KASPERSKY lab

GLOBAL IT SECURITY RISKS SURVEY 2014 – DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS

Table of Contents

THE MAIN FINDINGS

Costs and Consequences of DDoS Attacks

- The survey found that DDoS attacks cost small-to-medium-sized businesses (SMBs) an average of $52,000 per incident. For larger enterprises, the cost of a DDoS attack is even larger, resulting in an average of $444,000 in lost business and IT spending.
- These costs include all short-term and long-term responses to a DDoS attack. The most commonly-reported consequences of a DDoS attack include “hiring IT security consultants” (65%); “temporary loss of access to business-critical information” (61%), and “reactive spending on software or infrastructure” (49%).
- Another long-term cost of a DDoS attack is damage to a company’s reputation. 38% of businesses believe that a DDoS attack damaged their company’s reputation. 29% reported that a DDoS attack damaged their credit rating, and 26% reported an increase in their insurance premiums.
- During a DDoS attack, “Significant increases in page-load times” (52%) was the most commonly reported effect of a DDoS attack, with “slight increase in page load times” reported by 33% of victims. More severe outcomes of DDoS attacks included transaction failures in 29% of cases, and complete disruption/complete unavailability of service in 13% of cases.
- The most common types of disruptions of a DDoS attack – “significant” and “slight” page load times – were typically resolved in one-to-several hours. But 20% of victims were afflicted by “significant” page load delays that took more than a day to resolve, leading to massive losses of potential business.

Regions and Businesses Most Often Targeted by DDoS Attacks

- Businesses that provide online public-facing services are the most likely to be targeted by DDoS attacks. 38% of businesses in this category reported a DDoS attack within the previous year, compared to 18% of all businesses reporting a DDoS attack in the same period.
- The six business sectors within this “online service provider/financial company” category which are most highly-targeted by DDoS attacks are:
  - IT/Technology (49%)
  - E-commerce and Telecom (both 44%)
  - Media (42%)
  - Construction/Engineering (40%)
  - Finance (39%)
- When filtering attack rates in this “online service provider/financial company” category by geographical location, the survey found that businesses in China reported the highest regional rate of DDoS attacks (62%), with Russia next at 49%.

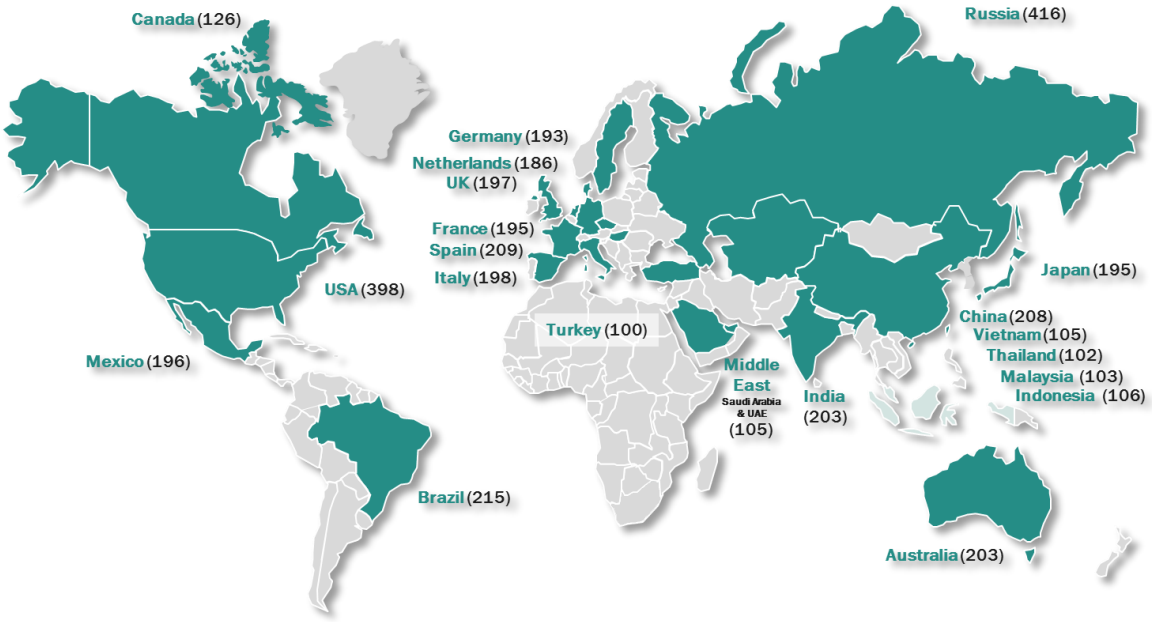
Levels of Concern and Anti-DDoS Solution Usage

