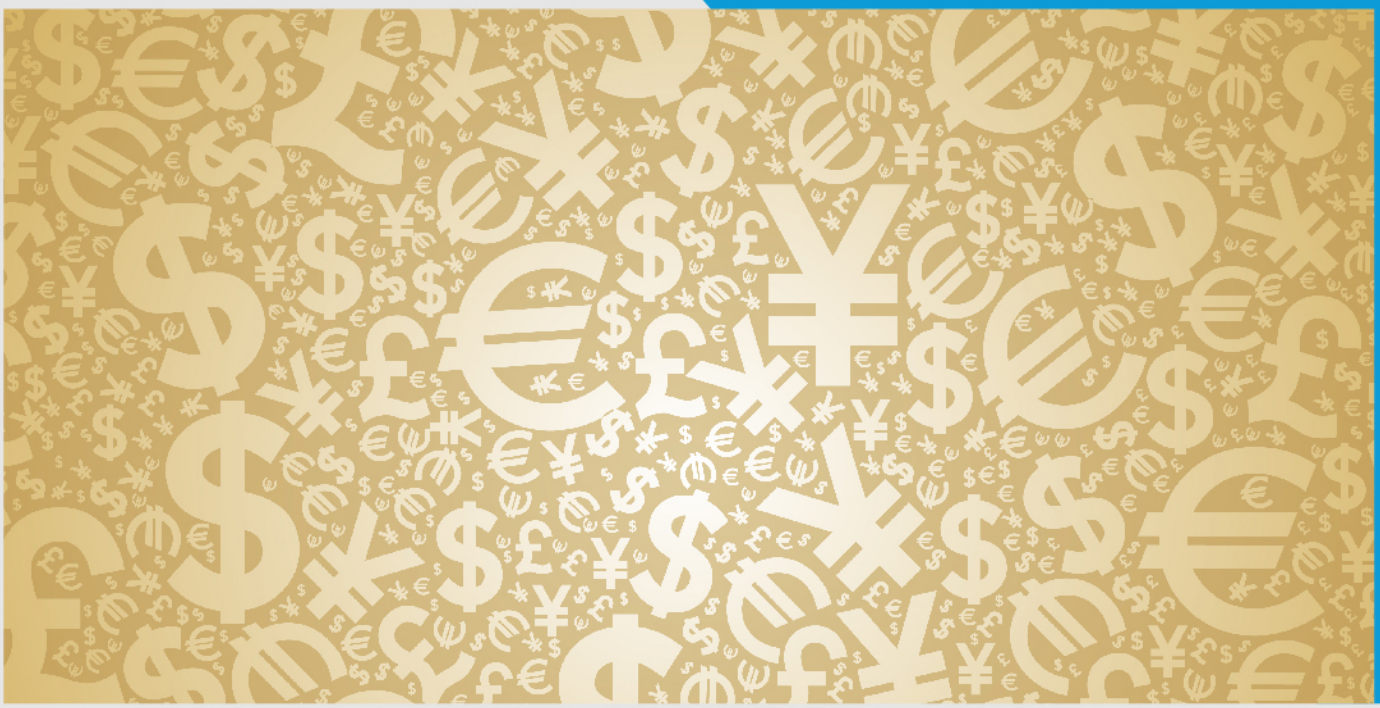
MAZEBOLT

WHITEPAPER



Cost and Implications of a DDoS Attack

This whitepaper explores the impact of DDoS attacks in terms of costs and implications for businesses and the best way to reduce DDoS risk to less than 2%

Table of Contents

EXECUTIVE SUMMARY 3

THE HIDDEN COST OF DDOS ATTACKS 4

IMMEDIATE RISKS 5

- Loss of Revenue from Site Inaccessibility 5
- Session Disruption 5
- Productivity Losses 5
- IT Staff Time and its Impact on Security 6

SHORT TERM RISKS 7

- Customer Loss 7
- Loss of Reputation 7
- Price of Distraction 7
- Consulting Fees 8
- Customer Service Overload 8

MEDIUM TERM RISKS 9

- SLA Noncompliance May Entail Penalties 9
- The Threatening Remains 9
- Breaking the Law May Result in Potential Fines 9
- The Blame Game 9
- Budget Reallocation 10
- Blackmail 10

