uberknowledge

Phil Dunkelberger, CEO and Founder, Nok Nok Labs

Trust is a Cultural Imperative

Phil talks about the erosion of trust in society, the increasing role of encryption in security, and the need for some privacy standards.

01:19	Privacy and security are two different things and not interchangeable.
02:06	How much access should governments have to their citizens' data?
04:22	The value of the information shared should determine the level of encryption in IoT devices.
06:04	Encryption will play an ever-increasing role in security
08:17	Digital transformation and security in design - can't bolt it on after.
12:04	Trust has been eroded in every area of society
14:06	Is cybersecurity attracting workers motivated by money rather than a desire to do good?
16:50	The U.S. needs a privacy minister. People should stop assuming business will be ethical in its use of customer data.
18:32	As long as we say the ends justify the means, we will fail.

Ashwin Krishnan: [00:00:42] So we have another edition of the UberKnowledge podcast. With me, following John Callas yesterday, is Phil Dunkelberger, who is the other side of the founding team of PGP. I'm sure all of you have heard of PGP. If not, go look up your history books because this is really one of those companies that have stood the test of time. So before going any further, I want to hand it over to Phil, to talk a little bit about something we chatted about just before the podcast: your journey and where we are today when it comes to security and privacy.

Phil Dunkelberger: [00:01:19] Yes, security and privacy has been a debate — the tension between both. Some people think that security means privacy, and inverted, they think that privacy equals security. Actually, they're two different parts of a broad skein of things that have gone on as we've evolved computing over the years. So from the PGP days, the idea that you needed encryption to be able to whisper on the Internet was a big thing. It's how do I ensure that my communications, my files, ultimately my disk drives, if I lose them, I'm not losing corporate secrets, I'm not losing personal information, etc. Some of that falls into business privacy and business concerns, other falls into personal concerns. I store my credit cards and wallets etc. on my devices.

> "We're literally back to ground zero of protecting both your business privacy and your personal privacy along with your data."

[00:02:06] So you've got that tension. Then you've also got the overriding piece of governments that want to know certain things about you, your life. What's personal? What's professional? What are the business things that you're doing, above board or maybe not? What are you doing in your personal life, above board or not? Who are you associating with? And the association piece seems to be one of the really big things. We don't talk about it in that term, but in the age of terrorism that's happened, a lot of what people want to see is who is on your contact list and who do you regularly email or contact or call? And that tension has become, you know, front page news for the last few years. So as much as encryption was key during the Clipper chip era of the late 90s, early 2000s, and that whole idea of government being able to see or not see or having essentially a key to your information, that has gone full circle again. And we're literally back to ground zero of protecting both your business privacy and your personal privacy along with your data.

Ashwin Krishnan: [00:03:14] So one of the things that I've been asking my podcast guests is the association of people or humans and the devices that go along with them. Whether it's a laptop or a mobile, up until this point, there's been a correlation between the number of devices that need to be encrypted with humans. With IoT in particular, where you have this disassociation, if you will, of devices that are proliferating at a scale we haven't seen before, what is your prediction? I mean, is the infrastructure set up, whether it comes to authentication,

whether it comes to encryption, key management, key rotation and that whole spectrum of things that have so far been limited to one of the seven billion humans on the planet? Where there's only X number of devices you can have, versus now, we are decoupled going on a path where these devices essentially have no correlation with human beings. Where do you see, whether it is standards, whether it is scale testing, whether it is root authentication, certificate authority, and the whole scheme, where do you think we are going?

Phil Dunkelberger: [00:04:22] Well, I think, first of all, we've got to change the conversation on whether it's machine-to-machine, as communication in IoT is traditionally thought of, or human-to-machine or machine-to-human types of transfer of data. First thing we've got to start really doing is talking about the value of the information. The value of the information is really going to be predictive of what devices need to be at what level of encryption, what people need to be involved. Sometimes we think about IoT as pure machine to machine. In reality, you're always going to have a human element.

