

Episode 52: How To Lockdown Your Company’s Info With Attorney David Harlow

00:00 S?: Welcome to the Neon Noise Podcast, your home for learning ways to attract more traffic to your website, generate more leads, convert more leads into customers, and build stronger relationships with your customers. And now, your hosts, Justin Johnson and Ken Franzen.

00:16 Justin Johnson: Hey, Neon Noise nation. Welcome to Neon Noise Podcast, where we decode marketing and sales topics to help your business. I am Justin Johnson, and with me I have my co-host, Mr. Ken Franzen. Ken, how are you doing today?

00:30 Ken Franzen: I am doing fantastic, Justin, and I'm excited to talk to our guest today because we're gonna cover a topic here that we haven't really touched on much and it's one I've really wanted to dive into. I'm gonna leave a little suspense there for when we dive, get going here, but I'm excited for today's conversation.

00:51 JJ: Absolutely. Today we will speaking with David Harlow. He is a seasoned healthcare attorney and consultant, recognized as an accomplished, innovative and resourceful thought leader in healthcare law, strategy, and policy. His experience in both public and private sectors over the past 25 years affords him a unique perspective on legal, policy, and business issues facing the healthcare community. Healthcare organizations, including providers and vendors of all shapes and sizes, rely on him to help navigate the maze of business issues facing them on a daily basis. Without further ado, David, welcome to Neon Noise.

01:30 David Harlow: Thank you, it's a pleasure to be speaking with you today.

01:33 JJ: Absolutely. Do me a favor and fill in the blanks in anything I may have missed, and share with us a little bit of detail about your background.

01:40 DH: Sure. I am a recovering real estate lawyer. I practiced as a real estate lawyer briefly early in my career, and for virtually my entire career I have been a healthcare lawyer in a sense of focusing on the healthcare that takes place inside certain buildings. And more recently over the past 10 years or so, as healthcare has moved online, so have I. And my practice is now almost entirely focused on digital privacy and security issues, primarily in the realm of healthcare services.

02:20 JJ: Very interesting.

02:21 KF: David, digital security is such an interesting topic. Recently we had the big Equifax breach, and that debacle as far as the way that it was handled and how much information was vulnerable. And can we just touch real quick on really some of the better ways that a business can go about and reference that particular instance and/or any others that you could think of where either they did a great job or perhaps they could have done things differently.

03:04 DH: Sure. So the Equifax debacle is a great example of how little things can get away from you and cause a major disaster, quite frankly. As I understand it, on the technical side, there was a patch that had been issued for one of the technologies that they used, and they had not applied the patch, and that's what created the vulnerability that was exploited and led to this monumental breach. So first order of business is if one of your vendors sends you an update about a patch, do whatever testing you need to do offline, but then bring it into your live environment as soon as you can. Failure to do that can lead to an exploit. Not everybody is gonna suffer an exploit on the scale that Equifax did, but even if it's a smaller scale breach, it's going to affect you in time. It's very important to stay abreast of these things. Often smaller organizations say, "Well, you know, I'm not going to deal with this sort of constant updating." But the cost of not doing so is just unbelievable, as we can see in this example.

04:25 DH: Also, with the smaller examples as well, there can be breaches, there can be things that happen on a smaller scale that also could easily be avoided. In the healthcare realm there's a steady stream of breaches, breach notifications, everything from electronic to paper. There are cases of people leaving paper records in places where they shouldn't be left and that's as much of a breach as a digital breach is. Even though we're focused now mostly on the digital breaches because they can be greater in scale, there's still a sense that we need to keep track of paper breaches as well, everything from confidential information being left in a folder on public transportation to being left in a town dump and being easily accessed because it hasn't been shredded, etcetera. But often we hear about breaches where somebody's laptop has been stolen out of the back of a rental car on a business trip and the hard disc wasn't encrypted. So that's a super easy step that businesses can take. And not taking that step, encrypting the hard drive, is really just malpractice, so to speak. Negligence. If you don't encrypt data, if you don't use the technical tools at your disposal to do the best job that you can, then unfortunately in this day and age, you have a lot of liability coming.

