

FTSE 350 CYBER GOVERNANCE HEALTH CHECK Summary

More firms are **GETTING THE BASICS RIGHT**



58% of companies

had assessed themselves against the government's "10 Steps" cyber security guidance



UP from **40%** in 2013

CYBER SECURITY is seen as a business risk

88% of companies

now include cyber-risk in their risk register



UP from **58%** in 2013

BOARD KNOWLEDGE of cyber security is **IMPROVING**



Training for board members has risen in the last **12 months**



In 2014 this was **48%** for audit chairs

UP from **29%** in 2013

30% of boards



received regular high level cyber security intelligence from their CIO or Head of Security

UP from **18%** in 2013

INFORMATION SHARING is improving

49% of companies

encourage employees to share information with other companies in order to combat the cyber threat



Companies are getting better at **UNDERSTANDING SUPPLY CHAIN RISK**



59% of boards

have a basic or clear understanding of where their critical information and data assets are shared with third parties (e.g. suppliers)



UP from **52%** in 2013

Companies know their **KEY DATA ASSETS**

92% of boards

have a clear or acceptable understanding of the value of their companies' critical information and data assets



However... 65% of boards

rarely or never review their key information, data assets and personal data to confirm the legal, ethical and security implications of retaining them

Companies can improve their **UNDERSTANDING OF THE THREAT**

ONLY 24% of companies

based their cyber risk discussion on comprehensive or robust management information

