Tony Buffomante, principal, KPMG in the US, joined KPMG in the US in 2004 after spending the previous 10 years of his career managing information security for a $ 42 billion retailer and spending time as an information security consultant for global organizations. He is currently leading the information protection and business resilience in the Central United States from the Chicago office and serves a number of global clients across industry sectors.

Information Protection... Back to the Future

Interview: Tony Buffomante

***Marty McFly**: "Wait a minute, Doc. Ah... Are you telling me that you built a time machine... out of a DeLorean?"*
***Dr. Emmett Brown**: "The way I see it, if you're gonna build a time machine into a car, why not do it with some style?"*

In the mid 80's, Emmett Brown was looking for 1.21 gigawatts of power to travel back in time, personal computers were starting to pave the way for how organizations could empower employees to work with data, and speaking of style... I was roaming the school hallways in the coolest pair of acid-wash jeans anyone had ever seen. We've learned a lot since then...how to turn cars into spaceship-like machines, how to interact with computers in all aspects of our lives, and maybe even a thing or two about fashion (ok, ok, I still like a pair of white puma hi-tops untied with the big tongue hanging out, but that's a different story altogether)!

One thing we knew back then, however,... just like Dr. Brown trying to get his machine to work...was that the information we had at our fingertips was power... in our personal lives or in business. It was all about the data!

When I started analyzing computer security in the early 90's, companies were very concerned about this new technology called the internet. How do they get on-line? How do they leverage automation like email and services to quickly move data files from one location to another? Could they communicate with customers in a new way? We spent a lot of time building physical security around data centers that housed company computing resources, tried to build "walls" around company networks with technology solutions, and educated users on how to access information they needed to do their jobs in this new way.

Over the years, the information security industry has certainly evolved, due to rapid technology advancements, a changing regulatory climate and the proliferation of new business models for information-security tools vendors and service providers. Oh... and let's not forget about the fact that the bad guys have figured out ways to monetize their efforts vs. just being cool and showing off to their buddies.

Nowadays clients are dealing with:

1. More advanced and resourceful adversaries
2. The proliferation of data via technologies such as Cloud, Social Media and Data Analytics
3. Increased regulatory pressures on reporting information-security incidents to the public

Sounds like a bit of a perfect storm. So what do they currently do about it?

Figure out new ways to lock down systems and the network, buy new shiny tools from security vendors who have "the solution," and try to add more resources to the team to keep up with the pace of change. All of this of course comes with a price, and a new approach to justify the return on investment of this "insurance" program.

Over the past 5 years, I can't tell you how many conversations I've had with companies who told me they just implemented a new security system, reported a successful implementation to the board of directors, and then 3 months later had to disclose that they had been hacked.

Why is this? Well, sometimes as security practitioners, we get blinded by the shiny lights of new tools and technology. We want to win the arms-race with the bad guys by making sure our weapons are better than theirs. We place these weapons all over the company as much as we can as IT professionals, and we try to figure out what the mountain of stuff that comes out of the tools really means. Since we can't find the real issue...more problems arise, via another attack or an audit finding. So what happens next? You guessed it: more security solutions layered on top of the program, and of course, more cost.

So when can we learn from going "Back in Time" (other than Huey Lewis and the News were absolute musical geniuses)?

It's all about the data.

In a world of unstructured information flying inside and out of the organization, over the network, on mobile devices; and increased collaboration with customers or partners requiring more access inside the company walls; how can we prioritize where to place our security investments? The answer is simple to say, and difficult to implement; which provides a great opportunity to assist clients with truly transforming their information security and risk management programs.

It's all about the data.

I think some of the best advice for clients in this space sometimes is to have the IT people stop acting like legacy IT people for a bit... and start talking business language with their partners. Change the conversation from one of "sure I can code that" to:

- What is the company strategy / initiative that we are supporting?
- What are your key business processes that support that strategy?
- What information is absolutely critical to those processes?
- Where does that information live?

Only then can clients have a meaningful conversation on how to prioritize their information security efforts and apply fiscally responsible insurance. Only then can they find that needle-in-a-haystack, because the haystacks are much smaller pockets of critical information assets to look through. Only then can they go to the board and describe how information security investments are being applied to items tied directly to business success.

As we look to the future... undoubtedly we will see continued technology advancements. Self-healing networks, automatic data destruction (poof!) and true artificial intelligence will test our resolve to yet again race to implementation. Additionally, we can all expect increased regulatory challenges, further globalization, and continued pressure on IT departments to support business initiatives better, faster, cheaper. This is great news for KPMG firms as they sit squarely at the intersection of business and information technology issues.

The ability for KPMG professionals to continue to drive the value conversations noted above will be critical to assist clients in making sound information protection and risk management decisions for the next generation and beyond. I look forward to the day when the 2030 version of Marty McFly comes back to ask me two key questions:

Hey Tony... did you know it's all about the data?... and where the heck can I get a pair of those jeans?

It's all about the data