- Preventing DDoS attacks (i.e. “ensuring continuity of service for business-critical systems”) was reported as a top priority for the IT department by 23% of businesses. Surprisingly, the E-commerce/Online Retail sector gave this the lowest rating of all business sectors (19%).

- On average, 61% of businesses felt it was the responsibility of their own IT department and management teams to defend themselves against DDoS attacks. 21% believed it was the responsibility of the network service provider or the website/hosting provider. Large businesses were much more likely to rely on internal resources, whereas small businesses were more likely to expect help from these external service providers.

- Overall, 50% of all businesses agree that specialized countermeasures against DDoS attacks are an important security requirement. The two business segments that feel the strongest about the importance of DDoS countermeasures are the Financial Services and Utilities & Energy sectors (both at 60%).

METHODOLOGY



A total of 3,900 respondents from 27 countries – including representatives from companies of all sizes – took part in this year's survey. The survey was bigger than last year's, both in total size and global scope (the 2013 survey included 2,900 respondents in 24 countries). More than 54% of the participants were mid-sized, large and very large companies. Approximately 17% of the respondents were corporations in the Large Enterprise segment (from 5,000 to 50,000 employees), while 12% of the survey participants were in the Large-Medium category (1,500 to 5,000 employees). About 25% of the survey participants were companies with anywhere from 250 to 1,500 employees, and the remaining respondents represented small and very small businesses.

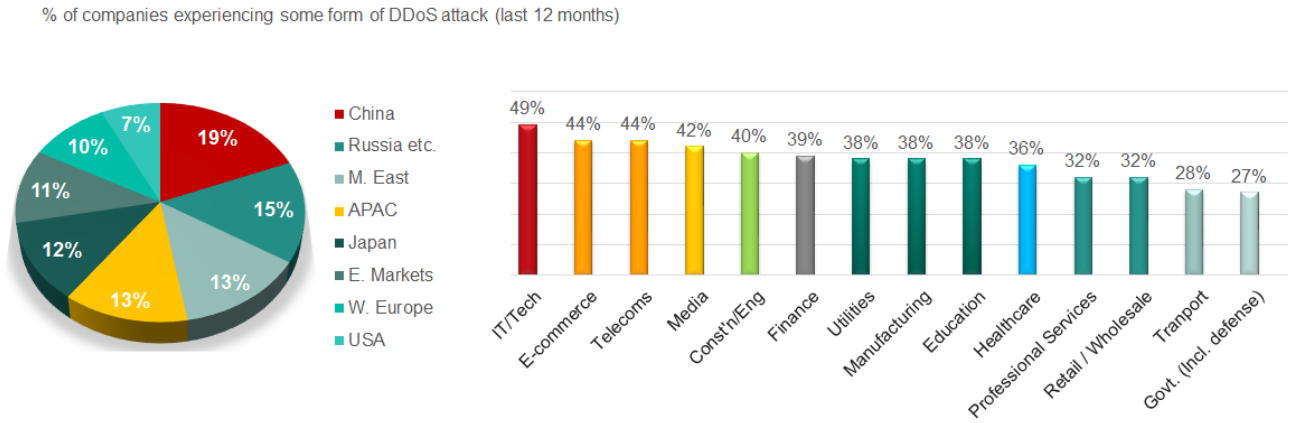
All of the companies that took part in the survey answered dozens of questions concerning the main obstacles that both the company's general management and IT management face, specifically when building and maintaining a reliable, smooth-running IT infrastructure. Additionally, respondents answered questions about the resources allocated by their companies for tackling IT problems, including data security problems. The survey questions asked respondents about business conditions over the preceding 12 months, from April 2013 through May 2014.

