

DDoS Attacks in the United Kingdom

2012 Annual Trends and Impact Survey



CONTENTS

Survey Findings, 2012–2011

Survey Methodology	3
Frequency of Attacks	3
Financial Impact	4
Attack Size	5
Length of Attacks	5
DDoS Protection Used	6
Conclusions	6

Introduction

In both 2011 and 2012, Neustar reported on the **DDoS attack landscape in North America**. This year, we also surveyed IT pros in the United Kingdom on the growth of attacks and their impact in 2012, as well as the types of DDoS protection organisations use. How severe was the danger? Does it differ between industries? What were the costs of downtime? Are companies prepared to protect their websites and their reputations?

In comparing threats to readiness, the answers are not encouraging.

UK DDoS Survey Findings Summary

When DDoS attacks hit, organisations are thrown into crisis mode. From the IT department to call centres, to the board room and beyond, it's all hands on deck until the danger passes. In April 2013, Neustar surveyed IT professionals across the United Kingdom to understand the impact of DDoS attacks and how companies are managing the crisis. Most respondents self-identified as working in IT, security, compliance or management roles. A total of 381 respondents shared details about attacks, defenses and financial losses. Of this group, 121 worked for ecommerce companies whose success depends on selling products or services online.

This report provides the UK results and compares the UK-specific responses to the April 2012 North American survey findings, detailed in Neustar's report "Hope is Not a Strategy." The 2012 findings outline the costs of DDoS attacks, how companies are responding to threats and the unique challenges for companies conducting ecommerce.

Key questions asked include:

- Who has been attacked and who hasn't?
- What are the costs of DDoS outages?
- How long have attacks lasted?
- What types of DDoS protection are people using?
- What are the sizes of DDoS attacks?

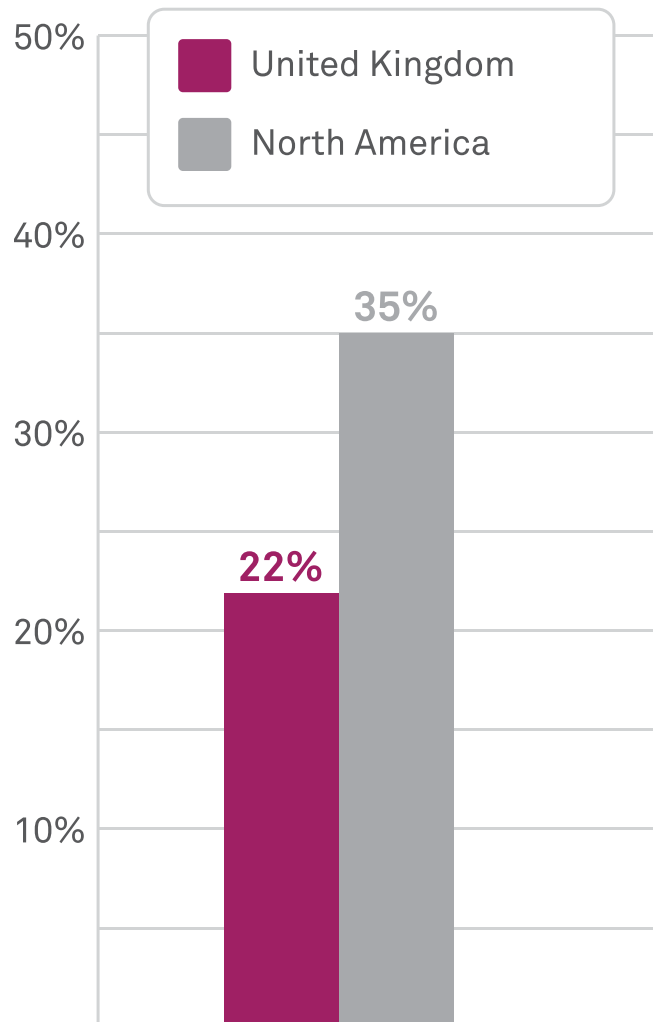
The survey also examined the operational impacts associated with DDoS attacks:

- How many people per organisation are involved in DDoS responses?
- What areas of operation experienced the greatest cost increases in a DDoS attack?

