An Interview with Mark Greene of IBM and John Clippinger of Harvard Law School's Berkman Center for Internet & Society

EDWARDS: I'm Ben Edwards, this is an IBM audiocast. And I'm joined today by John Clippinger of Harvard Law School's Berkman Center for Internet and Society, and by Mark Green, IBM's banking industry sales leader.

John and Mark will be talking about security: why collaboration between different companies, sectors and industries is so important to secure the customer, and how that collaboration can best be achieved. John, Mark, welcome to this IBM audiocast.

CLIPPINGER: Well, thank you very much.

EDWARDS: So Mark, let me start with you. Can you start by giving us a sense of the importance of security to business today, particularly the financial services industry where you operate?

GREEN: Well, of course, the hallmark of financial institutions is dealing in trust, right? The enormous credibility that banks have always had as being the custodians of people's information and money. And that's really under assault these days on the Internet. All of the survey work that we do sort of finds a lot of nervousness out there, and for some good reason.

We're all familiar with the headlines about information that's either been lost or tampered with as it transmits over the Internet.

Some statistics: the kind of fraud that the banks worry about is when their identity is hijacked on the Internet, what's called phishing. And that's easily a $200 million problem in the U.S. alone.

What we're going to be talking about on this call today is theft of consumers' information, identity theft, as it's called, which scored over a quarter million complaints with the Federal Trade Commission last year, over a quarter million consumers in the U.S. were worried that they had been somehow victimized with their information being stolen or misappropriated on the Internet...

Which leads to fully 43 percent of Americans being concerned as they conduct commerce or banking on the Internet about identity theft. So that's a pretty big inhibitor to commerce. And this area of how can consumers better manage and control the security of their own personal information is really center stage these days in the world of Internet banking.

EDWARDS: Okay, so John, let's take up that question. What is it about the way we as businesses and as consumers handle that identity question at the moment that leads to weaknesses in the system?

CLIPPINGER: Well, one of the things that the Internet was really never designed with the notion of identity protection in mind. So it was...it was...that was sort of the forgotten layer.

The problem is, is that people, there's a lot of information about people, and it's scattered in many, many different places. So and no one's sort of [seeing], has real

responsibility for making sure that it's right or protected. It's just too fragmented.

And so if you look at a perspective in the consumer, they would really like to have control over it, because they're most affected by it. They're really at sort of the point of accountability.

So I think the...the.... What you're seeing is, to give consumers power over what their information is and how it's used and how it's being protected, and part of that is then creating almost a marketplace of what they call information providers or brokers that can act on their behalf.

So it's a dual responsibility. It's not just people doing this all by themselves but saying they're really the parties that have the vested interest in getting it right.

GREEN: Yes, I think that's right, as John says, Ben, you know, consumers want more power over how their information is used, who knows what about them and what kinds of information can be used when.

But not every consumer wants to be able to do this all by themselves. Some will be happy to have trusted third parties manage some of it for them, either their bank or some other intermediary.

So this notion of...of shared responsibility, as John says, between a financial institution and a consumer and different individuals will [pick] that balance point differently depending on their preferences and technology savvy.

EDWARDS: Yes, Mark, give us some examples of that, you know, identity

fragmentation problem in action.

GREEN: Well, most interesting forms of commercial transactions will span multiple parties, right? So you're using your credit card to pay a merchant for something, but your credit card was issued to you by your bank which knows certain things about you.

Some of that information goes to the merchant, but of course the merchant may have you at another bank that it deals with. And so who's sort of vouching for the identity of all the parties in that transaction, and who has what view of the information as it flows?

These transactions especially those that span multiple steps, it's really a pretty sophisticated security engineering challenge to figure out how you identify people, authenticate them and then flow information securely at every step along the way.

So the project that Harvard and IBM and others will be launching here is a new approach to this, a sort of user-centered approach that gives the consumer a little bit more power over where those decisions are made.