DDOS RISK IMPACT ON INDUSTRY SEGMENTS 11

- Financial Sector 11
  - *High Impact – Customer Loss* *11*
- Insurance Sector 11
  - *High Impact – Legal Challenges* *11*
- Healthcare 12
  - *High Impact – Operational Disruptions* *12*
- Ecommerce 12
  - *High Impact – Revenue Loss* *12*
- Government 13
  - *High Impact – Security Breaches* *13*

CONCLUSION 14

- The 3 Pillars of DDoS Risk Management 14
  - *Verify your DDoS Mitigation works as expected* *14*
  - *Ensure your Vendors live up to their SLAs* *14*
  - *Does your DDoS response playbook hold water?* *14*

ABOUT RADAR™ 15

ABOUT MAZEBOLT 15

REFERENCES 15

Table of Figures

Figure 1 - What DDoS Attacks Really Cost Businesses _____ *3*
*Figure 2 – DDoS Risks by Type of Impact*_____ *4*
Figure 3 – Downtime of IT Production Systems _____ *6*

Executive Summary

65% of companies will encounter some type of downtime within the next 12 months, the average DDoS security gap of enterprises is 48%, RADAR™ brings down gap to under 2%.

Alarmingly, the number of attacks continue to grow in volume, intensity, and sophistication. `The Council of Economic Advisers' in its report, `The Cost of Malicious Cyber Activity to the U.S. Economy', says:

"The number of DDoS attacks continues to increase year-on-year, with millions of attacks reported annually". In 2018, DDoS attacks increased by 40% as large organizations faced an average of eight attacks per day.

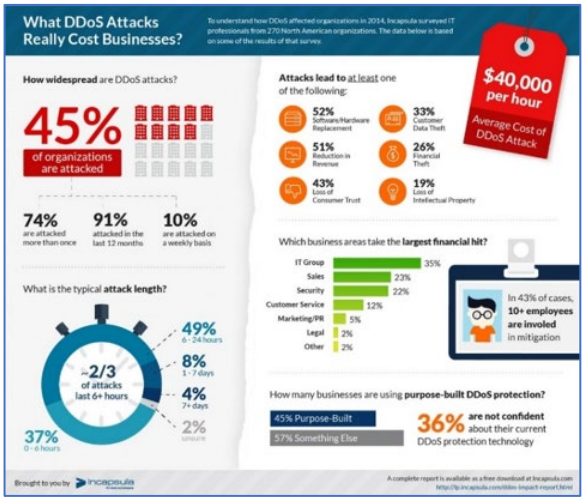
Distributed Denial of Service (DDoS) attacks can cause serious damage to business operations. Attacks cost safety of intellectual property and protection of sensitive data.

The costs can be debilitating, affecting businesses both in the short and long term. When assessing the damages wreaked by a DDoS attack, the primary cost factors that come to mind are related to lost business, and costs related to mitigation. However, DDoS attacks have **several costs, well hidden,** and it is mandatory for enterprises, to understand the implications and include the hidden costs of DDoS attacks in their overall business strategy.

To calculate the costs requires a thorough understanding of the **short term, long term and immediate implications**. Other factors that should be taken into account are **DDoS's impact, the speed, timing and penetration of the attack** and also, more importantly, **the industry segment that is targeted**. For example, an attack on an eCommerce site is different from an impact on a media organization in terms of damages.

This document takes **an in-depth look** at these risks and analyzes them to provide companies with a comprehensive understanding of the DDoS risk landscape. It then suggests pre-emptive measures that companies can take to minimize the impact of DDoS attacks.

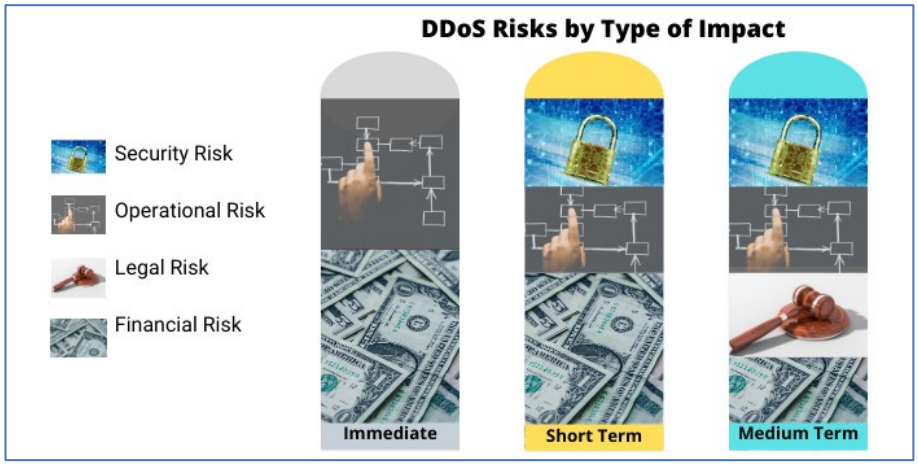
Figure 1 - What DDoS Attacks Really Cost Businesses



