

# Fin-tech Challenges: ‘Cyberattacks Are Becoming More Sophisticated Each and Every Day’

Date : September 8, 2015

[http://media.blubrry.com/kwhs/p/kwhs-media.wharton.upenn.edu/podcasts/150827\\_KWHS\\_PwC\\_Fin\\_Tech\\_02.mp3](http://media.blubrry.com/kwhs/p/kwhs-media.wharton.upenn.edu/podcasts/150827_KWHS_PwC_Fin_Tech_02.mp3)

Podcast: [Play in new window](#) | [Download](#)

*Welcome to the PwC-KWHS Podcast Series for High School Educators on Business & Financial Responsibility.*

*I'm Diana Drake, managing editor of Knowledge@Wharton High School, and today we are discussing the intersection of technology and finance. Technology is dramatically changing the way consumers handle personal financial transactions, everything from online and mobile banking and virtual wallets to bar code-based mobile payments and cryptocurrencies. We are here to explore what that changing landscape looks like, and what the technological shift means for the future of money management and financial capability. Also, how can educators prepare students to use these high-tech tools to manage their finances responsibly and successfully?*

*This is part two of our four-part technology and finance discussion with Wharton International Management professor Mauro Guillén and PwC Partner Elizabeth Diep. Here, we explore consumer and industry challenges.*

*Mauro Guillén is director of the Wharton School's Joseph H. Lauder Institute, a research and teaching program on management and international relations at the University of Pennsylvania, and he is also a professor of international management.*

*Elizabeth Diep is a partner with PwC's Asset Management Practice in New York City. Liz is a strong supporter of the firm's "Earn Your Future" program, a \$190-million commitment to improve the financial competency of youth and educators.*

*Thank you both for agreeing to share your knowledge and insights about technology and personal finance. During our discussion, we will also be addressing questions sent in from high school educators.*

*Below is an edited transcript of the conversation.*

**Knowledge@Wharton High School:** New ways of doing things, particularly involving [something] as intimate as one's finances are often met with a degree of skepticism and paranoia. Take for instance, the mobile wallet. Apps like Google Wallet allow consumers to transfer money, redeem coupons or pay for purchases with just a tap of their smart phones. Even so, this and other similar technologies are far from popular. Studies suggest that the way we pay for goods and services probably won't change any time soon. Ease of use does not always lead the charge. Creating the necessary supporting infrastructure is also an issue. So, Mauro, can you address in general this reluctance to adopt new technologies after doing something a certain way for so long? And what are the implications of this for consumers?

**Mauro Guillén:** There are many issues involved in the adoption of any new technology. Here, we're not talking about adopting just one thing. We're talking about adopting a number of different kinds of technologies. We're asking, essentially, the consumer to change his or her habits in a major way. This is not about something that people don't care about. This is about money. And so, there are many different kinds of considerations here that need to be kept in mind.

Starting with the user, with the consumer, habit is, of course, a very powerful force. And it goes without saying that older people have more trouble. Not because they're old but rather because they've been doing things in a particular way for a longer period of time. There's a lot of research that indicates that it is easier ... to introduce these new ways of marketing products and interacting with companies for younger people, for the millennials. Not only are they more familiar with the technology but they don't have any acquired habits that they need to overcome.

I would say security and privacy are really important, and they're two different issues. Security is what happens if I lose my smart phone. If I have all of my information there, all of my credit cards, all of my bank cards, all of my membership cards, what's going to happen? And perhaps technology actually in this respect can reassure users that there are ways of essentially canceling automatically all of your information on a smartphone, or deleting it even if it has been stolen.

Privacy's a different concern. That is to say that once we go digital, then your information can be easily communicated from one part of the world to a totally different part of the world. It can be bought and sold. And a lot of people don't like it. But I would say that with the arrival of flat credit cards 50 years ago, we already entered that world in which some companies, banks, would know everything about you, everything that you buy, where you spend your vacations and so on and so forth.

