Arbor White Paper

The Risk vs. Cost of Enterprise DDoS Protection

How to Calculate the ROI from a DDoS Defense Solution

ARBOR® NETWORKS

About Arbor Networks

Arbor Networks, Inc. is a leading provider of network security and management solutions for enterprise and service provider networks, including the vast majority of the world's Internet service providers and many of the largest enterprise networks in use today. Arbor's proven network security and management solutions help grow and protect customer networks, businesses and brands. Through its unparalleled, privileged relationships with worldwide service providers and global network operators, Arbor provides unequalled insight into and perspective on Internet security and traffic trends via the ATLAS® Active Threat Level Analysis System. Representing a unique collaborative effort with 230+ network operators across the globe, ATLAS enables the sharing of real-time security, traffic and routing information that informs numerous business decisions.

Understanding the Risk of Attack

The data center has evolved from what was once primarily a provider of enterprise back-office support services to the public-facing Internet data center (IDC) of today. The IDC provides real-time, business-critical functions such as sales, communications, customer support and so on. In many industries, the IDC is the only vehicle for transacting business (e.g. ecommerce, gaming, social networking, online financial services, Web hosting).

A continuing and growing threat to IDC availability is distributed denial of service (DDoS). Arbor Networks regularly surveys IDC operators and in cooperation with Internet Service Providers (ISPs), monitors much of global Internet traffic. Surveys and monitoring data show that DDoS attacks are occurring with increasing frequency and severity.[1] These attacks impose real costs and financial risk to businesses that rely on their IDC. An effective DDoS defense system can safeguard business operations against DDoS-related outages and a good first step in deciding whether to invest in such a system is to determine the expected return on investment (ROI). This paper provides a simple, step-by-step approach for evaluating the financial return on investing in a DDoS defense system.

Using industry averages for attack frequency and outage costs, the results show that investing in an effective DDoS protection solution, such as the Peakflow® SP Threat Management System ("TMS"), provides a strong positive ROI and lowers financial risk. Arbor Networks also provides online tools and resources to help IDC operators with the technical and business aspects of investing in DDoS defense.

Few studies focus on the probability that a business will experience a DDoS attack of significant impact. However, survey information from Forrester Research and Arbor Networks provides insight into the risk of such an attack.

Forrester Research conducted a survey of 400 companies with significant online operations.[2] The survey's objective was to gather basic information on the DDoS threat to these businesses, which included online financial services, media, news, political sites, gaming, entertainment, Web hosting and ecommerce. Among the results, over 70% reported at least one DDoS attack in the previous 12 month period. Attack durations were highly variable, but the most common duration for attacks that had operational and business impact was two to six hours.

Arbor Networks' annual *Worldwide Infrastructure Security Report*[1] is an excellent source of more detailed information on the frequency and nature of DDoS attacks on Internet service providers (ISPs) and Internet data centers (IDCs). Based on the responses from 111 ISPs and IDCs, the most recent survey data shows that these organizations are experiencing a high frequency of DDoS attacks—equating to multiple attacks per month (see Figure 1).

McAfee[3] also surveyed IT and security executives from seven industry sectors and found the frequency and impact of DDoS attacks to be similar to those Arbor reported. In terms of the impact of DDoS attacks, 84% of ISPs and IDCs reported incurring operational expenses, and 43% reported customer churn and revenue loss (see Figure 2).

Hosting providers in particular often have a higher risk of DDoS attack than stand-alone online businesses because hosting providers in effect aggregate the risk of all their customers. An attack on one customer can affect others and potentially the entire hosting operation because of the heavy reliance on shared infrastructure. Risk is also a function of the type of customers being hosted. Sites that engage in controversial activity, as well as large, visible businesses, are more likely targets of DDoS than small business Web sites. However, just one small customer can attract a massive DDoS response with a single controversial act.

Average Number of DDoS Attacks per Month

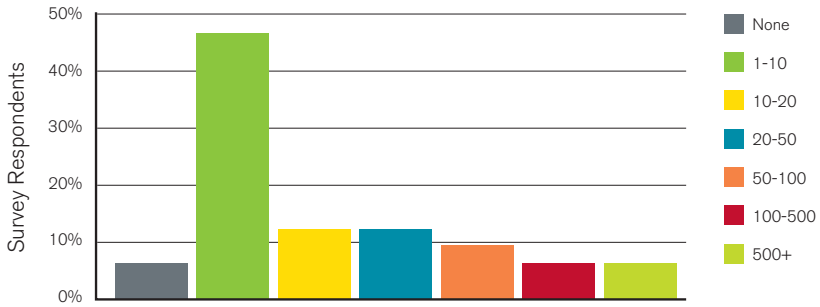

Figure 1: Average Number of DDoS Attacks per Month
Source: Arbor Networks Annual *Worldwide Infrastructure Security Report,* 2010