The Hidden Cost of DDoS Attacks

The analysis outlines these risks through two main dimensions as illustrated in Figure 1:

Figure 2 – DDoS Risks by Type of Impact



Time of Impact:

- Immediate,
- Short Term &
- Medium Term

Type of Impact:

- Security Risks,
- Legal Risks
- Operational Risks
- Financial Risks

The three sections that follow correspond to the same:

(i) Immediate Phase
(ii) Short Term Phase
(iii) Medium Term Phase

Companies can take pre-emptive measures to secure themselves using the above phases. DDoS Risks by Type of Impact

Immediate Risks

Loss of Revenue from Site Inaccessibility

This is the first risk that usually comes to mind when thinking of a “DDoS Attack” and rightfully so.

Neustar’s most recent study indicates that nearly half of the enterprises (49%) estimated their hourly revenue risk at US$250,000 or higher. When taking into account that mitigating DDoS attacks takes 45% of enterprises between 3 hours , to more than 24 hours, that amounts to significant financial losses.

The financial impact of a DDoS attack can have several implications.

The primary implication is related to the costs involved in mitigating and recovering from the attack.

`On average, the cost of a DDoS attack for enterprises is $2 million, and the cost of a DDoS attack for small and medium-sized businesses (SMBs) was $120,000 in 2019.

The second variable would relate to lost business and customers. This variable is difficult to quantify and can vary from business to business.

Session Disruption

Beyond ecommerce, DDoS attacks create session interruptions, where the customer is right in the middle of a transaction or game, and the system suddenly goes down. What kind of customer experience are you promoting? It is a well-known fact that the buying cycle and shopping cart abandonments are common experiences for ecommerce businesses.

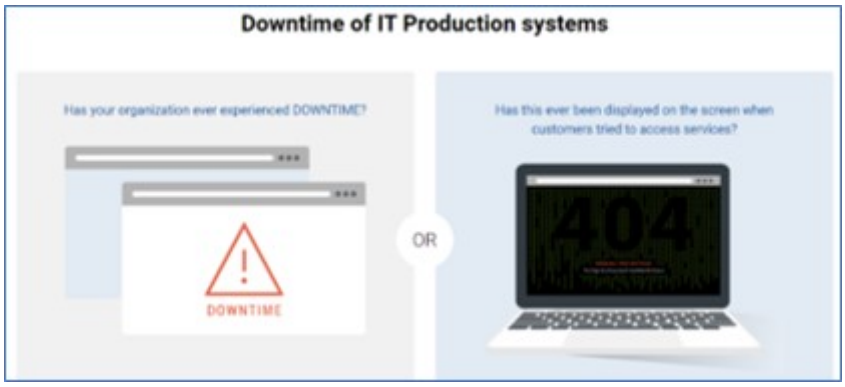
When the dropouts occur because a DDoS attack caused the site to crash, it can mean that the customer may not come back to the site. Finding customers who buy online, keeping in mind the severe competition, and then losing them to a DDoS attack is unimaginable.

For example, the result of 20 DDoS attacks in 30 days can degrade customer web traffic by 35%. Relatively speaking, a 35% degradation in traffic equates to a 60% drop in online purchases and 40% increase in abandoned shopping carts. [Building an Effective Cybersecurity Program, 2nd Edition]

Productivity Losses

What if your site serves as the gateway for remote employees? The longer it takes to get the site back up, the less work gets done by all employees in the organization. According to Gartner, the average cost of network downtime is around $5,600 *per minute.* That is around $300,000 *per hour.* For any business, $300,000/hour is huge loss. Along with the time required to get the network up and running, it takes an average 23 minutes to get refocused on one’s prior task. According to a Carnegie Melon University study, cognitive function can decrease by 20 percent after an interruption.