EDWARDS: So, why don't you say a few words about this user-centric model for tackling security, John? You've been pioneering this at the Berkman Center for a while now. Just first of all explain what it is.

CLIPPINGER: One of the key principles is that people have multiple identities. They're not...there's just...you're not just a single person. I mean, you have an identity in your working, in your family life, in your health care.

GREENE: So it's sort of analogous to all the pieces of plastic you might have in your wallet today, right?

CLIPPINGER: Exactly. Exactly. And so you have all these different identities, you have all these different relationships. And so you don't really...so you have different kinds of sets of rules that apply to each of those, I mean, to the extent to which you're willing to share and how much you're concerned about it being compromised.

For example, health care information is much more sensitive [to say] than other kinds of say merchant...purchasing behaviors. So there are multiple identities.

And part of the user-centric model is to recognize that there should not be a single repository, sort of what Microsoft did with Passport was have a single repository, and they say, well, trust me. That didn't work, and they acknowledge that.

What you're looking at is something that's much more distributed and open and transparent, and this is what's really neat about the notion of open security, sort of a contradiction, but in fact, it's the way you really achieve it because you create transparency.

The other thing about a user-centric model is that you really have to have.... If you're going to have security and trust you have to have accountability. In order to do that, you really have to be able to anchor the identity, authenticate the identity of an individual.

So there's a whole architecture of how to do authentication sufficiently for certain types of transactions, maybe heavy authentication for some; light for others.

EDWARDS: So as part of an initiative to further this user-centric model for identity management, IBM, Novell and the Berkman Center, Harvard's Berkman Center, have come together with an initiative you're calling Project Higgins.

CLIPPINGER: Right.

EDWARDS: Why don't you tell me in your mind what the significance of this project is and just explain a little bit about how it works?

CLIPPINGER: Well, it's an Open Source project, and the reason it's called Higgins is we took the name, it's named after a long-tailed mouse, and the idea is that you're able to get at the long tail of a market, which means you're able to get at very small market segments very efficiently and sort of aggregate markets around a particular profile or interest.

What Higgins really is, is a framework for managing contexts, different contexts around multiple identities. One of the principles of Higgins is that people don't have a single identity; they have multiple identities.

And associated with that are certain principles, how they want to share information about themselves. And the conditions under which they want to be sort of governed in the group. So it's not just profile information.

GREEN: It's sort of an extension of the traditional security idea of role-based access.

CLIPPINGER: Yes.

GREEN: You know, when I'm an IBM employee, here is certain information about myself I'm willing to share with my employer. On the other hand, when I'm a patient of my physician, I'll share these other sorts of information over there but not necessarily the same information I would share with IBM, et cetera.

So in every walk of life, in every commercial transaction you have, there's certain kinds of information about yourself that you're willing to share with certain [counter] parties.

CLIPPINGER: Absolutely. It's not like one size fits all. There are multiple sizes for depend--...depending on the nature of the...the relationship that someone wants to have, and basically a network.

There's another aspect of user centricity that's very interesting to me, I think, is that there can be a virtuous cycle created.

In other words, if the consumer really trusts the institution and the information is going to be used in the way they think it is, then they're more willing to divulge information, finer grained information.

And you have finer grains [of] sharing of profiles, which allows the vendor to provide more targeted services that are more relevant, which in turn reduces their marketing costs and transaction costs.

So if you get it right, I think there's a huge win on both sides, not just on the security side but also on the merchandising side.

GREEN: Right. So as an example, I think we have this notion of clues built into the software so that under this Higgins regime I as a consumer could decide to reveal certain information about myself that is a clue to merchants that might want to do business with me.

For instance, whether I'm interested in trading stocks, or conducting medical research, or buying auto parts, right? Those kinds of clues could be featured in my wallet...

CLIPPINGER: Absolutely, and one of the things you can do is, you can....