06:17 KF: Well, let's jump on that for a second. Because you think about... And you're an attorney, so there's no one better to answer this question. But as a business owner you have a due diligence... If you're going to collect customer data and store it in any capacity or even just collect it and have that pass through your hands, not even store it, you do have to perform your due diligence in the handling and either storage or the termination of that secure information. What are some of the best practices or what... Let's start first, where are the major vulnerabilities? You gave a great example of a laptop getting stolen from a rental car or someone on a business trip, but what are the other windows that are left open that even though you have a security system and you... Everyone knows how to lock the door and close the windows, if you leave the door unlocked or the window open or you don't arm the security system, your house can easily be broken into.

07:23 DH: Right. And the number of steps we have to take these days, it just keeps increasing exponentially. Things are getting more and more complicated. There are more and more things that we need to keep track of. And this causes problems for people, like in the laptop example. I think the biggest issue in any organization is what I call generically "human factors." We can lock down things from a technical perspective, but there's always somebody who will click on the stupid phishing email and thereby give the keys to the kingdom away. There's always somebody who will download an application on a computer and install it, not realizing that it's just a way for someone to log their key strokes and steal all their passwords, etcetera. So, there's a lot of education that has to be done and constant education and re-education, because these exploits become more and more sophisticated over time. I'm constantly telling people about exploits that I hear about and warning them not to do certain things or to take care in certain ways. And the answer that I often get is, "Well, how can I tell? How do you know that that email is a phishing email?" And there's a whole variety of things that you need to look at. Some of it is sort of a sense developed over time, and it's important for individual organizations and users of online services, social media, others, to just be aware of what looks right, what looks bad, and be always vigilant and skeptical.

09:29 DH: So, human factors. In a broader sense, there's at least three layers of protection that need to be in place, from some regulatory perspectives that incorporate best practices. From a technical perspective, we can divide this up into three areas: Administrative, technical, and physical controls. Starting with physical, you mentioned the idea of locking the doors and arming the alarms. Those are the physical controls. If you've locked everything down physically and nobody can get into the space where you have stored the unencrypted data, whether it's the back seat of a car or the desktop in an office, then you've done a pretty good job on the physical front. So you've addressed the physical security. If you don't let somebody past the front desk in your office space unless they sign in and show ID, that you've addressed some of your physical security with number two, an administrative protection. So you've added an administrative layer to the protection. So nobody gets into the back room unless they've signed in and identified themselves, so we know who they are.

10:56 DH: Technical protections would include things like encryption, would include things like two-factor authentication. If somebody's logging into a resource online, two-factor authentication means you don't just get to log in with a password. We've all experienced this on consumer-facing websites these days, where not only do you need to know your password and some answer to some security question that you may even not remember 'cause you gave an answer two years ago, but you also need something that you have. So it's something you know and something you have. And the something you have now is pretty universally a cellphone. So, when a website texts you a code to your cellphone that you then have to enter into the website, that's using two-factor authentication. So the something you know is the password or the answer to the secret question, and the something you have is your cellphone. So that's good, but not great. There are ways to exploit that. People can clone cellphone numbers, get text messages directed, misdirected, so better, but not perfect.

12:20 KF: Okay. So with that, though, those three components there, what is the weakest? Would it be the physical?

12:30 DH: So the physical is one weak link, but again, as I just mentioned, since people are today able to spoof a cellphone number and therefore have calls redirected to them, technically savvy folk who are motivated in that direction can do something like that, that's a concern. So you can steal a text message. You can hack into somebody's computer remotely if you get them to download something through a phishing email, and then you can track their messages and get those private texts that we otherwise assume are secure and then exploit them. So in the worst case scenario, some of us would say that, look, in this day and age, nothing is secure. Nothing is private. And we need to think about that for a moment and think about whether we need to retreat in a certain way, whether it's even possible to do so, or whether we need to live with the expectation that we need to be constantly vigilant, because there's always the possibility that the next message you get is gonna be a spoofed message, or that somebody is going to hack into your personal health record online or your credit card and make use of that information in some ways. We need to be constantly vigilant, not only to prevent breaches, but also to mitigate the damage once they happen, because they will happen.