Figure 3 – Downtime of IT Production Systems



IT Staff Time and its Impact on Security

While your 15 employees are fighting the DDoS attack, who is doing their regular jobs? Who is watching all the other systems not connected to the DDoS attack? In the world of digital transformation, IT manpower are key contributors to business revenue. Their responsibilities stretch beyond setting up hardware and network to ensuring seamless communication channels.

This ensures optimized operations, which in turn helps to bring down costs, and thereby impacts revenue numbers positively. As key contributors to the business's revenue, locking them up in managing an attack can impact the overall smooth functioning of the IT organization and thereby impact revenue numbers.

Short Term Risks

Customer Loss

Consider all the potential long-term customers a company has lost because a site was down when they began their shopping process? Instead of buying from this site, they may go ahead and purchase from a competing vendor.

The price is reasonable, the delivery gets to them on time, and the products are at an acceptable quality. The potential lifetime value of the customer has now been gifted to a competitor. Losing a customer has long term effect on a business. While some businesses like eCommerce find instant gratification from customers, B2B large value customers are key providers to the business revenue.

Large deals are difficult to close and therefore, existing customers, as referrals, become crucial to business sustenance. Losing customers therefore can have a strong adverse impact on a business. Companies linked to finances such as online transfer, banking and similar companies stand more to lose from a DDoS attack.

An interruption in a financial transaction can seriously impact customer faith in the company. In a highly competitive world, the customer can choose to abandon an enterprise purely because of loss of faith in the security and services offered by the enterprise.

Loss of Reputation

When a technology website is rife with spelling and grammatical errors, customers are less likely to buy because they assume that if a company cannot be bothered with the small stuff , they are not going to be bothered about the minor glitches that are wrong with their technology.

Potential customers have a similar attitude about companies whose DDoS attacks have been publicly reported. `If they cannot be bothered to protect their own systems, what kind of care are they going to take with the security infrastructure of the technology they are selling?'

Summarizing its importance, Forrester said in its report, "How To Safeguard Your Firm's Most Valuable Assets — The Intangible Ones" says, "Protecting hard-earned corporate reputations takes on greater importance as companies shift strategic priorities to win, serve, and retain customers. When a crisis strikes, whether the result of executive malfeasance, a product safety recall, a security breach, or another violation of a company's brand values — **the results can be disastrous.** Risk professionals can no longer overlook the growing value and vulnerability of corporate reputations."

There are several examples of companies that have withstood attacks and managed to reposition themselves while others are written off after a single attack. This is because of the relationship that organizations invest in with their customers.

If the building blocks are in place, the relationship will withstand a storm. More importantly, customer conscious enterprises do not leave anything to chance. They ensure that all the possible mitigation tools are in place to avoid an attack and if it does happen, they know how to mitigate the problem.

Price of Distraction

As your technology gets increasingly more sophisticated, so does the technology of cybercriminals. According

to recent DDoS surveys. It takes as many as 15 people to mitigate a DDoS attack. Whilst these 15 people are fighting the attack, they don't have time to focus on the rest of the network. This creates an opportunity for the cybercriminals to exfiltrate thousands to millions of customer records or proprietary corporate or governmental information, which they can use for financial or political gain.

Consulting Fees

In these cases, one needs to bring in a forensics team to determine what happened, instead of preparing yourself against the attack in advance. This type of consulting may be an external DDoS firm who advises you on what went wrong and why you had downtime. Last minute consulting is expensive in terms of time and money.

> "Nine in every ten organizations acknowledged some form of breach or associated activity with DDoS attacks with an average of 2 breaches per attacked company per year."- https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/

Customer Service Overload

This relates to the cost of the help-line personnel required to step-in and respond to the frantic customers calling to see if their bank transfers or bill payments went through? For an online gaming site, where customers were in the process of loading money into their accounts or in the middle of a tournament, the follow-up service to an attack can be DDoS difficult to manage in terms of resources and revenue. Irate customers in today's digital world can be voluble about their feedback. They can even go to the extent of creating legal issues.

Medium Term Risks

SLA Noncompliance May Entail Penalties

DDoS attacks automatically invalidate any type of SLAs the customer has committed to achieving. If the back-end system, which must be accessible 24/7 goes down, unhappy clients can demand refunds, sue the company, or simply wait until the contract expires and go elsewhere because of loss of confidence. SLAs or Service Level Agreements are bona fide documents that clearly outline the expectations of service levels and the implications of not meeting them. SLAs are signed by both parties under the safe assurance that commitments will be adhered to. However, DDoS attacks happen without warning and when they do, SLAs cannot be met. The implications can involve financial and legal battles at one end, and loss of customer confidence at the other.