We're working on something called authenticated anonymity. In other words, we can know that you are a real person with a certain kind of profile, and you post a clue but you don't have to divulge who you are. And but yet you can get the match, and then you can decide whether you want to sort of follow up on it.

There are many...once you start to put something like this in place, there are many, many opportunities for implementing different kinds of marketing relationships.

EDWARDS: Okay, so the code for this framework is going to be made Open Source. So why is that important?

CLIPPINGER: Well, we...we feel this is absolutely critical. I mean, there...there are a variety of reasons for this.

I mean, we actually started working with the Eclipse Foundation, and it was known as a trust framework. It's been renamed as Higgins. And the Eclipse Foundation is an Open Source foundation, was originally started by IBM.

The point is that you want to get as many people working on this as possible. So, lots of expertise. And if you.... And in order to discover different objections, different points of view, you really got to open it up. The second thing is that to...in order for it to be trusted it really has to be Open Source.

GREEN: And I guess the third element, the ubiquity element...

CLIPPINGER: Yes.

GREEN: ...it's great that it's Open Source, everybody can see it and it's trustworthy, but also needs to be accepted by lots of businesses and merchants and financial institutions.

CLIPPINGER: Absolutely...

GREEN: And so...

CLIPPINGER: ...interoperable.

GREEN: ...you know, there's lots of different vendors who supply those organizations; we need them all part of this initiative for it to...to succeed.

CLIPPINGER: So no one party can impose it on any other. I mean, that just...that's why the Open Source thing is so fundamental to this.

EDWARDS: So the openness makes it more acceptable to the community at large, is that right?

CLIPPINGER: Right. I mean, but.... It needs to be used by.... T he more people that use it, the great--...the higher the value. You don't want to balkanize this. You don't want to start putting walled gardens around this.

GREEN: So the gain to consumers I think is pretty clear here, but what may

be less obvious is this also opens up interesting opportunities for commercial establishments. You know, banks, financial institutions and other kinds of enterprises might set themselves up as providers of trusted intermediary services.

Right? I can be your broker operating on your behalf looking for things that you might want to buy or sell perhaps anonymously. But I can do it as a trusted third party.

CLIPPINGER: Right.

GREEN: And so the fact that we now have pretty fine-grained control around security and privacy information opens up enormous opportunities for new forms of commerce and new types of businesses actually to exist in this world.

EDWARDS: So in other words, Mark, because I'm in control of my identity and who I share it with, I'm more likely to share a deeper level of information with a certain limited number of counterparties?

GREEN: Exactly right, yes.

EDWARDS: Okay. All right, and just finally, Mark, just put this in the broader context of what we at IBM are doing in terms of building out a security framework. How does this...

GREEN: We have a number of related initiatives. There's a data governance and privacy council that thinks a lot about the safeguarding and protection of consumer information.

We've helped organizations establish something called an enterprise privacy framework that allows them to administer such data internally and make sure that it's not misused.

More recently we've been thinking about a number of new technologies to throw at these kinds of security problems ranging from biometric security technologies such as scanning your fingerprint, or your iris print, or indeed looking at the way you sign when you sign checks and other documents.

We have something called cancelable biometrics, which allows you to have separate and revocable tokens of security that you use with each of the parties you do business with.

All of these different elements play into a grander picture over time that says we need to always keep pushing the envelope. One of the truisms about the security business is the bad guys are typically one step ahead of you, and we aim to stay, you know, right up with them by continually innovating in this area of security.

This work on Higgins I think is an idea whose time has come, because everybody understands that the old model of everything being stored and managed for you by your bank centrally, that model is valuable in some situations but not all situations.

And now by allowing users to have more control over it, I think we'll see great advances in security. But it's one element out of a multi-pronged approach to security that we're taking.

EDWARDS: Terrific. Well, John Clippinger, Mark Green, thanks very much for your time and thoughts today. This has been an IBM audiocast.

GREEN: Thank you.

CLIPPINGER: Thank you very much.

[END OF SEGMENT]