BT DDoS Research
Summary

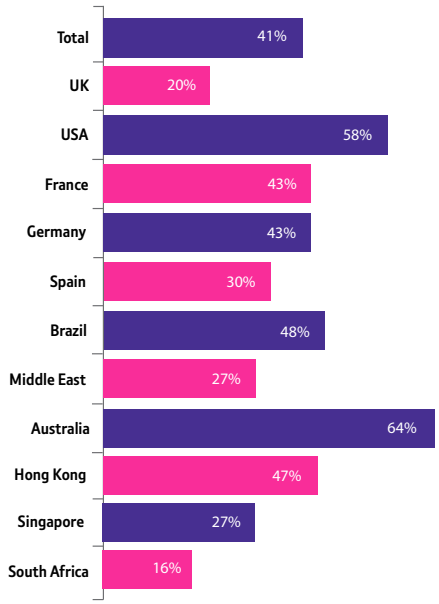
Based on 640 interviews with IT decision-makers in large organisations (1000 plus employees) across eleven countries – UK, France, Germany, USA, Spain, Brazil, Middle East, Hong Kong, Singapore, South Africa and Australia – and in a range of sectors -including finance, retail and public sector - this research explores attitudes and levels of preparedness of towards distributed denial of service (DDoS) attacks

The research provides an insight into the rapidly evolving DDoS threat landscape and reveals the extent to which DDoS attacks have already impacted organisations and their customers worldwide. With the growing challenge this is posing to organisations across the globe, it appears that this once niche IT issue has become a legitimate and serious business concern.

Organisations say DDoS attacks are getting better at bypassing IT defences

- Two-in-five organisations (41 per cent) were targeted by DDoS attacks last year.
- Of those, three quarters (78 per cent) were targeted twice or more in the year.
- While some regions such as UK (20 per cent) and South Africa (16 per cent) saw fewer attacks, more than half of organisations in the US (58 per cent) and Australia (64 per cent) were targeted.

Has your organisation's systems been targeted by a DDoS attack(s) in the last 12 months?

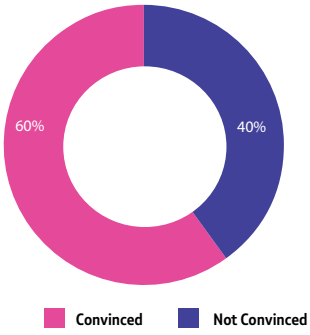


- Two-thirds (64 per cent) of attacks were multi-vector attacks. This figure increases to 75 per cent in US, Brazil and Australia – but falls to half or less in the Middle East, South Africa and UK.
- Across the board, more than half of IT decision makers worldwide think DDoS attacks are becoming increasingly effective at subverting IT security measures.

Response plans and appropriate resourcing important – but lacking

- Four in ten IT decision makers are not convinced that their organisation has a response plan in place in to counteract DDoS attacks

To what extent do you agree that your company has a response plan in place should a DDoS attack occur?



- Despite this, more than half of respondents (59 per cent) think that DDoS attacks are becoming increasingly effective at subverting their IT security measures
- 80 per cent are not convinced that their organisation allocates sufficient resource to counteract these attacks
- Combined, this has contributed towards 58 per cent of organisations identifying DDoS as a key concern to their organisation
- On average, organisations review their crisis response plans to DDoS attacks every 16 months.

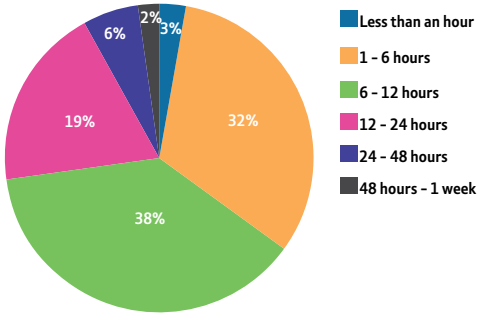
Impact of DDoS on organisations

- Unsurprisingly, almost every respondent IT decision maker (96 per cent globally) reported an increase in customer complaints when their network systems went down after a DDOS attack.
- On average, customer queries jumped 36 per cent following an attack. Although in almost a quarter of cases, complaints jumped by at least 50 per cent.