The Threatening Remains

Some of the attackers may be using the DDoS distraction to leave APTs. For example, backdoors are installed through a normally unexploitable vulnerability, but because certain protections are down during a DDoS attack, those vulnerabilities are now available to be exploited within an existing network.

How long and how many resources will it take before they are identified, if at all? The mystery of lingering bots is a threat that affected networks will continue to remain with. Even after identifying the bots, there is no real proof that backdoor entrants have been identified and squashed.

Breaking the Law May Result in Potential Fines

Regulatory requirements may demand that certain information must always be accessible. GDPR for example has two requirements that directly discuss availability in Article 32 and Recitals 49.

GDPR fines can reach up to 20 million Euros or 4 percent of annual global turnover, whichever of both is highest.

> **"…shall implement appropriate technical and organizational measures to ensure… the ongoing confidentiality, integrity, availability and resilience of processing systems and services" - *Art.* 32 GDPR Security of processing**

The Blame Game

When looking around, after an attack, it is unclear who is to be blamed for the attack. Is it someone within the IT team or a member of the senior management? If the system is inadequate to prevent against a major DDoS attack, it is difficult to assess. Even though the IT security team has put in budget after budget with requests to replace the aging network infrastructure, the manager responsible may be the first to go. If a DDoS attack leads to a significant exfiltration or extended outage, a member of senior management may need to take the fall – even though she had made cybersecurity a priority and systems were already in the process of being upgraded.

Budget Reallocation

The excessive cost of recovery from a DDoS attack may require budget cuts to other departments, affecting marketing, R&D, HR, and others. All the various internal realignment in the organization may be quite painful in terms of time and arguments, depending on the organization and the size of the problem.

Blackmail

What if your systems are overwhelmed, and you just cannot stop the attack? Maybe the hackers will do it – for a price. There are several examples of blackmail DDoS attacks. In the recent past, a member of the IT team at German payments processor Computop retrieved an email sent to one of the company's public addresses, threatening to hit the firm's customer websites with a massive DDoS attack if a ransom of 15 Bitcoins (about £7,900) was not paid to the attackers. The attackers had launched a smaller demo DDoS to prove their intent which the IT staff confirmed, after checking monitoring systems.

DDoS hackers see huge potential in cybercrime. Based on past successes, some of them adopt names of successful hackers to try and extort money. Fancy Bear is one such popular name that extortionists adopt. Extortionists mostly launch a small attack and follow it with an extortion note, threatening a larger attack.

The window of time provides enterprises with the time to analyze the IP address, and the bitcoin information to get a better understanding of the blackmailer. Most times, the small threats are not followed up. Having said, that, blackmail is still a big concern for online businesses across industry segments.

DDoS Risk Impact on Industry Segments

Financial Sector

Over the years, the financial sector has been a target zone for attack by cyber criminals essentially because of the **value of the information** involved. As a result financial enterprises are targeted **300 times more frequently** than other businesses. Often, attacks can be termed as **blackmail and involve high ransoms**.

A 2017 report by the Ponemon Institute and IBM revealed that while the average cost to U.S. businesses per record lost or stolen in a breach was $225 across all industries, the cost for businesses in the financial industry was $33614.

In fact, the average annual cost of cyber-crime in the vertical stood at an estimated US$18.5 million (£14.3 million) per company in 2019, 40 percent higher than the average across all industries.

This sector has been at the forefront of digital transformation, catering to a new generation of mobile and internet savvy customers. The transformation to online and cloud technologies has paved the way for hacktivists to look for vulnerabilities and plan their attacks. Most DDoS attacks on financial institutions are molded to cripple the websites through overwhelming traffic, and thus halting online transactions.

High Impact – Customer Loss

Customer confidence is the bedrock on which financial institutions build their businesses. The impact of a DDoS attack chips away this bedrock. It shakes the confidence level that customers have placed on the institution and the results can be long lasting. For financial institutions, the primary cost of a DDoS attack is loss of customer confidence. For example, during Operation Power Off, several banks reported that during a DDoS attack, the public impact that far greater than financial damage. This is followed by monetary losses, regulatory issues, loss of personal records which attract legal issues and so forth.

