Key questions:

- How high can, or should, the costs of effective cybersecurity go?
- What are the best (affordable) management tools to protect data, identities, the integrity of businesses, governments and individuals?
- How do we persuade individuals to protect their computers and mobile phones?
- Where will the next generation of cyberthreats come from?

Summary of debate

The debate was launched with the comment that people are losing trust in the internet and that in most cases people don't understand the technology, let alone the security needed to protect their personal networks and computers. Tech-savvy criminals are exploiting this complexity. In fact, many would argue that the vulnerabilities haven't changed significantly over the last years. There was a general consensus amongst the panelists, that security is not an optional component. Governments should implement policies that enforce security, while also ensuring that funding is allocated to ensure the integration of security components.

Continued technological advances bring increased vulnerability. For example, a smart grid market with billions of smart meters brings with it the serious risk of fraudulent use by cyber-attackers. In the US, one billion dollars has been dedicated to a smart grid grant, none of which has been allocated to security. This kind of "old thinking" needs to change.

The major issue of incentives was raised; based on Cambridge research, most errors occur because the incentives are wrong and that as a global community we "dump risk", continuously pushing the liability onto someone else. Taking the example of the Met in the UK, it was pointed out that there is little incentive to take major action against a global cyber-attack when the US, as a percentage of internet market, will always receive more of the virus-ridden email attack or spam. There also needs to be more consistent fraud and malware reporting.