"We think about IoT as pure machine to machine. In reality, you're always going to have a human element."

[00:04:55] People talk about blockchain as maybe curing the common cold these days, that's not necessarily true, there's security issues with that. You're going to have to look at this new modern way of doing things. As we start bringing biometrics in, we start bringing crossover pieces between humans and devices. Biometrics are a crossover. They are a human type of thing that we're now going to use to access data and machines. And they're not like a password; they're a different level of capability. So there's new things, there's innovation around things. My prediction is this: the evolution that will take us away, for instance, from usernames and passwords because that's a failed idea, that's been failed for a long time; it's the leading cause of data breaches, stolen credentials. As we do things like my current work on FIDO with my team, just like it was with PGP, the two kind of hand-in-hand things that have always been there are access control and authentication and encryption. And I see those roles playing out differently now than we had when we had self-contained environments.

[00:06:04] Now that we've got the cloud, you know, one of the big taglines here at RSA 2019 is cloud deployments are outstripping its security. Well, anybody who saw I can do something cheaper, I'm always going to opt for cheaper versus worrying about security. So given that we're already front running the next generation of shared information, given that we're now starting to put AI kinds of things, given the fact that we've got supercomputers doing data crunching for people, like Watson, we're going to have to think differently how we protect those data stores. And encryption is going to play an ever-increasing role, standards like Fast Identity Online alliance (FIDO), that the W3C just said is the future for browser-based security, for strong authentication. These things are all going to play a component

part in what the next generation is going to be. For the next generation is already here; they keep talking about 2020, 2020 is nine months away!

Ashwin Krishnan: [00:07:03] [Laughs].

Phil Dunkelberger: [00:07:03] I think there's a number of those things that are going to play together, to your point.

Ashwin Krishnan: [00:07:08] So let's talk about IT versus OT. If you've traditionally been in IT and you've had the luxury of having a security department, that's one thing. But if you're coming from industries where IT has never even been in place, let alone cybersecurity, I'm talking about, let's say, mining, even healthcare to some degree. There was this conversation yesterday in the CSA summit, where they were talking about why haven't we learned from our past failures? And there was this distinct point of view saying, we may have learned, but there's a new breed of people coming in who are encountering security for the first time in their life. So, they're probably going to make same level of mistakes that we did many, many years ago. Now you expand that to industries that are being cyberized or digitalized at record pace. How do the learnings of a Phil or a Jon Callas or all these people who have had the luxury of going through multiple failures and successes, how does it get bite-sized into this is what you need to know and therefore how do you secure the environment?

Phil Dunkelberger: [00:08:17] Well, I think you've got to go back and look again at what is it we're trying to do when we talk about digital transformation. You know, buzzword bingo says that everybody is doing it. And what I've seen is you can take a lot of new types of technology and try to deploy them at any scale. And what you do is you go fast, and then you suddenly slow down because you now are going to encounter the real challenges of changing manual systems to automated systems. Current automated systems where you made technology decisions 15 years ago that you're now trying to change. And it's digital to digital, but that doesn't go the way you want it to.

> "You can't design a system and then bolt the security on. That's been the mistake we've made over and over."

[00:08:15] So when you're looking at the transitions that we go through, this fast and slow, the learnings that you ask about, learnings are dynamic. When I keynoted at RSA a few years ago, I got up and said, you know, what do we learn from 40 years of cloud computing? That was the title of my talk. And what that really focused on was many things that we've seen in computing before, we just find better, faster, smaller, quicker, different ways to do things more efficient. At the same time, there's certain things like security that then have to follow. And I would argue that where security needs to go in the future is the dynamics are changing so fast, you have to have a best practices plan for your security implementation from the beginning. You can't design a system and then bolt the security on. That's been the mistake we've made over and over.