But you also alluded to another level of complexity here that is important to keep in mind — the infrastructure. So, it takes two to tango and this is a two-sided kind of dynamic. [It is more than] the consumer [needing] to be persuaded that the new technologies are important steps in the right direction in terms of making things easier and more efficient. But you also need all types of vendors and merchants — everything from shops to restaurants to airlines to hotels — you need all of them to accept these new ... forms of payment, these new ways of maybe using discount coupons and so on.

The obstacles lie at those two levels — the level of the individual and the level of the infrastructure because this is essentially a two-sided network dynamic. I don't think we have figured out exactly all of the pieces that need to be in place so that some of these innovations essentially would reach 70%, 80%, 90%, 100% of the population.

**KWHS:** One of the biggest challenges with online and mobile banking, digital credit card transactions and so on is posed by security concerns. David Janeski, a teacher at Fossil Ridge High School in Texas is asking that with the continuing news reports of companies like Home Depot and Target being hacked, how can we rest assured that data is truly encrypted? How can I tell if the transaction I'm doing online is secure? And what precautions should consumers take?

**Elizabeth Diep:** You have all these financial institutions spending billions of dollars on cybersecurity and yet we keep hearing about these security breaches. So ... what isn't working? What can I do as an individual consumer to protect against theft? What I've come to realize is that there really isn't anything that isn't working, per se, except that ["as technology evolves, cyberattacks are becoming more sophisticated each and every day."](#)?

What that means [for] a consumer is that we have to be smart about what personal information we actually share and where we share it. At PwC, we've developed a module on financial responsibility and decision-making as part of our financial literacy curriculum and it relates to consumer fraud because we see that as being such a big issue. As we go out into the middle schools and the high schools, we see students sharing a lot of information without thinking of where that may go and how that could be used.

The module is publicly available and teaches students about fraud, and precautions that they can take to avoid identity theft as well as resources [to tap] if consumers encounter any of these problems. I'll share with you an acronym that the module uses – SCAM or S-C-A-M. [It will] give you some tips on how to reduce the risk of becoming a victim of consumer fraud.

SCAM stands for the following four things: S [stands for being] Stingy about giving out your personal information to others [unless] you have a real reason to trust them and you know where that's going. The C is for Check — check your financial information regularly and look for what should be there but also what shouldn't be — looking at those credit reports and what kind of information is being reported in them. The A is for Ask — asking periodically for a copy of those credit reports. I think [everyone is] guilty [about going] too long without checking our credit reports. Nowadays, that is information that you can obtain on the web for free. Last but not least, M [stands for] Maintaining careful records of your banking and financial accounts. ... We sometimes, and I'm very bad this, will dispose of bank accounts and other information without shredding them or making sure that we know where that's going. There's a lot of very personal information in there that can be used to harm us.

These simple checks can significantly reduce your risk.

**KWHS:** We hear so much about financial institutions spending billions on cybersecurity but we repeatedly hear about these breaches. What isn't working? And are companies considering new models for consumer protection?

**Guillén:** I liken it to an arms race. The hackers are becoming more sophisticated and therefore companies need to become more sophisticated. But as companies become more sophisticated, the hackers and all of the bad people so to speak, they find a way to intrude into the information system. So, I think this is just the nature of the beast. Once we have information in the form of digitized code that's [stored] on an electronic device as opposed to paper and archives and all of that, then we become vulnerable. Somebody miles away — thousands of miles away — can actually hack into, can get into the system and get the data.

I don't think there's an easy answer to this other than it looks like an arms race.

["There's no substitute for innovation, for staying ahead of the curve, for making sure that your systems are safe."](#)

... Are there other ways of protecting the consumer? Well, as you know, credit card companies in particular have been very good at trying to use big data to detect unusual patterns in terms of the usage of cards. So, they know your history, they know what kinds of things you do with your credit card. ... If they detect any unusual activity [it raises a red flag,] or they can use big data to see if your demographic is unlikely to spend on certain things as well. It's not just your own individual history but its people like yourself and they have access to all of that data. So, they're developing tools to prevent fraud from happening as opposed to having to deal with the consequences of fraud after it has taken place.