Have you experienced a DDoS attack?

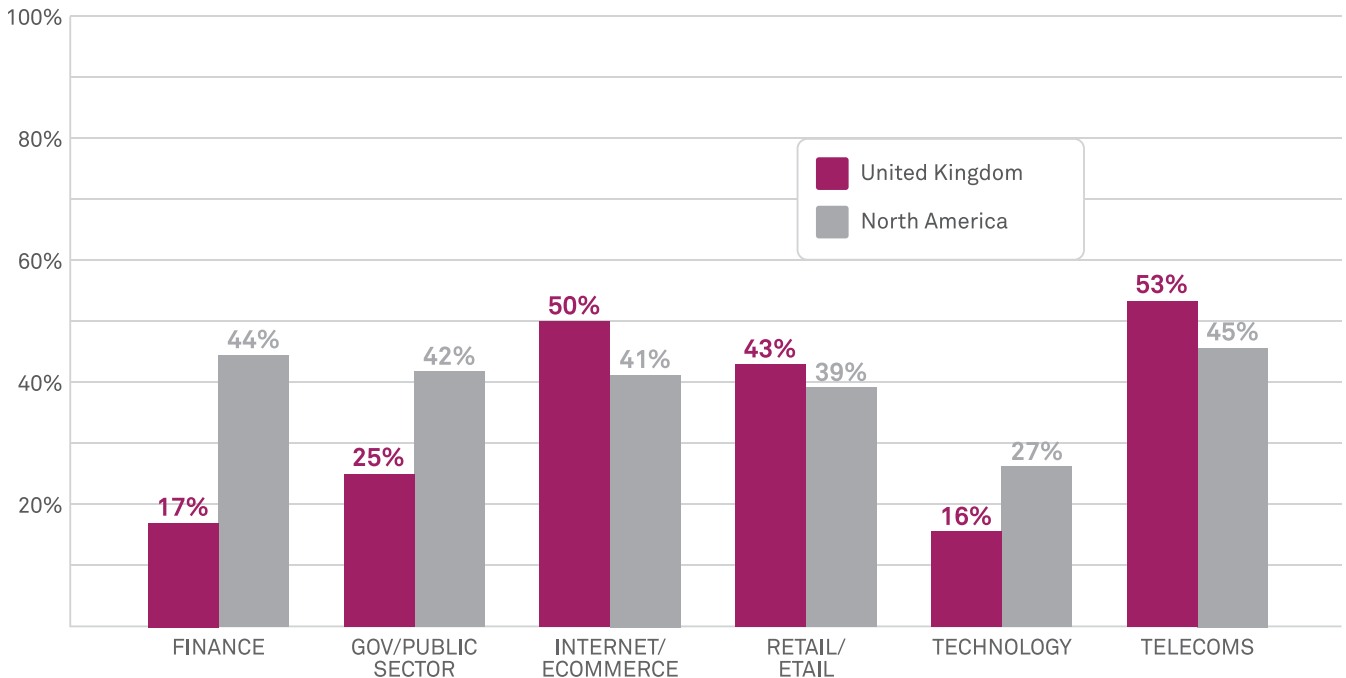
22% of UK companies surveyed experienced a disruptive attack in 2012, compared to 35% of respondents in the North American survey. The breakdown of attacks by industry was consistent with other survey results.

22% UK vs. 35% NA Organisations Experienced a DDoS Attack



Attacks were higher in North America due in large part to the unprecedented wave of DDoS against major American banks.