Ashwin Krishnan: [00:09:59] So one of your predictions, I'm actually reading this out, you mentioned providers need to get serious about authentication and signs that a company is serious include deploying standards and making them mandatory, support for legislation and embracing transparency by sharing actual metrics and other data.

[00:10:15] In today's keynote, the president of RSA, Rohit, was on stage and he was talking about trust in a way that I have not seen elevated to this level. It's one thing to talk about trust, it's another thing to actually do it and do it consistently. So talking about the culture of an organization, how does trust become a cornerstone of everything that you do?

Phil Dunkelberger: [00:10:45] I think that's a that's an interesting way of saying it. I'll go back to many years ago, I started talking about the cloud. I said the cloud's going to really start, not with technology because that's just taking data centers and sharing information and sharing resources in many ways, there's a bunch of other cool stuff that cloud can do for you, but in reality, it's the people. Are you really going to change the way you hire people? Are you really going to look into the security of who has access to multiple tiers of data that multiple companies are sharing - sometimes in competition with each other using the same service?

[00:11:18] Are you going to be able to have legislation that supports things like data breach? You know, we have 48 data breach laws in the country. I would not exactly say we're big on trust right now. We've not been able to ever agree on one data breach framework. Then you see something like GDPR, which is the inverse of trust. It basically says we're going to fine people a lot of money if they breach. And then you get into things like the medical industry where we've had HIPAA for years. If you look at most doctors or dental offices or any place you go to get medical care in this country or overseas, they struggle with what to do with the information you write down. They struggle with, you know, a screen full of information that might have another person's name on it as personally identifying information.

"Then you see something like GDPR, which is the inverse of trust."

[00:12:04] So the concept of trust is a cultural imperative. In an era where trust is eroded in almost all of the things we look at publicly. Government is at an all-time low, in most countries, their trust of government. It used to be 25, 30 years ago. Media's trust is way down. Personal trust. I cannot believe the amount of personal trust that is blown up on social media. I get mad at somebody or they get mad at me, and the next thing you know, our whole lives and conditions have been put up on Facebook or Twitter. This does not bode well for the concept of trust. "Trust but verify," Reagan said, you know, in negotiating arms treaties. The idea of can we build systems that are trustworthy and can be verified, I think are really critical to this.

[00:12:57] One of the really hard things in security development is, bad breath is worse than no breath. If you've literally got a system that people think is trustworthy and isn't, it's worse than telling people we have no security because at least I'm going to be careful of what I put in that data profile. That's something that I think when you look at everybody caught up in the social media phenomena, and now we find that were the big players complicit in something that is really, really near and dear to people's hearts, in this country at least. These are really hard concepts. So the abstract nature of trust, when you boil it down to technology is you better have people that ... you know, I remember Bruce Schneier saying once, the reason he trusted PGP so much wasn't just the technology and that we'd published our source and all the things we did to be transparent, Bruce knew the people that worked there. He knew Jon. He knew the other people. He knew what they stood for. And I think that there's a big part of that in the industry.

[00:14:06] What I've always worried about is a lot of people … because there's so much more money flowing to security IT these days and security IoT these days, all the different flavors. What I worry about is, are the right mindset people really coming to do this work? And I don't want to sound like everything has got to be a cause in life, but one of the things that's really got to be validated, like I said years ago around data centers, if you're going to suddenly be sharing a lot of information, you better know who's in that data center working on it.

"What I worry about is, are the right mindset people really coming to do this work?"

Ashwin Krishnan: [00:14:38] On a positive note, given that GDPR, which, like you said, is the inverse of trust, but it at least highlights what a consumer can and cannot do. Whether it is the keynote at RSA, whether it is a CSA — where Jon was up on stage talking about the very nature of what privacy means and the fact that you can have data as a commodity that can be transacted if you so choose — in your mind, do you feel that at RSA 2019 we're at a point where it's no longer taboo to have the conversation? People are actually willing to have the conversation, but once the show ends and you get back to business is when the rubber hits the road. Compliance is one aspect of it, whether GDPR or CCPA and all the other regulations. But in your mind, what would you envision a leader of a forward-looking organization — and I don't want to name names here — doing or setting the standard by which everybody else starts to say, okay, that's the gold standard, we need to strive for that?