BT DDoS Research
Summary

- Organisations take 12 hours, on average, to recover from a DDoS attack.
- Two thirds of IT decision makers say their systems were downed for more than six hours – almost a full working day – before returning to fully operating capacity.

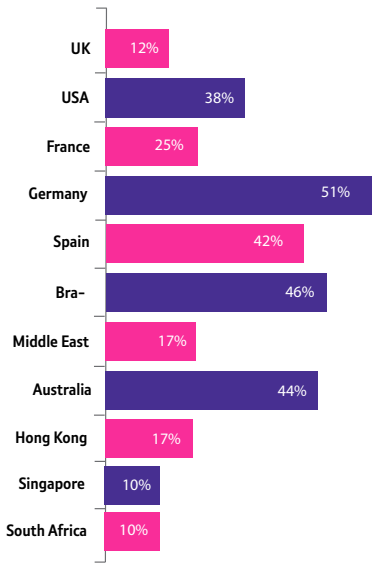
How long after the DDoS attack(s) you experienced in the last 12 months was it before your organisation's systems were operating at optimal performance again?



Board level attitudes to DDoS

- The research suggests that CEOs have a good understanding of the threat DDoS poses to their organisation – although this varies by region.
- Globally, two-thirds of IT decision makers say their CEO takes the threat of DDoS seriously.
- Further, one-in-three IT decision makers believe that their CEO has an in-depth understanding of DDoS and the risk it poses.
- These figures vary significantly by region, with just 12% of IDTMs in UK saying their CEO has an in-depth understanding, versus more than half (51 per cent) in Germany.

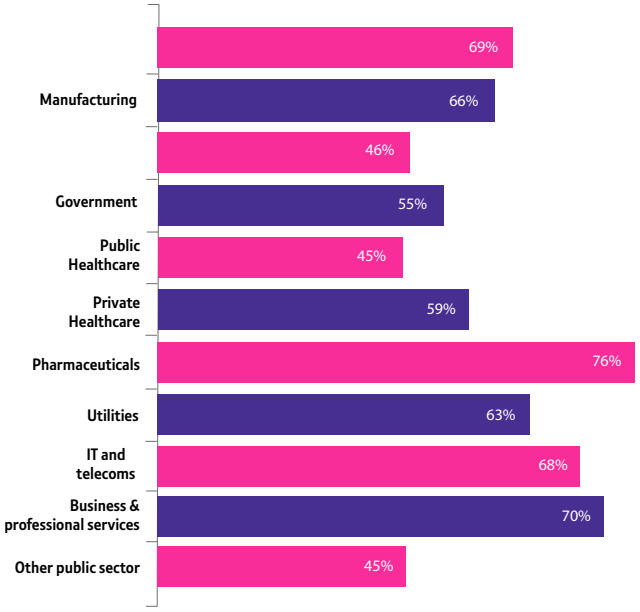
What level of understanding does your CEO have about what a DDoS attack is?



Some sector insights

- The majority of business & professional services (70 per cent), pharmaceutical (76 per cent) and financial services organisations (69 per cent) have a response plan in place should a DDoS attack occur.
- At the other end of the spectrum, less than half of retailers (46 per cent), public healthcare (45 per cent) and other public sector organisations (45 per cent) have response plans in place. (INSERT GRAPH 5 – combining all sectors)

What level of understanding does your CEO have about what a DDoS attack is?



Some sector insights

- When it comes to having the adequate resources in place to subvert an attack, again financial services organisations are ahead of the curve (74 per cent say they have the resources available).
- Meanwhile, more than half of retail and public sector ITDMs say they do not have the right resources in place (just 56 and 54 per cent respectively)
- Two-thirds (67 per cent) of pharmaceutical company IT managers say that DDoS attacks are one of the biggest threats to their organisations IT systems.
- Public sector IT managers believe that their CEOs are least likely understand DDoS and the threat it posses to their organisation – just 19 per cent say their CEO has an in-depth understanding.
- Similarly, public sector IT managers reveal that they only review their crisis plan every 19 months – 20 months for Government departments.
- Likewise, less than a third of public sector organisations can even identify if an attack occurs, with a further 37 per cent unsure if they could detect one.
- Unsurprisingly, the majority of sectors believe DDoS poses the greatest threat to their security through the website.

To learn more about this research and find out how BT is working with customers to ensure they are fully protected against threats, visit www.bt.com/btassure