The intelligence disconnect
The 2017 Cyber Defence Monitor: A global perspective

The study shows on surprising disparity between the views of C-suite respondents and those of IT Decision Makers.

Who's responsible in the event of an attack?

- **35% of C-SUITE** say the IT team is responsible
- **50% of ITDMs** think senior management are responsible

- **55% of board members** think that spending on cyber security will increase, and **82% of ITDMs** believe it is part of a comprehensive strategy.
- **Only half the board members** feel spending is part of strategy and **41% of ITDMs** believe spending in cyber security to be more ad-hoc.

$19.2 million
The cost of a successful attack, according to ITDMs.

$11.6 million
The cost of a successful cyber attack, according to C-Suite respondents.

- **75% of C-Suite** believe the number of cyber attacks will increase
- **78%**
- **84% of Board members** and **81% of IT teams** are confident that they have the right protection in place to defend against a cyber attack.

68% of ITDMs believe the number of cyber attacks will increase.

Copyright © BAE Systems plc 2017. All rights reserved. BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No.03785) with its registered office at Surrey Research Park, Guildford, England. G12 7HQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.