Hi, I'm Michael Hamelin. I'm the lead security architect with X-Force and the CTO for our infrastructure products. I work with the research teams at X-Force. We have content researchers, we have the advanced research team for malware, and we have engineers who develop things like our protocol analysis model that goes into the heart of our threat intelligence products.

As IBM grew and more security products came into the security division, we realized we had a whole lot of content, and it wasn't fitting into a short simple report we could read twice a year; they were getting pretty long. So, we decided we would break up the report and have a quarterly report, a little shorter, more focused and right to the point, something you could pick up and read quickly.

So, this is the first release in our new format. It's called the X-Force Threat Intelligence Quarterly Report. This is first quarter 2014. And hopefully everybody will enjoy reading it and like the new format as much as we do.

As we look back across all of 2013, there were several major incidents of watering hole attacks. A watering hole attack has been a little elusive, and until last year, a lot of people didn't believe it existed. What we've had is hackers have realized that they need a good return on investment of their attacks, so they're looking for Web sites where all of their targets naturally congregate.

For instance, in the early hack of the year, there was a target against Apple where a third-party developer's website was loaded with malware, and when the Apple developers went to that site, they were compromised.

One about mid-year involved the Department of Labor, and knowing the database updated at midnight, the developers of that site had a flaw in the site, the hackers were able to load malware on the site so everybody from the National Labs that visited that site in the Department of Labor instantly was compromised. So, it's a very focused way for hackers to get at a group of targets without just randomly breaking into a server on the Internet and waiting for the guy they want to visit.

Certainly as we came up to the end of the year, we're all pretty well aware of the Target retail breach. There was also much publicized about Neiman Marcus and a couple others. As you look back across the year, there were several point-of-sale systems attacked.

Starting back in 2010, 2011, we can track the first publications and talks about RAM scrapers and things popping up on the underground for sale. And so, as part of that ever-moving cycle, as we start focusing on controls and security in one environment -- for instance, as we get much more drilled out into payment processors because they've had breaches in the past -- we tend to find that the hackers look for the next lowest-hanging fruit they can find the target in.

And it looks like right now that's going to be our point-of-sale systems. Everybody who wants to get more data and read more about the breaches, and you can find it online at http://ibm.co/ibmx-force2014.

[END OF SEGMENT]