Many issuers of credit cards now offer you a guarantee that you will not pay for unauthorized use of your account. Unfortunately, I don't think this is going to be enough. If we are moving into the world of electronic wallets, if we're moving into the world of digital currencies and all that, we're going to have to come up with foolproof, very sophisticated security systems that essentially provide the overall system with [security].

Without that, people are not going to buy into these technological innovations. They're going to feel that they're perhaps at the mercy of these periodic breaches that get reported in the press. This is a serious issue and one that could slow down the pace of innovation and of adoption of new technology.

**KWHS:** You started to talk a little bit about cryptocurrencies. The question of risk is often associated with Bitcoin. Bitcoin is money in digital form that you can use to buy things anywhere in the world and that you can invest in. We heard recently about the opening of the first regulated Bitcoin exchange. Can you talk a moment about digital currency? How much traction does Bitcoin have and is the model sustainable?

**Guillén:** If I had a crystal ball I would be able to give you a definitive answer as to whether the model is sustainable. I guess it's not in its current form. But let me explain why.

This is broader than Bitcoin. Bitcoin is just one example of a digital currency, and it's not a particularly successful one

because as we know the value of a Bitcoin has been fluctuating quite a bit. That's a sign that something is wrong with the underlying system that supports it.

The whole point about digital money is the following — for certain periods in history we had currency that was either gold or silver or was pegged in its value ... to gold and silver. This has been the case during certain historical periods. At the present time, no country in the world uses gold or silver as currency and there's no country in the world that has its currency pegged to the value of gold or silver.

So the money that we have in the world right now is as good as the government who issues that currency. You may have a lot of trust in the Swiss government or in the U.S. government or in the German government when it comes to their currencies. But you don't have as much trust in the Brazilian government or the Indonesian government and so on. So, the value or the trust that we have in the money is only as big as the trust that we have in the government that issues that money because there's no other thing like gold or silver behind it.

That's exactly the issue with digital money. That is to say, there has to be enough confidence in whoever is behind that digital money. We know it's not going to be a government. It's going to be maybe a computer or it's going to be a community or it's going to be something that is definitely not going to be a government, but we need to have confidence in it. Whatever algorithm underlies digital currency has to generate enough trust in that the supply of that money is going to be kept under certain limits, that the value of the currency's not going to be eroded.

I think we're making progress in that respect because we see more and more experiments. But I think ["it's probably going to take five to 10 years for the world to see the first truly successful, trustworthy digital currency that can be used for payments."](#)?

That's the first step. And, of course, we could also discuss under what conditions one might want to use a digital currency as a store value — that is to say, to keep your wealth in it. That's a different issue because obviously the first step should be; can we create a digital currency that can be used for payments?

So, we are taking the initial steps. ... And again, I say this because it would be similar to what governments are doing right now in the sense that all it takes is to generate enough confidence. [However,] it's easy for me to say. It's very hard in practice to generate that kind of confidence. And to date, only governments have managed to do that, especially governments that are perceived as being serious and committed to stability.

**KWHS:** Five years is not a long time. It sounds like it would be a smart idea for teachers to start introducing this concept in the classroom. Would you agree — in high school?

**Guillén:** Absolutely. What I think is very important is for high school students to understand that there's nothing behind the piece of paper when it says one dollar other than the confidence that you may have on the entity that has issued that currency, which is the U.S. government. So, in other words, there's no gold, there's no silver, there's nothing backing up that piece of paper other than the trust that we have in its issuer, in this case the U.S. government.

So, you can easily then make the argument, well we could issue a digital currency as long as we can generate enough of a foundation of confidence and trust in it somehow. Now once again, there have been several attempts, perhaps three or four dozen of these digital currencies around. But so far, none of them has managed to generate the kind of generalized trust, especially on a global basis that could make that currency a true global digital currency.