DDOS ATTACK FREQUENCEY

More than **one-third (38%) of businesses which provide financial services or operate public-facing online services*** have experienced a DDoS attack from April 2013 – May 2014. These web-facing organizations, which depend on 24/7 client web access to run their businesses, are prime targets for these disruptive attacks which can cost hundreds of thousands of dollars in damage from missed business opportunities, lost reputation, and IT incident response costs.

As illustrated, the rate of DDoS attacks in the previous year reported by survey respondents varied greatly depending on industry and region. Chinese IT departments reported an extremely high rate of DDoS attacks (62%), almost double what was reported by businesses in Western Europe (32%). When looking at specific industries, e-commerce (44%) and finance (39%) were at the high-end of the spectrum, but businesses in the IT/technology sector were targeted the most, with 49% reporting a DDoS incident in the previous year.

(* *note: the chart below reflects this specific subset of businesses: financial services or companies operating online, public-facing services*)



REGION INDUSTRY

DDoS attacks aren't limited to just financial services firms, or companies with public-facing services, however. Overall, almost 1 in 5 (18%) of businesses experienced a DDoS attack within the year-long timeframe. The graphics below show the frequency of DDoS attacks against all survey respondents, divided by region and business sector.

EXTERNAL THREATS EXPERIENCED

	Globally	Russia etc.	China	N. America	W. Europe	E. Markets	APAC	Mid-East	Japan
Dental of Service (DoS), Distributed denial-of-service attacks (DDoS)	18%	17%	34%	15%	17%	17%	20%	22%	13%

This larger sample size confirms that businesses from China reported a much higher level of DDoS attacks than other regions. Also, the data shows that Russian financial services and public-facing web services are 32% more likely to be targeted by DDoS attacks than Russia's "non-public-facing" business counterparts, the greatest divergence amongst the regions.

The IT/Software and Telecom sectors still rank highly in their reported rate of DDoS attacks. In general, this data illustrates that although businesses and service providers with public-facing web services are targeted by DDoS attacks more frequently, these attacks are not exclusive to companies with public-facing services.