Companies Attacked by Industry



Industry Breakdown

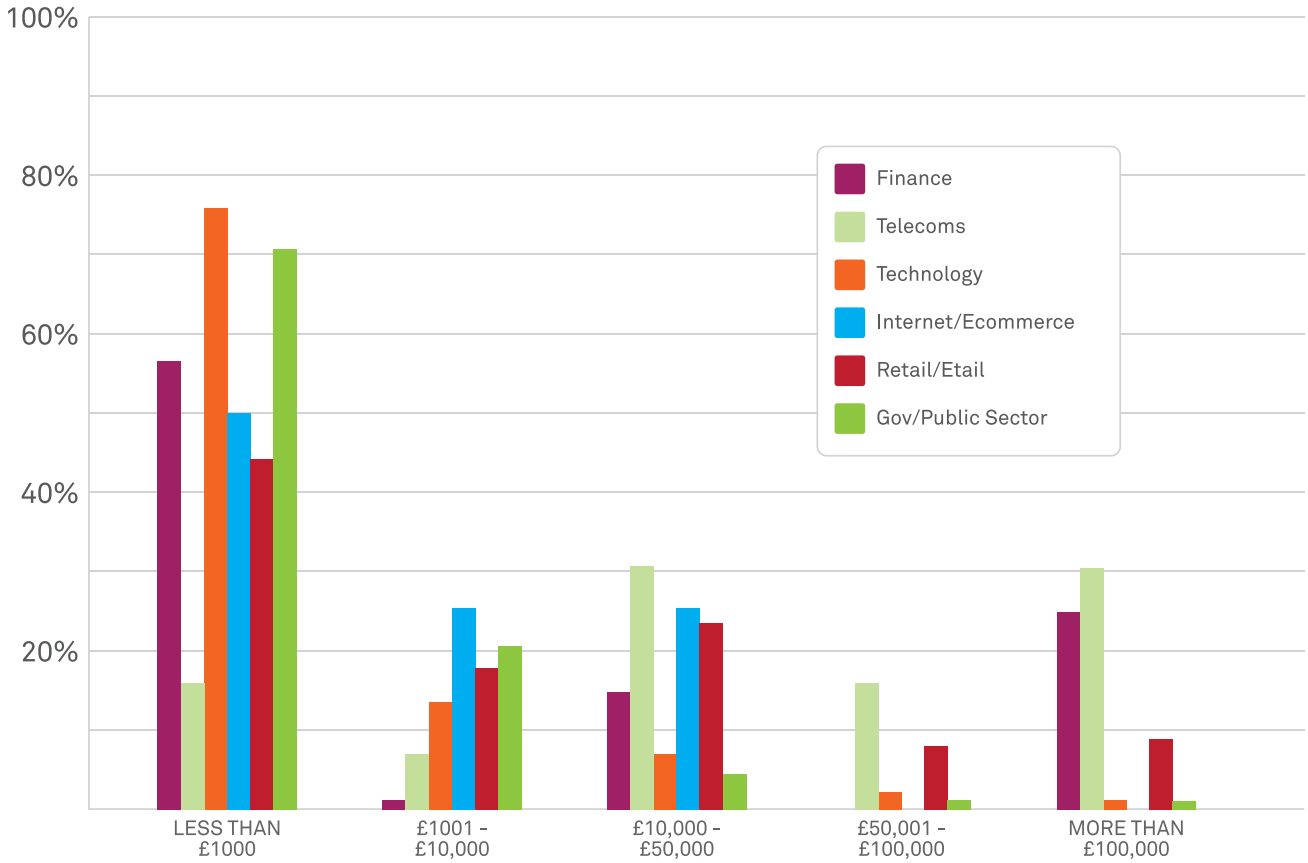
Within key industries, the risk of attack varies. Among those companies that were attacked, a high percentage of respondents were in telecommunications (53%), Internet-ecommerce (50%) and online retail (43%). In contrast, the North American survey showed a higher percentage of targets in finance and government.

Among North American respondents, 44% of financial companies reported being attacked, versus just 17% in the United Kingdom. The attacks on US banks by Al Qassam are likely the reason for the disparity; massive attacks were staged from September 2012–April 2013. These attacks have opened the doors for others to mimic the tactics, such as the DDoS attacks against Dutch banking systems in April 2013.

