imagine that this type of technology will eventually be given this type of authorization capability. Therefore, the question arises as to how to verify the legitimacy of a request from an AI. Sure, this is far-fetched at this stage, but the technology is quickly approaching the point where such things become possible and financial actors need to think about how this changes their security ecosystem.

Interview with Professor Stuart Madnick, MIT

We recently spoke with MIT's Stuart Madnick, John Norris Maguire Professor of Information Technologies at MIT's Sloan School of Management and Professor of Engineering at MIT's School of Engineering, about the Internet of Things and the cyber security risks associated with the future of this technology in private banking. Below is a short excerpt of this discussion (edited for clarity).

Q. What types of concerns do you see as being particularly salient to the use of IoT devices in banking?

A. *First, it greatly increases the number of attack points. However, the more subtle issue is cyber safety. What we can learn from decades, from looking at corporations, is that whenever there is a major change in the way that an organization runs then the risk necessarily increases. The general newness of the technology causes these security issues.*

Q. How does this tie in, if you will, with the Internet of Things?

A. *There are two possible problem areas with IoT devices: It can do exactly what it was intended to do – but with unexpected consequences - or it can do something that it was never intended to do. Most people are pretty bad at thinking about bad things that could happen and instead only think about the 'standard' uses of a technology or device. As an example of the first case, Alexa was intended to take action after hearing 'Hello Alexa,' but it has been reported that Alexa, upon hearing a show on a television in the same room that mentioned Alexa and a product, proceeded to order the product! For the second case, there are a variety of ways to combine different IoT services together. For example, many IoT devices depend on the smartphone or other types of devices for determining location and such. Each service alone is doing what it is intended to do, securely. However, when you put them together you might know things about the user that was not intended by either service separately.*

Q. Is there anything a private bank or wealth manager can do to mitigate these threats?

A. *I believe training is important and, especially, training people to think outside of the box. Much of today's IT and cyber training puts people in the wrong position. It teaches them to look at probabilities and mechanical outcomes. But cyber criminals think about things in terms of getting the device to do something that it wasn't meant to do. So one clear suggestion is to train people to be able to think about things like a cyber criminal: thinking not about what something normally should do but what it could do.*

Q. Any last comments, perhaps on the biggest cyber risk you see for private banks and wealth managers?

A. *The number of reported breaches are likely a drop in the bucket compared to what is actually going on. The vast majority of cyber security efforts in every industry go into prevention—this makes sense and prevention is a good thing to invest in. Low hanging fruit is a target. I often say: "You can install a stronger lock, but if you still leave your key under the mat, you're not necessarily any more secure." Furthermore, no amount of prevention can guarantee you complete safety, so you need to minimize the damage that can be done. People do remarkably little in terms of detection and recovery. In many cases, a cyber attack has been underway for hundreds of days before detection. Whatever you're spending on detection and recovery needs to be increased. The dark web and cyber criminals are amazingly adaptable and creative. Very creative.*