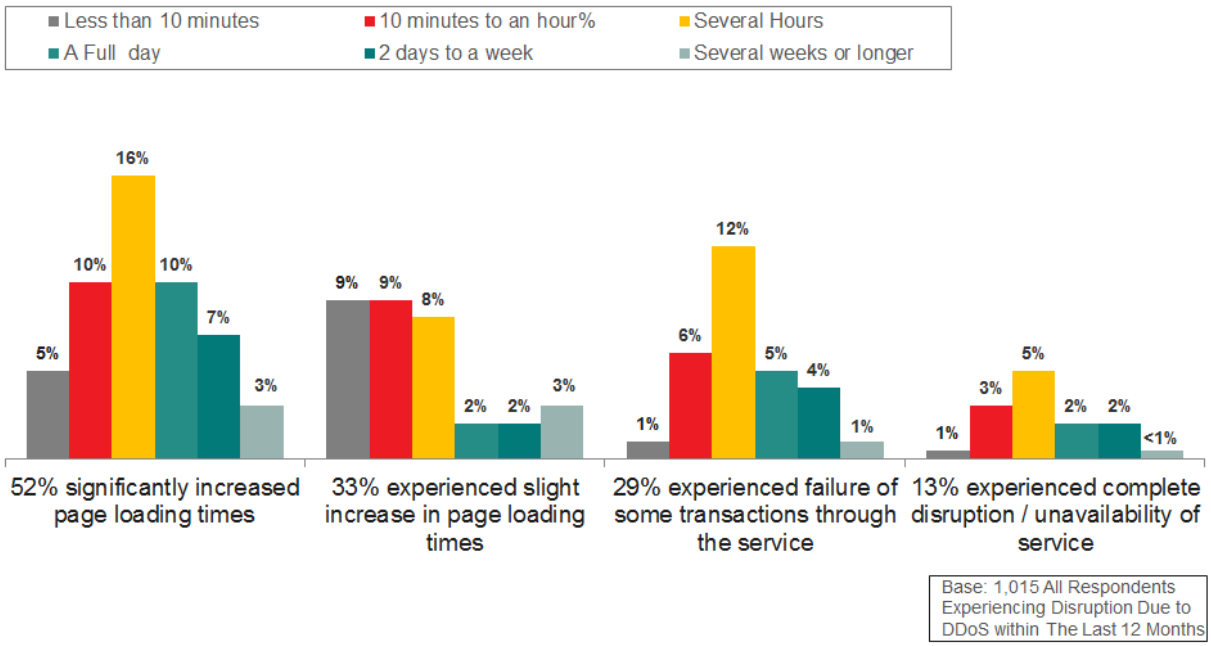
EXTERNAL THREATS EXPERIENCED

	Manufacturing	IT/ Software Etc.	Financial Services	Business Services	Construction/ Engineering	Government /Defence	Education	Healthcare /Services	Consumer Services	Other	Transportation /Logistics	Telecoms	Real-Estate	Utilities & Energy	Media /Design	Non-Profit /Charitable	E-commerce /Online Retail
DoS/DDoS	15%	27%	20%	18%	13%	12%	19%	23%	16%	12%	14%	29%	20%	25%	16%	13%	21%

A DDoS attack can have a range of negative effects while the incident is underway and can have a lasting impact on the business once the attack is over. Of all businesses that had suffered a DDoS attack, 52% reported "significant" delays in page loading times, and 33% reported "slight" delays. DDoS attacks caused transaction failures in 29% of cases, and caused complete disruption/complete unavailability of service in 13% of cases. That means nearly half of businesses affected by a DDoS attack were completely unable to generate revenue while the attack was going on.

Which prompts the question: "how long does a DDoS attack last?"

DURATION OF DISRUPTION



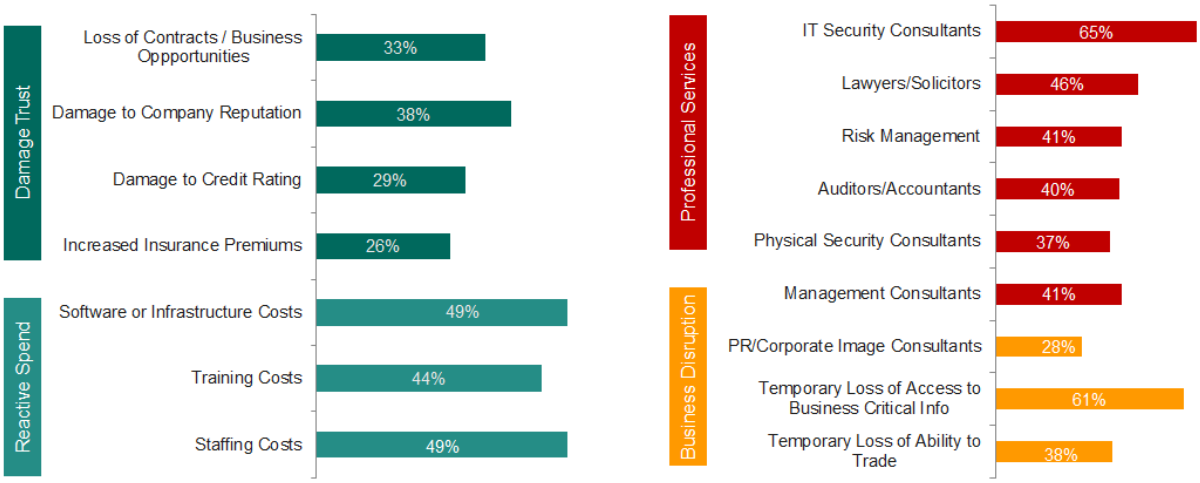
The most severe level of disruption, “complete unavailability,” was typically felt for the shortest duration of time. Of the 13% of businesses that experienced this catastrophic level of attack, 8% had at least partial functionality of their service restored after in “several hours” or less.