14:18 KF: I think it's an important point when you say they will happen, because we hear these new stories about Equifax or these larger instances where whatever database that was compromised. And as a small business owner, we think, "Well, that's a likely target because there's millions and millions and millions of pieces of data, but, who would target me? I'm just a local plumber with a couple hundred clients, and I'm doing a couple million dollars in sales each year." But they should be equally as concerned and follow a very similar protocol as a large organization, or is it different?

15:05 DH: The risk is the same, but obviously on a smaller scale. So if I had a limited number of hours in my day and I'm a black hat hacker, I'm gonna spend more hours trying to get into the Equifax website than I am getting into the local plumber's website, because once I get in, the payoff is greater. That said, if I have access to a hundred or a thousand records that have name, address, credit card number, etcetera, etcetera, that's worth something. And I can try to use those credit card numbers or sell them on the dark web, and they have a certain value, so I can sell them by the hundred or by the thousand, and that's worth something. So everybody's a target is the bottom line, but it makes sense to scale your responses based on your size, and what kind of information you have. Someone like an Equifax has to be held to the highest standard. They have social security numbers. They have banking information. They have all the answers to those secret questions that we use for password double checks on other websites, right? So they need to be held to a higher standard. They should be. And they are. In the healthcare realm and in the broader realm, the broader realm is regulated at this point on a national level by the Federal Trade Commission.

16:48 DH: So poor privacy and security practices conducted by a business are considered an unfair business practice, and that brings it within the jurisdiction of the Federal Trade Commission. So if it's a big case, if it's a national case, the Federal Trade Commission can get involved. And if it is a small case, if it's a local case, state regulators or a state attorney general's office would get involved and say, "You've breached somebody's privacy because of your sloppiness. That's an unfair business practice. You, the plumbing contractor. And because of what you've done, we're gonna fine you. We're going to put in place a compliance program. You need to hire someone to oversee the privacy and security of your customer data over the next five years, make sure you do everything right 'cause you weren't able to do it right before. And they'll have to report to us, and if you fall off the wagon, you're gonna get whacked again," etcetera etcetera. There's a lot of after the fact enforcement tools that are available to law enforcement. My goal is to help people not fall down that rabbit hole in the first place. Prevention is the best medicine. I like to say I practice preventive law and try to help folks put appropriate data privacy and security programs in place in advance so that you never have to deal with that eventuality.

18:35 KF: So the anti-attorney approach: Keep them out of trouble so that they don't have to go down that rabbit hole, so to speak. So let's talk a little bit about that maybe for a quick second. What are some of the things that you work with, businesses, organizations on to prevent? Because I look at this and I say, "Okay, great. This sounds like a very reactive type situation where you hear about another business, local business," something to bring us down to a local level saying, "Okay, great. Frank the plumber, he didn't follow the proper protocol, didn't have the systems established and was careless, was compromised, and now he is getting more than his wrist slapped and is really putting the hurt on him." And you think of that as top of mind as a business owner and then you have that conversation with yourself, like you said, what are my resources, what are my exposure, and you conclude that I probably should do this but I eventually don't or it doesn't become top of mind, it becomes back of mind, and on you go. What are some of the things that you do and how do you work with business organizations in helping them with this?

19:57 DH: Sure. So again, prevention is the best medicine. So what does that mean? We need to start with looking at what kind of data do you use. Do you really need to be using all of that data? Maybe there's stuff you could do without and thereby reduce your risk. So the first step is a broad-based sort of risk assessment. And as part of that, we're gonna inventory, what are all the kinds of data that you use? Where do you store them? How do you use them? Why do you use them? Who within your organization has access to the data? Do they really need access to everything? Why does everybody who logs on to your internal network have access to absolutely everything? Not everybody needs access to full identification, full credit card numbers, etcetera, etcetera. There should be role-based access to limited amounts of information.