What is the financial impact of a DDoS attack?

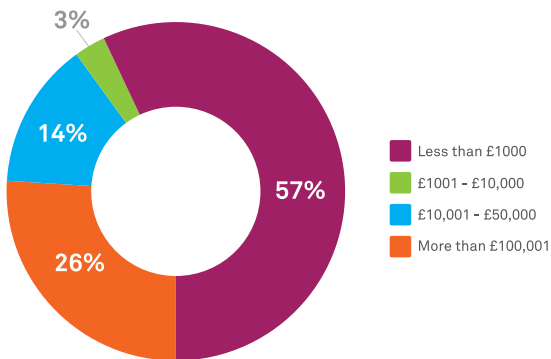
A DDoS attack can inflict a grave toll on revenues. Overall, the survey results varied in showing financial impact, especially when broken down by industry. But to put things in perspective, an outage costing even £1000 per hour would be expensive for a small e-tail site. The industries with the highest losses from an outage were financial services and telecommunications companies.

Revenue Risk Per Hour of Downtime by Industry



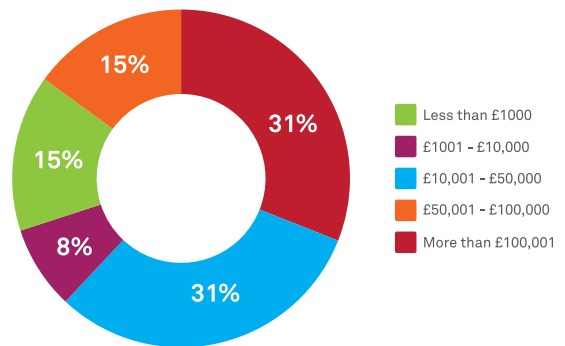
Financial services and telecom had the highest revenue risks.

Financial Service Revenue Risks Per Hour of Downtime



Over £100,001 Per Hour: 1 in 4 Institutions

Telecom Revenue Risks Per Hour of Downtime



Over £100,001 Per Hour: Nearly 1 in 3 Companies

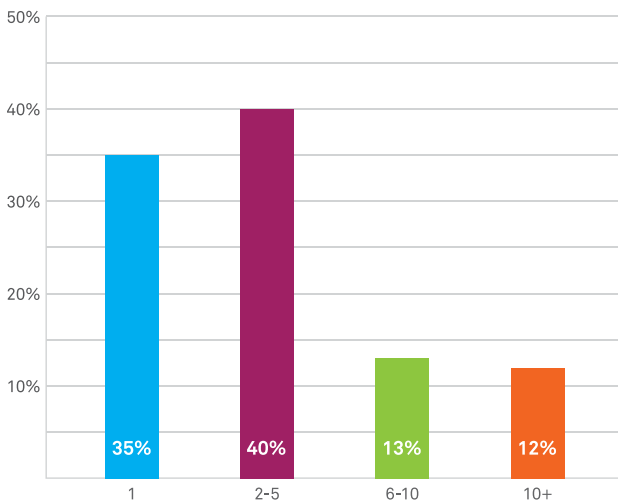
What is the broader impact of DDoS attacks?

DDoS attacks do damage that goes beyond revenue loss. Brand value erodes, along with public reputation and customer trust. If not fixed fast, short-term problems turn into lasting PR issues. For example, customers unsuccessfully trying to buy shoes online are left wondering what happened to their purchases. Did they complete the process? Are their credit card numbers safe? Soon, call centers are flooded with questions and hold times increase. A positive shopping experience becomes a stream of loud complaints. Some customers are forgiving, but certainly not all.

To identify the costs related to DDoS protection, including those specifically associated with attacks, the 2012 survey asked several new questions. The first addressed staffing levels for attack mitigation.

How many people are involved in mitigation?

