hay Newman:

We've got to do it.

Gene Marks:

We've got to do it. Obviously, it's everywhere and it's affecting everyone, including small businesses.

Gene Marks:

So I'm going to ask you to please terrify me and my audience about ransomware. Go.

Lily Hay Newman:

Well, yeah. Ransomware is just on the rise, or sort of, it has been a really major presence for many, many years. I'm sure I'm not telling listeners and viewers anything new with that. But, it just, it continues to be unrelenting.

Lily Hay Newman:

I think the terrifying part, especially if we're thinking about small and medium business, you know, a lot of the super terrifying stuff is huge, critical infrastructure being targeted and things like that. But, to the extent that small and medium businesses could be something like a dentist's office, or an accountant or a contractor who works on food supply, or anything — water, any utilities, any type of contractors working on that-

Gene Marks:

You're exposed to it.

Lily Hay Newman:

It really could be ... I mean, it can be a huge threat to any small or medium business, but just that fear and urgency is there, for I think any entity of any size.

Gene Marks:

As a reporter for WIRED though, am I right? And be for real here, if you're going to report on a story, you're going to lean more towards the ransomware attack that happened on something that's more recognizable, a company that's recognizable. Like you said, infrastructure, the government, large companies, because that's what gets eyeballs.

Lily Hay Newman:

But, I've got to say, it's not just that that's what we're going to lean towards. Small and medium businesses tend to be not wanting to disclose or publicly talk about ... I'm not trying to accuse anyone about disclosure obligations. But, you don't really want to talk about or call attention to the fact that you've had a ransomware attack, if you can avoid it.

Lily Hay Newman:

So you know, the Colonial Pipeline just couldn't hide that something was going on, because it was pretty obvious that there's no gas at the pump.

Gene Marks:

Right.

Lily Hay Newman:

But, if you're a small organization and you maybe grind to a halt for days or weeks — and I don't wish it for anyone — but if you can kind of not talk about that, that's the way that small and medium businesses tend to go. They don't really want to publicize.

Gene Marks:

So you're not finding out about it as much, as a reporter.

Lily Hay Newman:

At least, not on the record.

Gene Marks:

Right, that's fine. And also, if you even sniff that there's a problem somewhere, like you said, business owners like myself, no offense, we don't really want to talk to you about our private business and whether we were attacked, so there's that as well.

Lily Hay Newman:

I'm always making the pitch and while I'm here, I'll make the pitch to all the listeners out there. I think it would be constructive, and valuable and would reflect positively for organizations to start coming forward, you know, and having some of this stuff reported out, to destigmatize and really create more resources for themselves, you know? I'm not trying to put the onus or the blame on victims of these attacks. It's not anyone's fault if this is happening to their business. But, I'm just always trying to make the pitch. The reason reporters are wanting to get information about these attacks out there is not to drag anybody's name through the mud, or to blow up their spot, shall we say, but to raise awareness that it's a huge issue with small and medium businesses, too.

Gene Marks:

That is the thing that I think that a lot of my clients don't really recognize. They hear about the big companies, and the utilities and the transportation systems being attacked. You don't hear as much about small businesses being attacked for the reasons that you just said.

Lily Hay Newman:

Right.

Gene Marks:

And yet, I'm assuming as somebody who covers this stuff, at the very least your sense is, is that many small businesses are being attacked. They're just not talking about it.

Lily Hay Newman:

Yeah. One of the reasons I was hesitating right when you said, "Okay, knock our socks off about ransomware," is that really, the threat that I think small and medium businesses are dealing with the most — not to say they aren't dealing with a lot of ransomware — but "Is business email compromised? Phishing. And then, having either your emails spoofed or your own email systems infiltrated. And, attackers are sending fake invoices to contractors, and all this stuff is going on, or customers.

Lily Hay Newman:

BEC [Business Email Compromise] is a huge, huge, huge threat to small and medium businesses and it's also a tough sell to get people to ever talk about that.

Gene Marks:

Yeah.

Lily Hay Newman:

Ransomware, again, even small and medium, sometimes you just can't avoid people finding out. But business email compromise, you really can. Nobody's going to know, it's just your money being taken, "just."

Lily Hay Newman:

So those, really, it's very hard to get organizations to go on the record about their experiences. And, if it was going to go away, I would get it — you know, I totally understand. But these threats are not going anywhere so to me, the only path is to destigmatize, and to talk about what went well, what could have been better, and kind of all start to share and collaborate more.

Gene Marks:

You talk about phishing, that's P-H-I-S-H-I-N-G.

Lily Hay Newman:

Right.

Gene Marks:

Again, that's an email that pretends to be something else, or from somebody that you might know, or from a legitimate site that's really not. You know, it leads you to an illegitimate site, you click on a link and then that downloads malware.

Lily Hay Newman:

Or, steals your passwords!

Gene Marks:

Or steals your passwords. And now, the latest thing is "smishing," which is SMS texting phishing. Same thing, customers are starting to get all these spam text messages on their phones and I know that I am as well.

Gene Marks:

You bring up a really good point. Anecdotally, the clients that I deal with, and the people that I talk to, when they are hit by a malware attack — emails being stolen, passwords being stolen, like you said, the majority reason why tends to be just us — and I mean me — being dopes. We're not trained well. You know, we click too fast, we don't really recognize it. We don't. We're busy doing ... It's human error. It seems to me that you're right, if more small businesses were to report these things, or be open to having people like yourself write about them, that would help the overall awareness of the issue. It might help people getting more educated about how to identify this stuff.