21:02 DH: Then you need to put in place, as you can start to see what kind of information there is, what are the kinds of uses that are in place, you need to put in place appropriate policies and procedures internally in order to manage the privacy and security of data that you're handling. Because if you don't have a rule book that you can refer to, nobody's gonna know what you need to do. It doesn't matter if it's a two-person office or a 10,000 person organization. You need a basic guideline to understand what you need to be doing and how you as an organization address the three general categories that I mentioned earlier, sort of the physical, technical and administrative protections of data in order to make sure that it's not misused, abused or breached. You have to be conscious of federal laws, the Federal Trade Commission in healthcare, there's the HIPAA rules in every state. There's your state attorney general that enforces these things, there's local state laws that are different from state to state in the privacy realm, and you need to be able to demonstrate that you're complying with those things.

22:31 DH: So just as an example, in my state, in Massachusetts, there is a privacy law that applies to all businesses, not just healthcare, and you need to have a plan in place. And there are very specific elements of the plan that detail how you deal with certain kinds of information. If you're brought under this law because you hold certain kinds of information, then you need to have this kind of plan in place. You need to have these certain protections in place. I always tell clients, "You should also buy cyber liability insurance so that one bad event doesn't destroy your business, because the costs for responding to an incident, depending on the size, is not gonna be a million dollar event for the plumbing contractor, but once you get to any sort of larger size organization, this could be a business-ending event if you have a breach." So you need to have that insurance in place.

23:38 KF: Okay. Now, when we get to all these policies or procedures and establishing the rules or the guidelines that need to be followed, how much training or how much... 'Cause you have that physical interaction, again, how much training or what's the... What do you... 'Cause if you have employees, and let's say you do have these roles properly set up where only the people that need access to the information have that access to the information; now you've reduced, let's say you have 20 employees who all 20 had that access, now it's down to five, the five that actually need the access. Now you've reduced your vulnerability points down to five individual, walking, human, error machines, which is what we basically are, we all make mistakes, and that's the policies and procedures you're talking about is to minimize or reduce the amount that we make. What takes place there with them in instructing them going forward?

24:43 DH: So, first of all, congratulations, you've reduced your exposure by 75% if you've taken that first step and reduced access to five out of 20 employees, that's terrific. You're ahead of most people. But what has to happen is role-based training and testing, so you need to train people, not giving a general overview seminar of privacy and the importance of privacy and security, but something that's very relevant to their responsibilities at work, and very relevant to the things that they're gonna encounter. But today that includes things like phishing emails, 'cause we're all on email, for better or for worse, and anybody can get a phishing email any hour of any day, click on a link and end up wreaking havoc with their computer system and their company's computer system. So, a lot of education that has to go into this.

25:50 DH: And part of the education that can go on is sending fake phishing emails to your workforce and seeing how they react. So you can send an email, you can send a fake email that looks like it's one of those emails from Chase, or one of the other big banks, they say, "Oh, we noticed there was a security problem, and just enter your username and password, and we're gonna check it out for you." Some people still fall for that. But if you set up a fake one and send it to your workforce, or something more sophisticated, you can... When they do the thing they're not supposed to do, they'll be taken, not to some criminal's website, but to some webpage that you've set up or your contractor has set up that says, "Hey, you blew it, but here's what you did wrong, here's what you should've noticed about this email," and make it an educational experience, not a punitive experience for the employee.