Phil Dunkelberger: [00:15:44] Well, I think you're talking about a couple of concepts beyond trust in this way. I think that when you look at transparency of an organization, that there is not only a cultural transparency, but truly a transparency that deals with issues when they come up openly and honestly. I think that we've kind of lost sight of what transparency really is. And I think that's critical as part of the conversation.

[00:16:13] I think that the conversation about privacy and security has actually been being had for a long time. I just don't think that the devices were as prolific. And the proliferation advices and data, the way they've come in the last 10 years, have really now begun to showcase that conversation. Unfortunately, people enter the constituents of this conversation globally. It's not a U.S.-based discussion or a Europe-based discussion, or an Asia-based discussion. It's not a Latin-American-based discussion. It's not a Nordic discussion. I said this recently, humans really? You know, humans really?

[00:16:50] We have so many things that are challenging in this planet, and the undergirding, whether it's warfare or it's medical systems or financial systems, they all need security. So it goes hand-in-hand with those concepts and the concept of liberty. The concept of having European privacy. They have privacy ministers all over the world. We don't have one. We assume privacy in the United States, that our data will be kept private, that people do the right things with our data.

"They have privacy ministers all over the world. We don't have one."

[00:17:20] It wasn't that long ago that people were shocked, and I mean shocked, that data brokers were buying and selling their data!

Ashwin Krishnan: [00:17:25] I know lots of people are still shocked today.

Phil Dunkelberger: [00:17:28] They had no intervention: I didn't give permission to gather that and sell my data and sell it to advertisers.

[00:17:35] So the interesting piece is that tension between business practice and personal practice, the effects of social media and Twitter. The self-interested parties that when they come to the table, are they really coming to the table looking to solve some of these really thorny issues globally, or are they really looking to game it and trying to make money on it? I think that's where a lot of the broader concepts of trust break down, and I think a lot of the transparency breakdown.

Ashwin Krishnan: [00:18:06] Fascinating conversation. Any last takeaway for you that you would feel like RSA 2019 was a success in your mind?

Phil Dunkelberger: [00:18:15] I think that people need to really look at the fact that trust and security, there is no perfect trust, no perfect security. That's why it was always Pretty Good Privacy; there is no perfect privacy; there is no perfect security system.

[00:18:50] There's a lot of really well-meaning people and people that are trying to do the right thing. It's a journey and we're going to fail. If you look at a pandemic, it's beyond a pandemic now of data breaches. It's beyond a pandemic of really serious things that are encroaching on our personal and professional lives. And the clarion call to me has been — I've been involved in a number of things, as people who know my background of trying to get standards set, trying to get associations

to work together, trying to get cross-cultural boundaries between us and the EU, us and Japan, us and Asia, us and China — Looking at data as currency, **data is currency. It's traded in the black market today. It has high net value.** As long as we continue to have the element that says the ends justify the means in a lot of cases, whether it's a security company, business model or anybody else's, you're going to have failure rates that are going to be very discouraging. The flip side of that is we're probably doing a better job today than we've ever done.

"Data is currency. It's traded in the black market today. It has high net value."

[00:19:41] And for me to say that RSA, the gathering that has become RSA — RSA used to be almost an educational conference years ago — the gathering that it has become, we really need to focus on is there unanimity at some level on certain things within the industry that people can trust and verify, or are we just going to be an industry that's a get some? You know, it's the 80s all over again. And, you know, greed is good and let's just get after it. Because I think that those are the orthogonal drivers right now in our industry, and they can't last in that tension for very much longer.

Ashwin Krishnan: [00:20:23] Well, again, thanks for being here and great to have you, Phil. Thank you.

Phil Dunkelberger: [00:20:29] Thank you.