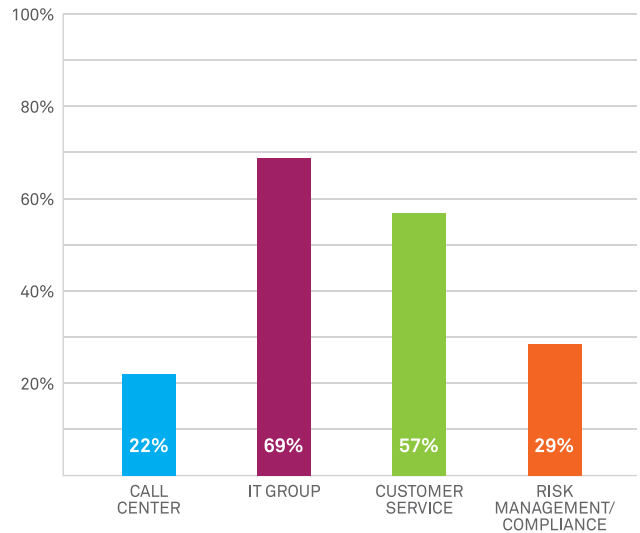
Overall, companies reported that 40% of attacks involved 2 to 5 people in mitigation; 25% required more than 6 people, similar results to the North American survey.



Number of People Involved in a DDoS Mitigation

The survey also asked respondents to identify the two areas of their organisation with the greatest increase in operational costs related to a DDoS attack. The IT group was the leading area at 69%, with customer service second at 57%.

Areas of Greatest Cost Increases in a DDoS Attack



How big were attacks in 2012?

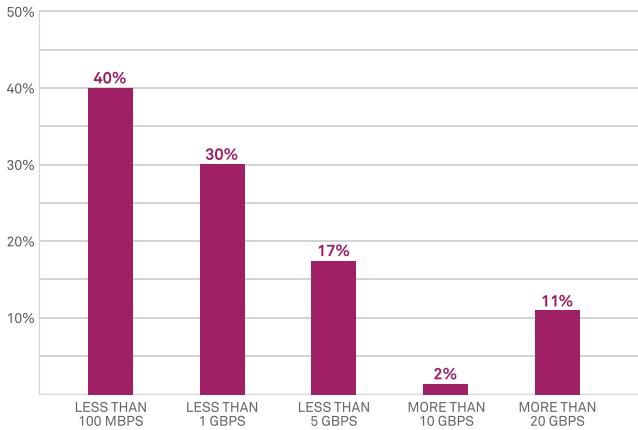
Some DDoS attacks today are massive – like nothing seen before. These high-bandwidth attacks use compromised commercial servers versus personal computers, allowing attackers to harness unprecedented system and network resources. This method is also used to launch high-packet rate attacks, which aim to exhaust purpose-built DDoS protection hardware.

While the large attacks make headlines, industry experts agree that a well-crafted, multi-vector attack as small as 2Gbps, a common attack size, can take down a site.

According to a 31 May article published in Techweek Europe (“Europe Sees ‘Extraordinary’ Spike in DDoS Attack Power”), “Attacks over 10Gbps in EMEA were up 23 percent from between 2011 and 2012, but already in 2013 it’s up 82 percent. So far this year, the average size of attacks has increased 84 percent, from 1.06Gbps in all of 2012 to 1.95Gbps in Q1 of 2013.”

Any attack, including Layer 7 application attacks which make up 25% of attacks today, can be measured in terms of bandwidth. Following is a breakdown of UK attacks by bandwidth size.