27:01 KF: I like that. That's a great little role-playing or real-life, because when you know you're being auditioned or you're on the clock, for lack of better terms, that you need to respond with an answer, that's easy to regurgitate what needs to be said. But when you're not aware and not thinking, that's a better way to gauge that. How much does password, use of strong passwords, 'cause this amazes me still when I go out, visit with clients, we do a lot of website design development, and with that, the platforms we construct, the CMSs, we give them user access. And a lot of times when I'm doing the training I have them set a password then and there, and WordPress is one of the platforms we use quite often, and the default WordPress password is long and very, very, very abstract, rightfully so, and it's a "secure password," and everyone looks and says, "Oh, my gosh, I am not dealing with that password, can I type in my own?" And, I'm like, "Sure," and they type in five keystrokes and I look at 'em like, "It's the name of your dog, right?" They're like, "Yep," and I'm just like, "Come on." [chuckle] There's just this scary... People are scared of forgetting their passwords and they make them ridiculously easy. Is that still a major vulnerability point for some of these points of entry?

28:36 DH: Yes, absolutely. And equally problematic is the approach to password policies that we've been taking, collectively, over the past number of years, where you need to have an uppercase letter, a lowercase letter, a symbol, a number, and you have to change your password, your system makes you change your password every 30 days or every 90 days. The guy who came up with that policy recently said, publicly, "I just made that up, it wasn't based on anything and as it turns out, it was wrong." And the NIST, the government agency that actually publishes technical recommendations and standards around things like this, has withdrawn their guidance that was based on what this researcher had said 10, 15 years ago, 20 years ago, whatever it was.

29:41 DH: And this has long been mocked, there's this technical comic strip online called XKCD, people have probably seen this, and they came up with... The artist, the author of the script, came up with an idea that it would be much better to have a collection of four random common words than something that has a capital and a number and an exclamation point and something else, 'cause you're gonna forget it, you're gonna have to reset it, it's gonna be problematic. Just come up with a couple of words. So I think the phrase that he came up with was "correct horse battery staple," and it's a bunch of characters, and it's gonna be hard for somebody else to come up with. And once you come up with some weird way of remembering that, you're gonna remember it, and it's pretty secure. Even the password tools that auto-generate complex passwords for every website that you use and then you just have to log into that one service and it automatically logs you into everything and you don't have to remember your passwords, you have to remember a password for that one site, and if somebody hacks that password then you're doomed, 'cause all of your passwords, all of your financial websites, work websites, everything else, are all exposed by breaching a single password.

31:21 KF: So would you suggest not using something like LastPass?

31:25 DH: Well, I think it has good points and bad points. On the one hand, each individual site that you use it for is probably better protected than it would be otherwise. However, if somebody breaches your LastPass account, then, like I said, you're doomed.

31:43 KF: Right, they have the skeleton key to every door.

31:45 DH: So is LastPass doing a better job at security than Equifax was? I don't know.

31:52 KF: Sure. Now, let me touch on the scenario where you've done everything right, you're being preventative, you have the three components in place that you described earlier, you have trained employees, you've reduced as much of the vulnerabilities as possible, and I always get the question, "Can my website be hacked?" from my clients. And I say, "We put all the proper measures in place but if you have a castle with a moat around it with sharks with laser beams on their heads and all the security measures in a place, if somebody wants to break in, there's still a possibility that they could get in, so in the event that you've done everything right and you still are compromised, which does happen if... What liabilities do you hold as a business owner then?"

32:56 DH: Excellent question. So, there are still losses that have occurred and the question becomes less a question of legal liability as, "Is anyone ever going to do business with me again?" So you need to think about this as a PR exercise as much as a legal exercise. You can say, "Okay, I wasn't liable," end of story, but that doesn't help the people whose identities were breached. So, again, that's why it makes sense to have the cyber liability insurance in place that can help cover the cost of the identity theft protection services, etcetera, etcetera, the credit monitoring services so forth. The real issue there is also, if you've done everything that you were supposed to do, you may then get out from under the crosshairs of government investigators. So I've seen this happen. If there's a breach but you can document not only have you done it but you can document clearly that you've done absolutely everything you're supposed to do, then that's a good thing and maybe you have a get out of jail free card as result.