Insurance Sector

The insurance industry has seen a large opportunity in cyber insurance. However, whilst it is busy offering cover for other businesses, this sector itself is under threat. This industry has been targeted for PII (personally identifiable information), financial data and anything else that can be monetized.

The average insurance company will face an average of 113 targeted breach attempts per year, in addition to millions of random attacks each week. According to Accenture, a typical insurance organization faces more than three effective attacks per month, yet four fifths of the larger insurers security executives were confident in their cybersecurity strategies.

High Impact – Legal Challenges

Most companies will not be willing to disclose details about security breaches for obvious reasons. However, over the years there have been several companies that have been dragged into the public eye for the wrong reasons. In the past, Anthem, the second-largest health insurer in the US, had up to 80 million customer and employee records exfiltrated. In another incident, 11 million customers PII was stolen from Premera Blue Cross, one of Arizona's largest healthcare providers.

Banner Health, saw 3.7 million patients, customers and doctors PII stolen in a breach. The implications of an attack will cause legal issues which will affect the enterprise's future revenue, operations, and customer base.

Healthcare

Healthcare organizations were targeted by distributed denial of service (DDoS) attacks 12 percent of the time in 2018, up from 10 percent in 2017, according to NETSCOUT's annual Worldwide Infrastructure Security Report. The healthcare industry is targeted for DDoS attacks for one single reason – money! It is estimated that by the year 2026 healthcare expenditure will cross 20% of the GDP. It is also believed that the cost of medical records is higher than even that of passwords and credit cards on the darknet.

See if below statements make sense :

For healthcare enterprises, the main challenge is adopting digital transformation. With increased digital disruption, healthcare is moving towards Electronic Health Records and IOT. However while migrating from legacy infrastructure, healthcare enterprises face grave challenges with regard to security as vulnerabilities emerge during the process. Accenture estimates that the loss of data and related failures will cost healthcare companies nearly $6 trillion in damages in 2020, compared to $3 trillion in 2017. There have been incidents in which DDoS attacks overloaded hospital networks, disrupting operations and causing immense damage.

High Impact – Operational Disruptions

For the healthcare industry, the eye-opening incident was the **DDoS attack on Boston Children's Hospital.** The hacktivist group called Anonymous was suspected of launching the attack. During the DDoS attack, the hospital's electronic health records system was compromised greatly, inconveniencing patients, and the hospital staff. The implications can stretch from operational to security to loss in revenue and in patients' confidence.

Ecommerce

As the retail and ecommerce industries continue to transform and adapt to disruptive digital transformations, the threat of DDoS looms over these businesses like a dark cloud.

Peak business times, like the holiday seasons should bring good cheer, but for many the last few years, these times have also been nightmarish. In 2019, security firms report a 150 percent increase in DDoS attacks in the months between summer and the end of the year.

Summarizing this rise in attacks, the Organized Crime report has found DDoS to be a top five threat emerging from organized crime, for which extortion was the most common motive with DDoS attacks targeting retailers during the peak holiday season.

High Impact – Revenue Loss

When Dyn was hit with DDoS, Etsy, Shopify, and PayPal amongst others experienced lengthy outages. The potential lost sales may be difficult to quantify but there is no doubt that the losses were significant. .

Amazon suffered an attack way back in 2000 when it was an ecommerce provider. Fast forward to 2019, Amazon's cloud services (AWS) were targeted. The Threat Landscape Report for 2019 identified Amazon as the most targeted cloud service, accounting for 25.92% of attacks.

Government

Cyber security has become a global priority and governments worldwide are either impacted or learning from those already affected by DDoS attacks. In the recent past, the National Action Party or PAN – Mexico's political opposition party – was targeted by DDoS attacks that took down its website for about 15 minutes. Every month, 20 to 40 million cyber attacks are launched against Taiwan's government websites. Millions of Australians were unable to fill out mandatory Census online data forms because the government website was slammed by a distributed denial of service (DDoS) attack. Government servers were forced offline in Luxembourg when they came under a DDoS attack. Politically motivated attacks have impacted several governments and governmental organizations, escalating the importance of cyber security measures. NETSCOUT Arbor's recently released Worldwide Infrastructure Security Report, and noted that **57 percent of surveyed enterprise government and education respondents had seen their Internet bandwidth saturated due to a DDoS attack – well up from the 42 percent figure a year ago.**

High Impact – Security Breaches

When governmental organizations are impacted by DDoS attacks, the effects are far reaching, and the damages cause ripple effects that can negatively impede several other stakeholders, governments and countries. These attacks continue to happen and continue to catch targets by surprise by their suddenness and intensity. Mitigation measures more often than not **fail in the face of DDoS attacks** as seen in the above examples.

