New research uncovers cyber security threats posed to UK's Financial Sector

Clearswift surveyed senior business decision makers from financial organisations in the UK about attitudes of businesses and employees relating to cybersecurity.

Here's what we found:

70% of financial companies suffered a cyber security incident in the last 12 months

43% Nearly half were caused by employee failure to follow company data protection policies

Other causes of security incidents:

- **32%** Introduction of malware and viruses via third party devices, including USB sticks and BYOD
- **25%** File and image downloads
- **24%** Employees sharing data with unintended recipients

32% Fear of large fines is cited as primary reason for increase in board-level involvement and/or spend on cyber security

23% Less than a quarter of UK financial companies believe their cyber security spending is at an 'adequate level'

Focus of cyber security investment:

- Data loss prevention 53%
- Database security 42%
- Regulatory compliance 40%
- Advance threat protection 40%
- Endpoint security 39%

73% of financial firms would like to see an increase in cyber security spend

"Understanding the latest data loss threats and the potential consequences from next generation attacks will help drive the business case for investment in new technology to mitigate information borne risks. Cyber security needs to rapidly evolve and the budgeting process should take this into account – the threat which can bring down a company today may not have existed three months ago."

Guy Bunker, CTO, Clearswift

clearswift
RUAG Cyber Security

www.clearswift.com

Statistics in this infographic come from a survey conducted by technical research firm Vanson Bourne on behalf of Clearswift in August 2019.