34:24 DH: That is certainly the case in the healthcare arena, where the rules are pretty specific, even though they are "flexible," because they're not necessarily... They're a one size fit all set of rules, which means that they are apply differently to large organizations versus small organizations. But the bottom line, you can document what you've done, that you've done what you're supposed to be doing and the regulators, if they see that you've done what you're supposed to be doing, will not necessarily fine you if there's just been something bad that's happened. On the broader stage, the Federal Trade Commission famously does not have any actual rules defining what you're supposed to do. It's sort of like the old Supreme Court cases on pornography. "I don't know what it is but I know it when I see it." That was the Supreme Court definition of pornography. We have the same problem with the Federal Trade Commission when it comes to unfair business practices. "We can't tell you what a fair business practice is in advance, but if something is breached, we are surely gonna let you know if we think that what you've done was unfair business practice," and the same goes with state attorney generals and state regulators.

35:56 KF: That seems unfair in itself, because every while you look at things that we should be doing, and going back to my, "Hey, we've done everything right, we've done everything," and again, I'm looking at this from the idea of regulation versus public perception, consumer confidence. But if I'm looking at it from a business owner standpoint, stating, "Okay, I've done the things that were 'defined,' but there's so much grey area here that I feel is left open for interpretation," and is that basically what you're saying, is that there's s a lot of grey area open for interpretation and should they decide or determine that this does look like pornography, then they can make that judgement in a case-by-case scenario?

36:47 DH: Right. The Federal Trade Commission operates on a case-by-case basis, that's just the way they work, which is nervous making, of course. So what's the appropriate reaction to that? Is do everything you can do that you feel is appropriate, that your advisors feel is appropriate, and document that you've done it.

37:12 KF: Sure. And we walk that line with, "Okay, great, how much do we want the government defining everything?" Because the dynamics of the online, let's just stick with the online world right now, because that's where most of the change is happening, the advancements in technology, the advancements in security measures, but also the advancements in technique that these identity thieves are taking or data thieves are taking, they're gonna be more sophisticated, they have better tools, their tools are advancing as well. How is the FTC keeping pace with this, or how do we feel the government's doing with at least keeping pace with technology? And then maybe we can touch just quickly on the European Union's GDPR that is going to go into effect, I think it's May of next year, that'll have an impact on anyone doing business in Europe, even if you're located here in the States, but to be mindful of not only what we have here in the United States, but also what others are doing, because it seems like the European Union is taking a little bit more of a definitive approach here, if I'm not mistaken.

38:35 DH: Sure. To start with, there's a need to establish policies and procedures, establish an approach that you're gonna be comfortable with, that you're gonna be able to execute consistently and commit to that. And again, on the Federal Trade Commission level of you may not know until after the fact whether you've done enough, but you can certainly demonstrate that you've done a pretty good job. At the state level, things are often a little better defined, every state has its own privacy law, or just about every other state does. And there's certain things you can do to comply with those laws that would also show that you're being a good citizen if the FTC comes knocking. Just as one example, California a couple of years ago passed a law that says not that you have to definitely allow a user of your website to select a "do not track" option, but you have to let people know whether you do or not, so it's sort of a disclosure, maybe you need to use the tracking because you're using retargeting marketing techniques online and so forth, and that's okay, that's the way we live in this day and age. But you need to tell people that you're doing it and you need to tell people whether or not they can opt out or, if they opt out that means they can't use your website or your service or whatever it is that you're selling online. That allows the consumer to make an informed decision.

40:37 DH: And on the other inside, we may say, "Well, what does that mean? So you're gonna tell me I can't use a website if I don't agree to this technology, and you're shutting me out of a market?" It's probably not as bad as all that, you can use another website, but again it depends on the service that you're trying to use, how important it is to use that particular website, and if they're not letting you select a "do not track" option. But, anyway, the disclosure element of this is important, having good policies and procedures that are not only internal facing in terms of how you manage data, but externally facing, so terms of service on a website, privacy policy on website. Now, to be honest, most of us never read those things that are linked to at the bottom of the page, but over time there's been more of an effort to create plain English versions of those things, or what's called a layered privacy notice. So you can give the equivalent of one page with circles and arrows and a bunch of bullet points and say, "At a high level this is our privacy policy. If you want all the legalese you can click here and dig below," but the top layer is a pretty simple and clear statement of what your approach to privacy is.

