



High performance. Delivered.

# Risk Minds

Modern Threats

## Risk Minds: Modern Threats

We talk about where do the threats come from? And I said from the cost across industries, 300bn to 1trn, the amount the industries are spending to combat will be in the region of, today, about 77bn and we get to 2020 it will be 2-3 times that, 170-200bn. So the investments versus cost make this very significant for all of our players.

I tried to break it down between multiple levels of where to the attacks come from?

At the first level, around the Activist Groups: The importance of you managing your reputation and not being one that falls into the situation, where previously people would show up in front of your Corporate Headquarters with banners and protest. Yet today, they go in and they look at social media and something like 600,000 Facebook accounts per day are in some way altered.

Corporate Espionage: A bit more robust, of course, than just somebody who wants to damage your reputation. As I said before, these organisations now have the ability to sit undetected for much longer periods of time and, when you look at big companies and what they are spending...

Let's look at the US Government. President Obama just signed up to spend \$14bn for the upcoming year to protect the US Government websites against espionage.

From an employee or partner's perspective, our data says that nearly 60% of employees who quit or are fired take proprietary data with them. 59% of employees leaving the building take something with them.

And also, in our experience, this is one of the areas around employees and access to information that many of our clients, many of our businesses, I think have, in some ways, have been too trusting. Everyone here looks at, increasingly, third parties. They look at the administration staff, they look at branch staff and retail but in Corporate Headquarters and for our well paid professionals, why is it that people sitting in New York have access to customer and other data that sits in Europe or Africa or Asia and, increasingly, we see that they are also falling foul, taking that data and selling it down on the dark web or other.

Organized Crime: So we said that the numbers are big but what it also important is that the recoveries are very low. 68% of all cyber crime funds which depart firms are never recovered. So more than 2/3 of the dollars that flow out and never returned, so it is pretty efficient and effective, so there are reasons why it is a growing market.