Conclusion

The 3 Pillars of DDoS Risk Management

To continuously eliminate DDoS risk, enterprises today need to be prepared rather than react.

Verify your DDoS Mitigation works as expected

Having served almost 100+ enterprises in the field of DDoS Mitigation, MazeBolt found that DDoS mitigation solutions, be it CPE, Cloud Scrubbing services or hybrids solutions are vulnerable to DDoS attacks by design. Every posture carries its pros and cons however no posture can completely eliminate DDoS risk. Explore more about it in the whitepaper - `Beginner's Guide to DDoS Mitigation Technology'.

Ensure your Vendors live up to their SLAs

Cloud Scrubbing Services will typically commit to mitigating DDoS attacks within a certain time frame. This leaves the window open for odd hours DDoS attacks. For example, when an attack took place in the middle of the night, it was unable to be dealt with by the Cloud Scrubbing Services team on call and the issue was escalated at 02:00 to get someone on deck. This took up valuable time (and money).

> **"Everybody has a plan until they get punched in the face."**
> ***Mike Tyson***

MazeBolt has partnered with several companies for SLA level performance to evaluate vendor.

Does your DDoS response playbook hold water?

Coming under attack in any circumstances takes people from theory to practice in unexpected ways. Generally, results are very often not as planned.

Having a DDoS response play book is a necessity nowadays. Equally important is running drills that allow the different teams involved in DDoS mitigation to make sure communication paths are clear, roles & responsibilities are defined, and tasks are preformed adequately.

About RADAR™

From the above analysis, it is obvious that DDoS threats are a reality and their prediction nearly impossible. Even with the most sophisticated DDoS mitigation and testing solutions deployed, most companies are left with a staggering 48% DDoS vulnerability level. The vulnerability gap stems from DDoS mitigation solutions & infrequent Red Team DDoS testing being reactive, instead of continuously evaluating and closing vulnerabilities.

Mitigation solutions do not constantly re-configure and fine tune their DDoS mitigation policies. Leaving their ongoing visibility limited and forcing them to troubleshoot issues at the very worst possible time, that is, when systems are brought down by a successful DDoS attack. These solutions are all reactive, reacting to an attack and not closing DDoS vulnerabilities before an attack happens.

DDoS Red Team Testing simulates a small variety of real DDoS attack vectors in a controlled manner to validate the human response (Red Team) and procedural handling to a successful DDoS attack. Red team testing does not identify a company's vulnerability level to DDoS attacks and is usually performed on average twice a year. Red team testing is a static test done on dynamic systems. Any information gained from this testing, is valid for that point in time only.

Red Team testing is very disruptive to IT systems and requires a planned maintenance window.

RADAR™, MazeBolt's new patented technology solution is part of the MazeBolt security platform. RADAR™, simulates DDoS attacks continuously and non-disruptively. Delivering advanced intelligence, through straightforward reports on how to remediate the DDoS vulnerabilities found. With RADAR organizations achieve, maintain, and verify the continuous closing of their DDoS vulnerability gaps. Reducing and maintaining the vulnerability level of a damaging DDoS attack from an average of 48% to under 2% ongoing.

About MazeBolt

MazeBolt is a leading innovative cyber security company, and part of the mitigation space. Offering full DDoS risk detection and elimination. Working with any mitigation system to provide end to end full coverage. Avoiding downtime and eliminating mitigation vulnerabilities before an attack happens.

References

1. https://www.computerweekly.com/news/252439254/DDoS-attacks-cost-up-to-35000
2. https://usa.kaspersky.com/about/press-releases/2018_ddos-breach-costs-rise-to-over-2m-for-enterprises-finds-kaspersky-lab-report
3. https://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/
4. http://www.privacy-regulation.eu/en/article-32-security-of-processing-GDPR.html
5. http://www.privacy-regulation.eu/en/r49.html
6. https://hello.neustar.biz/201710-Security-Solutions-Siteprotect-DDoS-2H2017-Report-LP.html