42:08 DH: Now, when we go across the pond, we're dealing with an entirely different approach to privacy. You mentioned the GDPR, the European approach to privacy regulation. It comes from a different place, because the whole basic idea of privacy comes from a different place in European law versus United States law. So, it is more comprehensive, it is more overarching, there's much more of a grand unified theory of privacy that starts with the individual, and is really a right of privacy than exists here in the US. And that's just, that's a matter of historical accident and cultural history and all that good stuff. So, it's not an apples and apples comparison. But, as you note correctly, to the extent that US companies are doing business globally, they need to deal with the privacy regimes that exist in Europe and elsewhere around the world. And other parts of the world are more like GDPR, and some are more like the US approach. And I have occasion sometimes to work with companies who are serving global businesses, and need to be up to snuff on the GDPR and other approaches, and help them get into compliance, so that they can do business around the world. Because given the nature of business today, that's what's happening more and more.

43:54 KF: What do you see coming down in the future? What are you excited about or what... And I may ask you to do some future-telling, 'cause I'm thinking of so many different things from a security standpoint. You have the new iPhone 10 coming out with the... And I think the 8 might even have this too, with the facial recognition, so you don't even really need to have a password, it's going to read your face, and you access your phone. So, we have these advancements in technology that are replacing passwords. I always think the house key is such an ancient tool for entering your home, but it still exists today. And you'd think that there would be more advanced ways that we could enter and exit our house and secure it. From not even only a technology standpoint, but maybe even just an evolution of how we're progressing with data changing, what do you see coming down in the future that has you really excited, has you concerned, or that you're really mindful of right now?

45:04 DH: The biometric issues that you mentioned, whether it's facial recognition or something else, or iris scans, or the fingerprint sensors that are on so many phones and other devices these days. The question is, is that easier or harder to hack than something else? So, Apple's initial release of this facial recognition service on the new iPhone claims that it's more secure than the fingerprint recognition, but I think that remains to be seen. I'm sure somebody will try to to hack it, we'll see if they're successful or not. But when the first fingerprint sensor phones came out, there were internet memes, photos online, showing a kid holding a phone, and taking the sleeping dad's hand off the couch.

[laughter]

46:05 DH: And putting the thumb on the phone and unlocking it.

46:09 KF: You're right.

46:10 DH: So, these things can be hacked one way or another. It's only a question of human ingenuity, I think, over time. Maybe we can make it harder, maybe we could make it more difficult, the timeouts involved in unsuccessful attempts. The issue that came up in that regard, with respect to the California shooter, and the unlocking of his iPhone, over the past year or so. So, there's things that are generally out there, and we need to be aware of the limitations of these security services. We keep getting better. We keep getting more secure, but we need to not stop and rest on our laurels. Things keep getting... People keep hacking the things that we thought were secure yesterday, so to speak.

47:06 DH: One thing that I've seen used in the healthcare context, but can be used in other contexts, as well, is sort of another way of using a unique personal identifier. Not when we're all sitting at home, or out in the field with our laptops, or iPhones, or whatever, but if we're interacting with a service provider in some way, where we need to be authenticated. So, the question is, can we use something other than a password? If I go into a bank, if I go into a doctor's office, and I'm signing in, and I'm about to access a treasure trove of personal data, how do I authenticate myself? Well, one way of doing that now is with a hand vein scan. So, it sounds kind of futuristic and science fiction, maybe, you can put your hands down on a scanner and the pattern of veins in your hand is harder to spoof than a fingerprint, than maybe than a face scan, or something like that. Maybe even harder to spoof than a retina scan, according to some of the manufacturers of these devices. So having the ability to have a face-to-face interaction with somebody where they sign in using their hand is potentially much more secure.

48:37 KF: Interesting. And I wonder how many of our listeners looking at their hands right now.

[laughter]

48:44 KF: Like, "Uh, I do have veins in there."