The remaining 5%, however, were completely offline for at least a full day, and a few for up to several weeks! The most common effect of a DDoS attack (“significantly increases page loading times,” experienced by 52% of DDoS victims) were most often resolved in less than a day, with 26% requiring “10 minutes to several hours” to mitigate. But once again, 20% of unlucky (or unprepared) businesses suffered from significantly increased page loading for several days, and even several weeks.

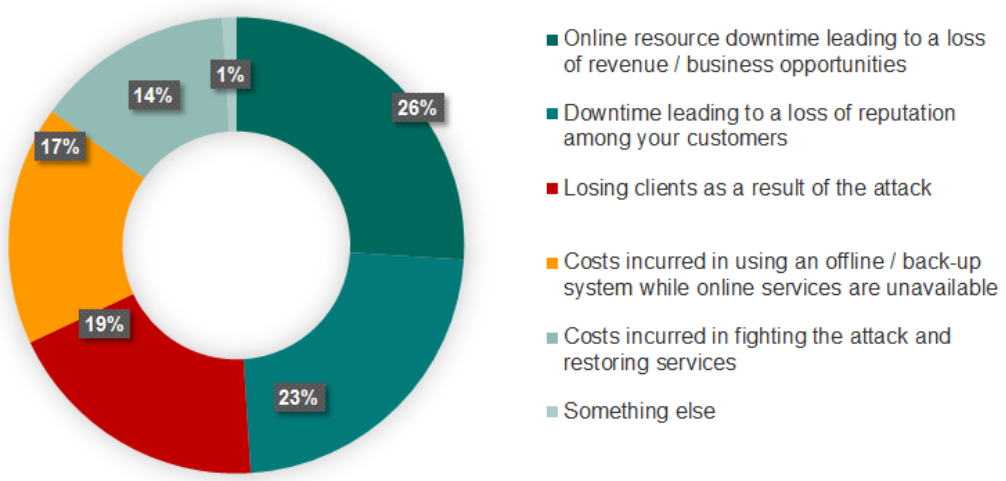
FINANCIAL AND REPUTATIONAL IMPACT

While it's clear that the frequency, duration, and severity of DDoS attacks can vary widely, it is certain that these disruptions of service usually prompt large financial outlays, as well as damaging a business's reputation and long-term prospects. The survey results found that a **DDoS attack cost small-to-medium-sized businesses (SMBs) an average of $52,000 per incident**, including all lost business and reactive IT spending. **For larger enterprises, a DDoS attack resulted in an average of $444,000 in lost business and IT spending.**

The types of damage experienced are broad, and some are more difficult to quantify than others. The illustration below shows how DDoS victims reported costs from a number of different categories, including "Reactive Spend" and "Professional Services" (easier to quantify), as well as "Damaged Trust" and "Business Disruption" (more difficult). But regardless of how measureable the damage, it's clear that DDoS attacks leave an expensive mess behind in their wake.



It is interesting to compare the outcomes reported with the potential outcomes that IT managers fear the most. The two "most feared" consequences – regarding loss of revenue opportunities and loss of customer trust – are in fact two of the most common outcomes of DDoS attacks:

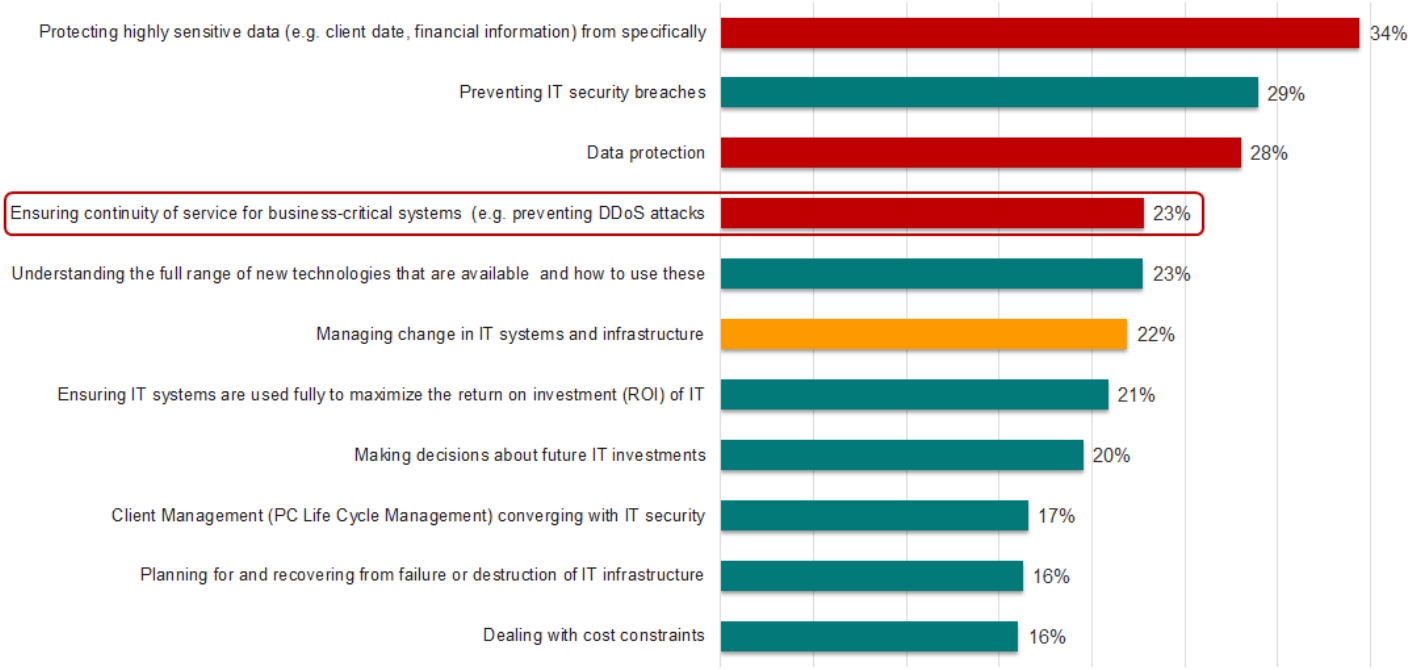


BUSINESS CONCERNS AND RESPONSIBILITIES

It should come as no surprise that when asked to name the "top three concerns of the IT department," keeping systems online and protected against DDoS attacks rated very highly. "Preventing DDoS attacks" was listed as top priority by 23% of respondents, the fourth-highest rating, and ahead of other key IT functions.

TOP CONCERNS OF THE IT FUNCTION

DATA PROTECTION ISSUES AND ANTI-DDOS ARE AMONGST THE TOP CONCERNS FOR THE IT FUNCTION



When examining the responses to this question based in different business sectors, the responses are mostly consistently in the mid-20% range, with a couple notable exceptions**: the e-Commerce/Online Retail segment ranked "ensuring continuity of service" the lowest of all business sectors** at 19%, which is strange given that their entire business model depends on being able to process online transactions.

There were some surprises when examining the responses to this question from a geographical perspective as well.

TOP CONCERNS OF THE IT FUNCTION BY REGION

	Globally	Russia etc.	China	N. America	W. Europe	E. Markets	APAC	Mid-East	Japan
Ensuring Continuity of service	23%	29%	15%	25%	23%	23%	20%	25%	21%

The data from the previous section showed that Chinese businesses reported substantially higher amounts of DDoS incidents than any other region, and here we see that Chinese businesses place the lowest value continuity of service – 15%, compared to the global average of 23%.

While these questions have established that service continuity is highly-prized by most businesses, they don't establish who is responsible for actually managing the threat of DDoS attacks? The answer: each business is responsible for protecting itself. While business may be content to rely on banks for financial transaction security, businesses clearly look to their own in-house resources to manage the DDoS threat. When asking respondents in the financial services sector or those operating online public-facing services, an average of 61% responded that the internal IT department and senior management were responsible for managing DDoS attacks against the business. Only 21% believed that protection from DDoS attacks was the responsibility of their network service provider or website/hosting provider.