Lily Hay Newman:

Yeah. I don't want to be blaming anyone for clicking-

Gene Marks:

You can blame me.

Lily Hay Newman:

The thing is, I totally get what you're saying. When sometimes- It's happened to everyone, where you click something from CVS Pharmacy and then you're like, "Wait, was that really CVS?" You know, we've all been there.

Gene Marks:

Oh no!

Lily Hay Newman:

Whatever. But the thing is, it's not really human error, because phishing is designed to get people to click. So when you do fall for it, you're meeting someone's expectations, or you're fulfilling the thing that the scheme is set up to achieve. So you're really doing the right thing, it's just wrong, you know?

Gene Marks:

Yeah.

Lily Hay Newman:

But, I completely agree with your pitch. Please, everyone send me your hot tips, by all means.

Gene Marks:

Fair enough.

Gene Marks:

So, Lily, final question. Ok, we've talked about two major security issues and all the things that can result from it, and you cover security, you've been doing it for a while for WIRED and even before that. So, just share with us, I'm assuming you live in a cave somewhere in Montana and you're afraid to leave, right? You've got no technology, whatsoever. Even the fact that we're having this conversation right now is making you nervous, is that true?

Lily Hay Newman:

Yeah, I keep my safe under a pile of rocks.

Gene Marks:

Gold bars.

Lily Hay Newman:

And, inside is my laptop.

Gene Marks:

I am curious, sometimes it's better to be dumb and happy, you know? You're not dumb, you know about all of this stuff. I'm just curious, how do you deal with this? All of the threats, you personally, that you know about. How do you deal with that personally?

Lily Hay Newman:

So, there's a few concepts that are relevant here. I'm not going to go into all of them, but I have written about them on WIRED.

Lily Hay Newman:

But, the one that speaks to me most is this concept called the Attack Surface. An attack surface is all the windows and doors in a house, basically. And also, could somebody dig a tunnel under your foundation and jackhammer from below, that's the attack surface. What are all the different ways they could get into the house. Could they fly in from above and rappel down?

Lily Hay Newman:

The reason I find attack surface to be, obviously I was joking around, but we think about this in the digital realm as well. What are all the different points of entry and egress for data? The reason I find this concept really useful, and maybe we could also call it harm minimization — if there's less attack surface to work with, that's better.

Gene Marks:

Okay.

Lily Hay Newman:

That what I try to do, is just-

Gene Marks:

Minimize it.

Lily Hay Newman:

-minimize where it's feasible.

Lily Hay Newman:

I'll just give one brief example. Smart speakers are a really good example of something where, for me, currently in my life, I just don't need it.

Gene Marks:

Not needed.

Lily Hay Newman:

I just don't need it. For me, why expand my attack surface to include what if I have an Amazon Echo, and there's some bug and hackers could exploit it, or whatever's going on. For me, that does not need to be something that's making my attack surface bigger.

Lily Hay Newman:

But, I know there's real accessibility issues, real life-circumstance issues that could make a smart speaker really crucial to someone's quality of life.

Gene Marks:

Sure.

Lily Hay Newman:

You know, mobility stuff. If you are a parent, and you have, you're holding kids in each hand and juggling all this stuff, suddenly being able to get information, or set reminders or calendar, or do whatever you need to do, make calls with your voice, is a huge quality of life thing.

Gene Marks:

Hundred percent. My, My father-in-law is like, 150 years old and he's not very mobile. And he has an Amazon Alexa, and he talks to it and it plays him classical music and all that. It-it's sustaining him, he loves it.

Lily Hay Newman:

Right. Yeah. So, I think that's why the attack surface concept is helpful to me, because otherwise you would just have to go to a cave. But I think about, it's just about what do you really need to do, what is just not going to be practical in your life to avoid. And then, what could you cut? What could you cut out?

Lily Hay Newman:

I also don't use a fitness tracker, I don't use a lot of smart tech or internet-of-things devices, I try to minimize that as much as possible. But like you're saying, the ultimate internet-of-things device is my phone and I have it with me all the time. I'm not going to get to zero, but just reducing that attack surface as much as possible I think is good advice for anyone.

Gene Marks:

Lily Hay Newman is a senior writer for WIRED. Lily, that was awesome, thank you for your advice and insights on what you're reporting on. Again, I've scratched the surface of questions I wanted to ask you. We'll definitely have you back, if you'd like to come back, because you mentioned internet-of-things and that's another big issue, from a security standpoint, that is affecting and will affect many small businesses. I think we need to raise awareness about that.

Gene Marks:

For now, just thank you for your time, I appreciate it.

Lily Hay Newman:

Yeah, thanks for having me. Stay safe out there, everyone.

Gene Marks:

You, too. Take care.

Gene Marks:

Do you have a topic or a guest that you would like to hear on Thrive? Please, let us know. Visit payx.me/thrivetopics and send us your ideas or matters of interest. Also, if your business is looking to simplify your HR, payroll, benefits or insurance services, see how Paychex can help. Visit the Resource Hub at paychex.com/WORX, that's W-O-R-X. Paychex can help manage those complexities while you focus on all the ways you want your business to thrive.

Gene Marks:

I'm your host, Gene Marks, and thanks for joining us. 'Til next time, take care.

Announcer:

This podcast is property of Paychex Inc 2021, all rights reserved.