[laughter]

48:48 DH: That's right.

48:48 KF: Great point.

48:48 DH: Because think about it. It's not just a question of, why do we care about that at a point of sale? It's not just about the transaction you're doing today or in the physician office example, right? If you can spoof someone's identity enough to check in as somebody else as a patient in a clinic or a hospital, that means you're doing that in order to access somebody else's healthcare insurance benefits. There have been cases of people who have bought a medical identity on the dark web and then used it to get double knee replacement surgery.

49:29 KF: Oh, wow.

49:30 DH: 'Cause that's expensive. And then imagine if you're the guy whose card they used starts getting bills for co-pays and anesthesiologists.

49:47 KF: Yeah, especially with...

49:48 DH: And then tries to get that information out of their health record, they've been told, at least initially, "Oh, I can't give you that information because it's private health information about somebody else." Yeah.

50:09 KF: But that's awful.

50:10 DH: It's sort of going down the road and thinking about what are the effects of some of these breaches. If we lose a credit card number, somebody goes on a shopping spree in a mall, and the credit card company takes the hit, and we shut it down and we get a new credit card, a new number in the mail. But somebody starts using your health identity, medical identity theft has much broader, deeper, longer-lasting ramifications.

50:47 KF: You hear services like LifeLock or... It's a very popular one out there, I think the CEO put a social security number out there to be hacked, and I think somebody did hack him. But what are some of the measures that a business owner or even a consumer could put up there that would help, that level of defence up for themselves outside of the policy procedure, but once your information's already out on the dark web, let's say you're one of those that were exposed in any of the breaches that have happened in the past, and I feel like all of us have been exposed with as many breaches and as much of our data, at least from a consumer standpoint, would you have any insights on that or what could be done to help set up some firewalls yourself?

51:32 DH: As I mentioned earlier, I think the key thing there is to be vigilant, and one of the ways we can be vigilant is by signing up for various sorts of alerts and locks and limits, so that you can restrict the ability of somebody to apply for new credit in your name, for example. Like a credit report can't be released unless you personally okay it each time, if you put that credit lock or whatever they call it, in place. So there are things that ultimately make your life more complicated and less convenient, but they protect you in some way. So there are some tools out there like that through the credit agencies, although it's... Sometimes we get frustrated and think, "Well it's the fox guarding the hen house," or whatever you wanna call it. Why should I trust these guys to do anything at this point? At the moment, that's all we have and there are the other agencies that weren't hacked this time around who are offering the service as well.

52:50 JJ: Very interesting. Hey, David, if you had one piece of parting advice for our listening audience, what would that be?

52:56 DH: What would that be? Well, to [chuckle] to quote the old desk sergeant from the Hill Street Blues program, "Be careful out there." It's a wild and wooly and dangerous world that we've created and as a result there's a lot of exposures that we're all subject to, and we just need to be aware of it, being conscious of the problems is the first step towards solving or at least minimizing some of these problems.

53:30 JJ: Great advice. What is the best way for the listeners to get in touch with you?

53:35 DH: I am online as HealthBlawg, H-E-A-L-T-H B-L-A-W-G, that's the name of my blog, that's also my Twitter handle, I'm also at harlowgroup.net, that's my law firm website, and for the healthcare crowd I am providing a HIPAA tools tool kit, and you can find me for that at hipaatools.com.

54:04 JJ: Perfect. Neon Noise Nation, we hope you enjoyed the conversation today with David. We will be sure to include all of those links in our show notes, which will be available at neongoldfish.com/podcast. Until next time, this is Justin, Ken and David signing off. Neon Noise Nation, we will see you again next week.

54:25 S?: Thank you for listening to this episode of the Neon Noise Podcast. Did you enjoy the podcast? If so, please subscribe, share with a friend, or write a review. We wanna cover the topics you wanna hear. If you have an idea for a topic you'd like Justin and Ken to cover, connect with us on Twitter @neongoldfish or through our website at neongoldfish.com.