UK Attack Size Measured in Bandwidth

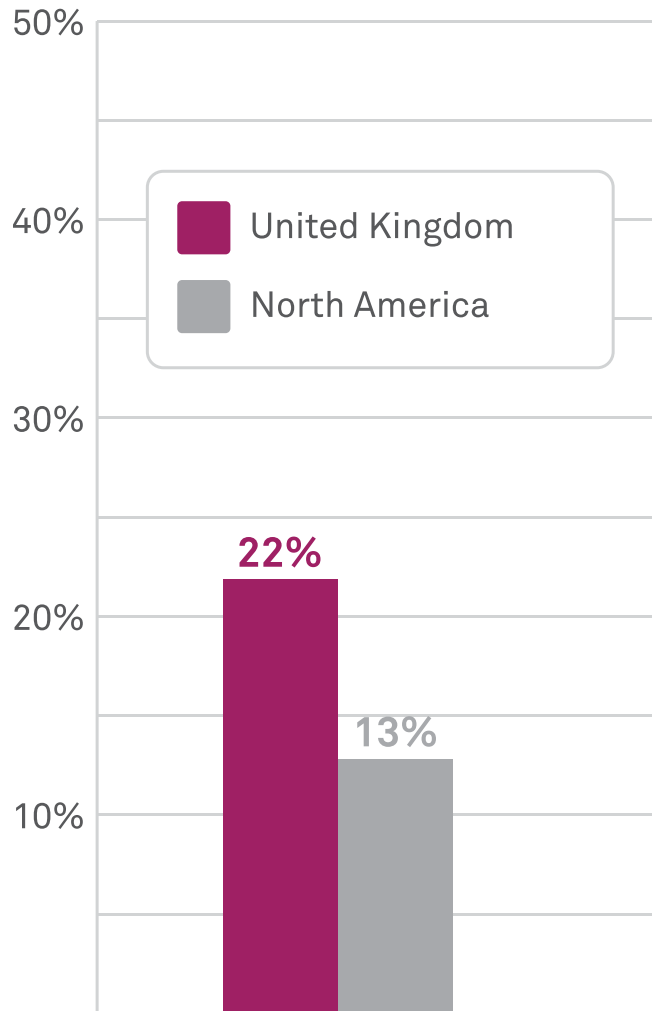


THERE'S BIG AND THERE'S BIG.

In early 2013, there were news reports of massive, high-profile DDoS attacks. The attack that shut down Spamhaus, the well-known spam tracker, was reportedly measured at 300+ Gbps. Some attacks on major banks may have reached over 160 Gbps.

But while industry reports estimate that DDoS attacks increased in size an average of 27 percent – from 1.23 Gbps in 2011 to 1.56 Gbps in June 2012 – successful attacks typically use less than 1 Gbps per second. That's all it takes to bring a website down.

Attacks Lasting Over a Week – 22% UK vs. 13% NA

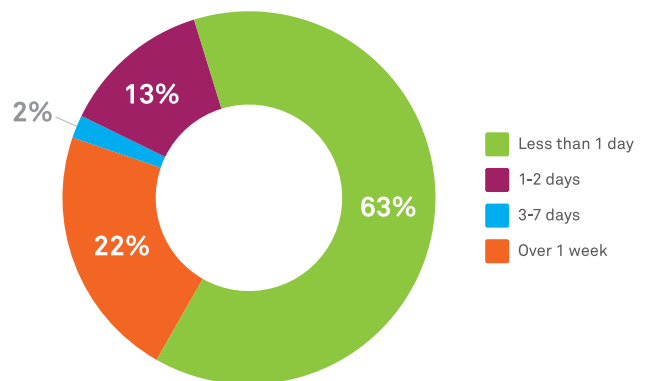


How long did attacks last?

Tracking with the North American results, over a third (37%) of all DDoS attacks in the UK lasted more than 24 hours

Some attacks stretched out for several days or longer. In fact, 24% of attacks lasted between 3 days and 7+ days. The longest attacks, those lasting over a week, were a significantly higher at 22% compared to only 13% from the North American survey.