It should be noted, however, that smaller businesses are more likely to rely on the assistance of these providers than larger businesses. 41% of very small businesses would look to the network service provider or website/hosting provider to help them mitigate a DDoS attack. Enterprises, on the other hand, would not only rely on their own IT and internal management teams, but would lean heavily on dedicated "security department" resources, which simply aren't found in smaller businesses. In fact, only 8% of enterprise respondents would look to an external hosting provider to mitigate a DDoS attack.

USAGE OF ANTI-DDOS SOLUTIONS

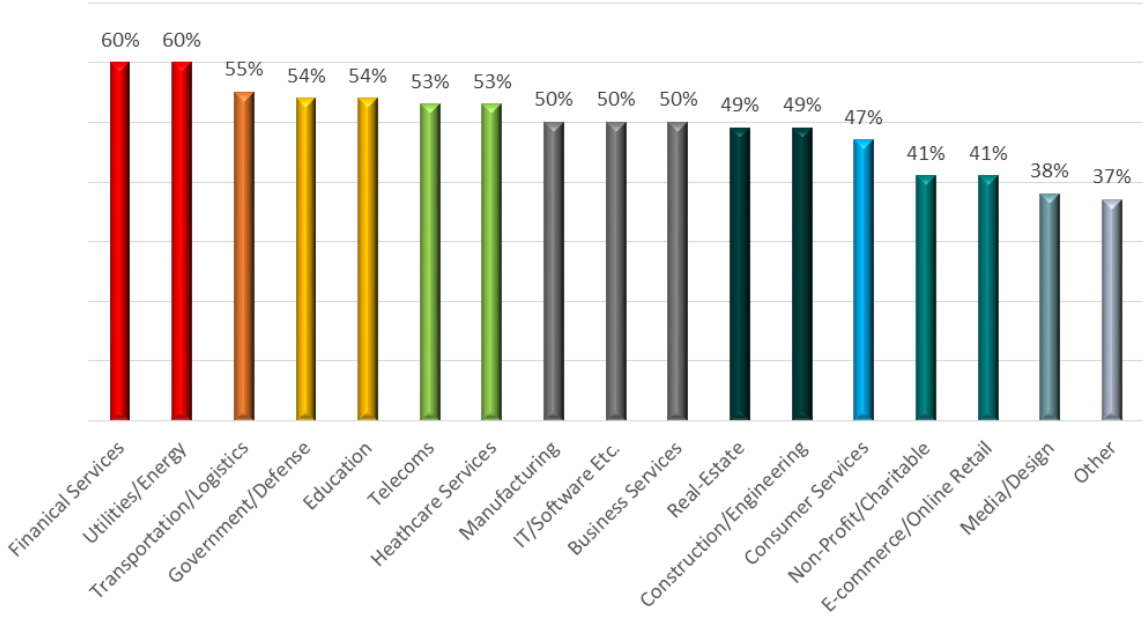
Around the world, **37% of businesses use "specialized services designed to protect web service continuity**." In most regions, more than 40% of businesses use a specialized anti-DDoS solution, with Western Europe reporting slightly lower usage (35%). Surprisingly, Russia was the country where anti-DDoS solutions were least widely used. That was unexpected given how this report has noted how frequently their financial services sector and web-based service providers are attacked, and how highly Russian businesses rate the importance of service continuity.

The perceived importance and usage of a specialized DDoS countermeasure is somewhat dependent on the size of the business, as 60% of large businesses and enterprises agreed that such a function was "an important security requirement for our organization," compared to just 46% agreement amongst SMBs. Overall, 50% of all businesses agree that countermeasures against DDoS attacks are an important security requirement.

When examining how various regions and business sectors rate the importance of DDoS countermeasures, some familiar patterns emerge.

