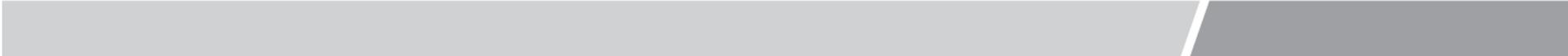


Cyber Coverage – Affirmative / Silent / Standalone



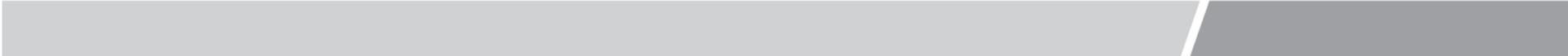
By Scott Sayce – European Underwriting Director CNA Hardy

The Challenge



Should **you** or shouldn't **you**?

Threat **Land**scape



Over **1,000,000,000** data records
were lost or stolen in **2014**

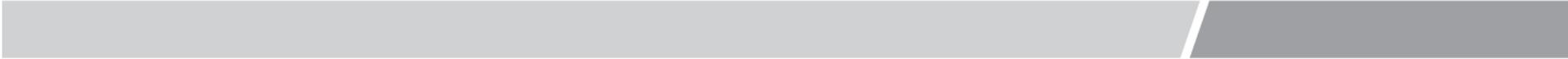
That's **32** Per Second!

Threat **Landscape**



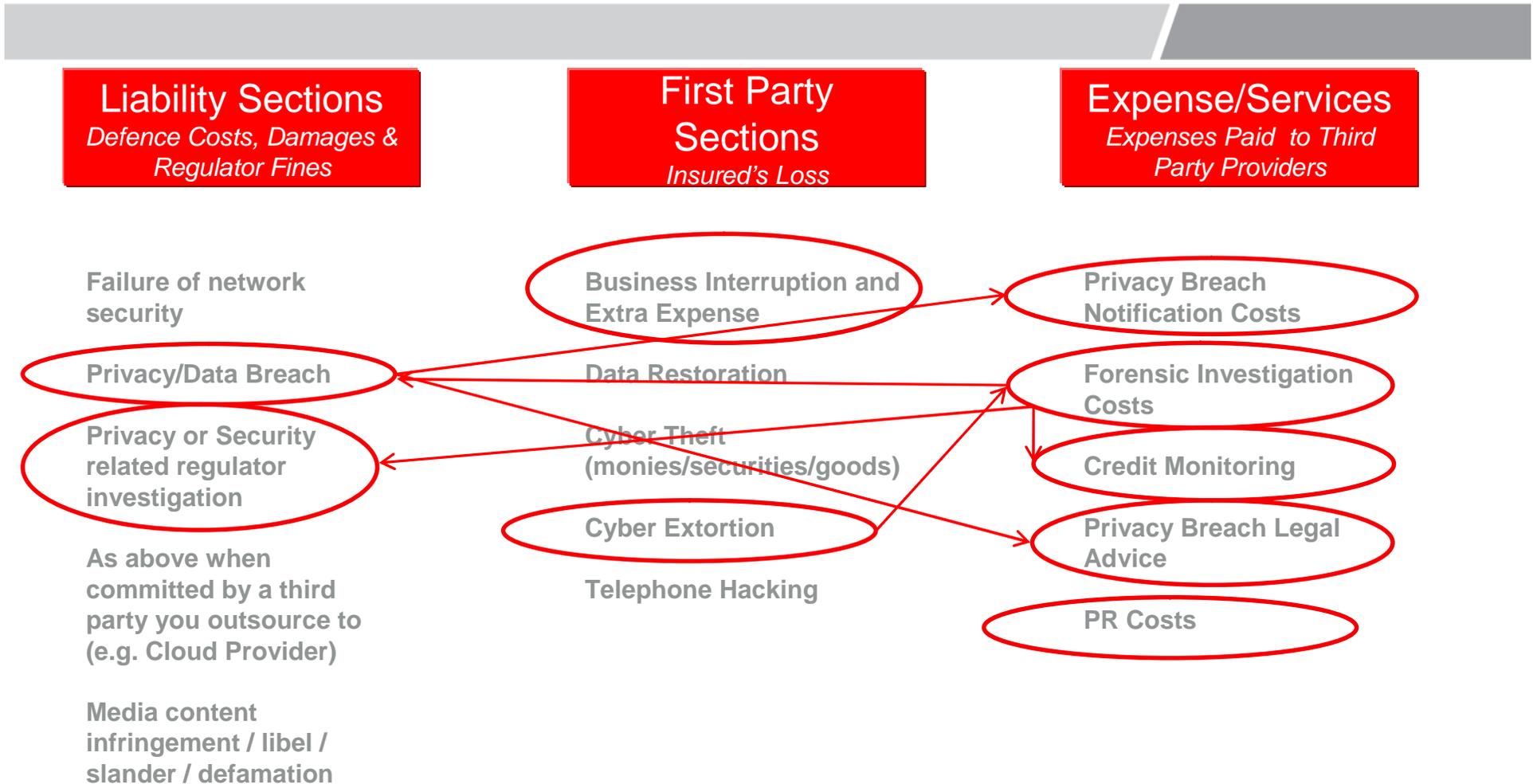
Average of **315,000** varieties of
malware created **every day**

Threat **Landscape**



60% of the attacks in 2014 were due to the exploitation of critical vulnerabilities that were known publically since **2012**

Full “Cyber” Policy

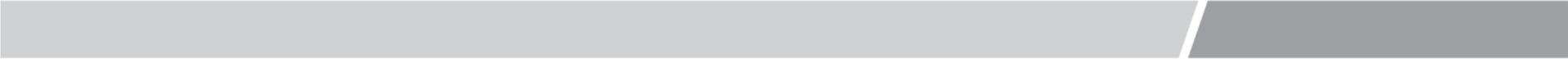


Cyber Underwriting **Factors**

Underwriting cyber risks are complex and therefore technical dedication and knowledge is required. Areas assessed (this is not the entire list) include:

- Understanding IT and broader risk management policies and controls (standards, policies, protocols, controls outsourced providers such as The Cloud and payment processors)
- International laws, regulations and contractual liabilities
- Relevant technology, vulnerabilities and security controls (hardware and software)
- Appreciation of dependency upon data and business models
- Industry specific risks
- Aggregation and accumulation risk
- Numerous systemic risks

The Cyber Insurance **World**



- Cyber Insurance is unrecognisable from 15 years ago
- Evolving legal landscape
- New technological innovation
- Data as a business tool rather than a by-product of doing business
- Continuous product innovation