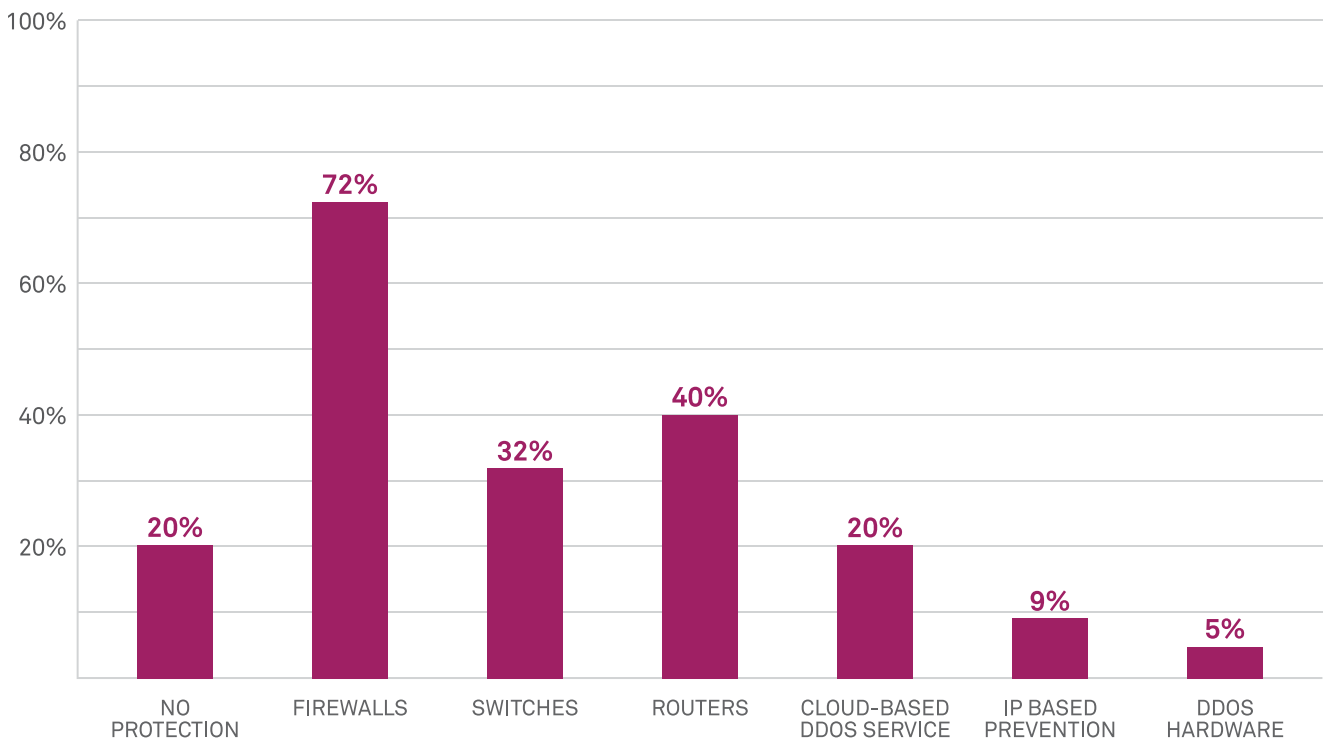
Duration of Attacks in the UK



What kind of DDoS protection was used?

A full 20% of responding UK companies reported having no DDoS protection in place. There is a high reliance on devices not built to mitigate DDoS attacks, with switches, routers and firewalls utilized most often.

Types of DDoS Protection Used



Products and Services Used for DDoS Protection

While it seems as if many companies are covered, it's important to note the distinction between network protection solutions and DDoS protection solutions. Firewalls, routers and switches can protect against intrusive attacks at Layer 3 (to some extent) but compound the effects of DDoS attacks by allowing malicious traffic to reach networks and bottlenecking traffic. Attacks often target both the network and application layers, with Layer 7 attacks accounting for more than 25% of attacks. Routers are not effective against Layer 7 application attacks.

More respondents used on-premise hardware to mitigate attacks in 2012. Larger organisations with specialised IT staff are best equipped to do this.