ATTITUDE TOWARDS TECHNOLOGICAL TRENDS

BY VERTICAL: FINANCIAL SERVICES WERE THE MOST INTERESTED IN DDOS COUNTERMEASURES

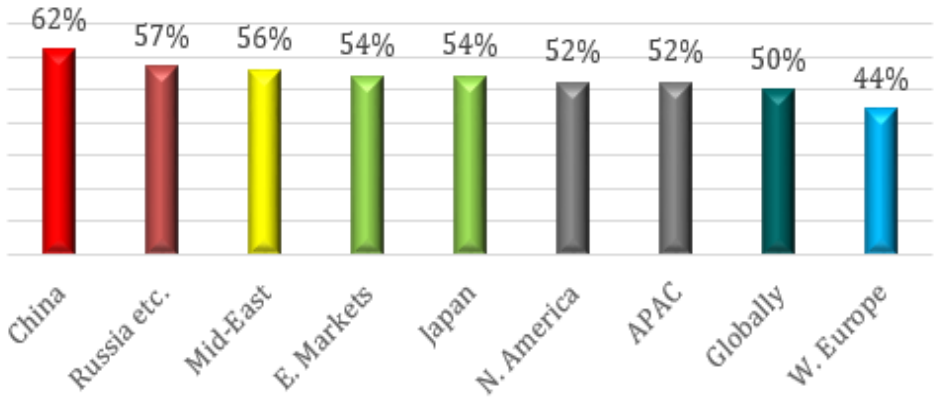


The two business segments that feel the strongest about the importance of DDoS countermeasures are the Financial Services and Utilities & Energy sectors (both at 60%). Given how often financial service providers encounter DDoS attacks – and how they presumably have the funds available to invest in specialty solutions to fight this problem – the enthusiasm of this sector shouldn't come as a surprise. The response from the Utilities & Energy sector speaks volumes about how much this sector values its "constant uptime," where

protection against service disruptions takes priority over data security. It is noteworthy that several other industrial segments – Telecom, Transportation/Logistics – reported similarly-high response rates.

Here again, we see China and Russia placing the highest value on DDoS countermeasures. Again, the discrepancy of Russia's perceived value of service continuity and DDoS countermeasures seems to contradict the low deployment rate for anti-DDoS solutions in this region.

ATTITUDE TOWARDS TECHNOLOGICAL TRENDS



CONCLUSIONS AND RECOMMENDATIONS

DDoS attacks can be particularly frustrating for IT managers, since they require relatively little technical expertise to conduct, and don't require the attackers to breach the carefully constructed network of the business. But by simply flooding a company with inbound traffic, a DDoS attack is able to achieve outcomes comparable to much more sophisticated cyber-attacks: a business unable to function, and left with large clean-up costs.

Moreover, DDoS attacks are targeted and not indiscriminate. They're an "easy" way for opponents of an organization to sabotage an organization – including business, political organizations, charities, etc. – making DDoS attacks a leading tool for "hacktivists." They're also an effective way for cybercriminals who are motivated by more traditional goals – money – to extort businesses: "*give us a ransom, and we'll turn off the attack…the ransom costs much less than the money you'd lose by having your service blocked for hours*." Many businesses would opt to pay this ransom, and who could blame them? DDoS attacks are also an affordable way for an unscrupulous business owner to cripple his competitors' web operations and drive their customers away.

For years, Kaspersky Lab has been accurately predicting the rise of DDoS attacks, and has paid closer attention to the botnets that fuel these attacks. Kaspersky Lab decided to counter this threat directly, and announced the company's intention to create specialized anti-DDoS technologies and solutions for businesses. The company has spent years building and testing these technologies in laboratory settings, as well as in the field protecting multi-million dollar networks, including successfully protecting several Russian banks targeted by hactivists in 2013.

The full solution, Kaspersky DDoS Protection, is now being introduced in selected global markets, and will continue to be launched in more markets as we customize the solution to meet the individual legal requirements of each country. To learn more about DDoS attacks and Kaspersky Lab's anti-DDoS technologies, please review the following resources:

Kaspersky DDoS Protection Whitepaper

What is a Botnet?

Data sheet "Discover how Kaspersky Lab defends businesses against DDoS attacks"

Kaspersky DDoS Protection webpage