“For those organizations that determine they are most at risk and have made the decision to invest budget in a comprehensive DDoS strategy, IDC finds it should include the following: A mix of on-premise and cloud monitoring and mitigation managed internally or externally or a combination of the two.”

— IDC Worldwide DDoS Prevention Products and Services 2013-2017 Forecast, doc #239954, March 2013

Intrusion detection systems are used by 20% of respondents as DDoS protection when, in fact, like a firewall, an IDS becomes a bottleneck during attacks. It can, however, help defend against growing two-pronged attacks, in which DDoS is a distraction while the attacker breaches the system, aiming to steal customer data, government secrets or intellectual property.

Survey Conclusions

Anyone following industry news knows DDoS attacks are worse than ever. They have become the cyber-attacker's preferred method to create disruption, distract from other crimes or promote a cause. Owing to the barrage against US banks and attacks in other sectors, the topic of DDoS has moved from the IT department to the board room. Neustar's survey of UK-based organisations reflects these trends in a number of ways:

- In high-risk sectors, approximately 48% of companies reported being attacked, including retail and ecommerce and telecom.
- The potential cost of DDoS attacks continues to be a concern, with some downtime costs estimated at higher than £100K per hour.
- Aggravating financial risk: UK attacks tended to be longer than in North America, with 22% lasting over a week.
- DDoS increases the cost of business operations, particularly among IT and customer service departments.
- Though DDoS is a growing concern, 20% of companies surveyed do not have DDoS protection and 72% rely on inadequate devices like firewalls. The good news is that 25% of organisations reported using purpose-built DDoS equipment or cloud-based services.

As in North America, UK companies face serious challenges as they decide on DDoS protection and attempt to mitigate losses. While many companies are hoping traditional defenses will suffice, given the frequency of attacks, their growing complexity and the impact when sites go dark, such hopes are badly misplaced.

Neustar SiteProtect

Neustar SiteProtect offers intelligent **DDoS protection**, blending the people, processes and technologies to stop today's complex attacks. Using battle-tested procedures and best-of-breed equipment, the experts in the Neustar Security Operations Center work swiftly to eliminate downtime and protect your brand.

Based in the cloud, SiteProtect offers 24/7 **on-demand traffic scrubbing**. Immediately accessible through DNS or BGP re-direction, it provides instant relief from DDoS attacks involving network Layer 3, application Layer 7, IPv6 and/or encrypted traffic – or any combination of these takedown methods. SiteProtect reroutes traffic to unclog your network, filters malicious traffic and permits valid traffic to return to your infrastructure.

Built on a dedicated, globally distributed Anycast network, SiteProtect can be instantly deployed and remains activated until the danger is gone. With SiteProtect handling the DDoS, your responses remain nimble and in sync with customer requests. Online business continues even as the attack unfolds.

For larger organisations, SiteProtect is an ideal complement to in-house mitigation hardware. As a cloud-based failover solution, SiteProtect provides the bandwidth to absorb malicious traffic and enables you to launch counter-measures in real time. Using a hybrid approach, you can leverage your investments in DDoS detection and alerting, avoid outages and minimise disruptions.

When it comes to DDoS protection, we've got you covered. Learn more at www.neustar.biz/ddos.

FOR MORE INFORMATION

Online www.neustar.biz/ddos

Email Euroinfo@neustar.biz

Phone **+44 (0) 1784 448 444**

About Neustar

Neustar, Inc., (NYSE: NSR) is a trusted, neutral provider of real-time information and analysis to the Internet, telecommunications, technology, financial services, retail, media and advertising sectors.

Neustar applies its advanced, secure technologies in location, identification, and evaluation to help its customers promote and protect their businesses.

More information is available at www.neustar.biz.

Neustar Ltd:
Venture House
42-54 London Rd
Staines
TW18 4HF
United Kingdom
www.neustar.biz
©2013 Neustar, Inc. All rights reserved.

ES-WP-DDoS-008UK-v071513

neustar[®]
Real Intelligence. Better Decisions.