Impact from IDC DDoS Attacks

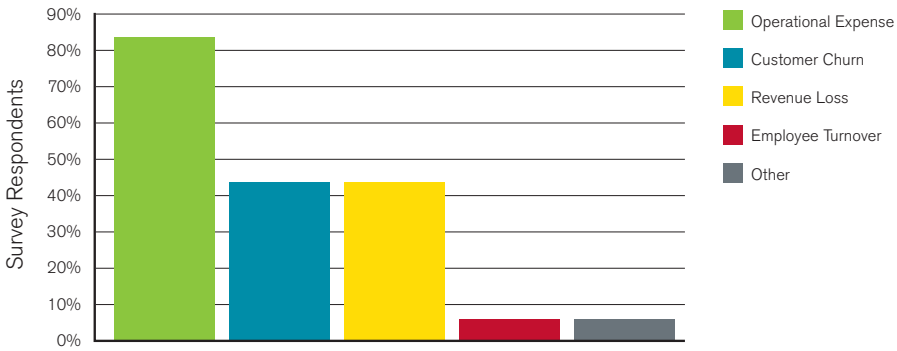

Figure 2: Impact from IDC DDoS Attacks
Source: Arbor Networks Annual *Worldwide Infrastructure Security Report,* 2010

The capacity to unleash a large DDoS attack is available to anyone simply by renting a botnet. Figure 3 shows a typical advertisement for botnet services. Table 1 shows the results of a survey on botnet rental pricing. In short, the resources needed to carry out large-scale DDoS attacks are low cost and readily available.

Botnets are not the only source of DDoS attacks. Social media sites can coordinate large numbers of willing users to carry out DDoS attacks as illustrated by the WikiLeaks inspired attacks in late 2010. Coordinated through Twitter, large numbers of end users downloaded a simple attack tool and directed attacks at numerous companies deemed complicit in interfering with what the users viewed as the legitimate activities of WikiLeaks. These attacks successfully targeted high profile companies, including PayPal, MasterCard and Visa. The attacks went both ways as well. The provider hosting WikiLeaks had to remove the site from its infrastructure because DDoS attacks directed at WikiLeaks were impacting service to all its customers. This example illustrates the reality that hosting providers bear the aggregated risk of their customers.

The overall impact of a DDoS attack is a function of the time it takes to detect the attack, the time needed to mitigate it and the extent of service degradation both before and after mitigation. For many IDC operators, detection consists of simply waiting for customers to complain, and mitigation consists of dropping all traffic destined to the resource under attack. This form of mitigation may protect the IDC infrastructure and other customers, but it completes the attack on the particular target of the DDoS event. If the target is a high-value customer or service, there will likely be financial loss.

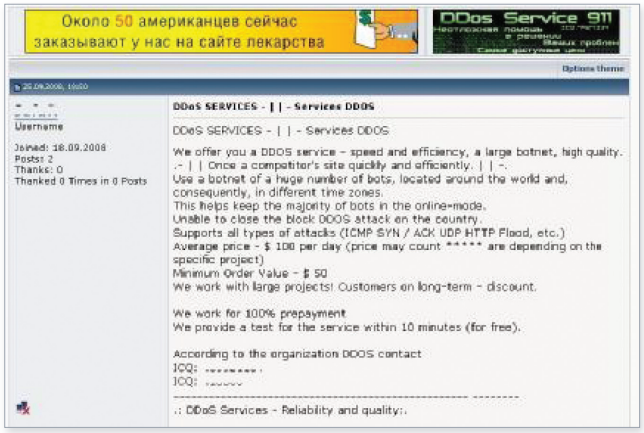

Figure 3: Advertisement for Botnet Services[4]

Price	**Duration** Hours	**Bandwidth** Mbps
$20	2	45
$30	6	45
$50	12	45
$70	24	45
$75	24	100
$100	24	1,000
$250	24	1,000
$400	5	5,000
$600	168	1,000
$900	24	4,750
$1,000	24	4,750
$5,500	168	4,750
$6,000	168	4,750

Table 1: Botnet Rental Pricing[4]

Using the survey data (Figures 1 and 2) a conservative estimate of the number of high-impact DDoS events (events resulting in outages of at least 2 hours) is shown in Figure 4. The figure shows the expected number of outages (ranging from 2 hours to over 24 hours) that a typical IDC will experience over a three year period. A period of three years is used because ROI is generally based on a three year time frame.

The cost of outages due to DDoS attacks is comprised of operational costs and revenue impacts. Lower-impact and lower-duration attacks may result only in added operational costs. Higher impact attacks will also negatively affect revenues as business operations are partially or fully impaired. For Internet data centers, the elements contributing to the overall cost of DDoS consist of some or all of the following:

- Personnel time spent addressing and recovering from the outage.
- Incremental help desk expenses.
- Lost sales.
- Customer credits and refunds.
- Lost employee productivity.
- Cost of customer defections and lost or missed sales.
- Degradation of reputation resulting in higher customer acquisition costs and a lower rate of business growth.

The specifics of how outages result in financial losses vary with the type of business. Businesses that are transactional in nature, such as ecommerce, suffer loss as the result of lost sales that are not made up later and lost future business as customers go to alternative suppliers on an ongoing basis. Other IDC-based businesses are service or utility-based such as hosting services (Web, email, communications). Financial losses for these businesses result from issuing customer credits, non-renewal and early termination of contracts and lost future business. Finally, enterprises with IDCs supporting business-critical functions experience financial losses as a result of lost productivity, lost sales and recovery costs.

A generic approach to calculating cost regardless of business type can be based on the annual company revenue and the percent dependence of the business on the IDC. Some businesses, such as ecommerce, are effectively closed when their IDC is unavailable while other businesses can partially function during IDC outages. However, for virtually all businesses, the impact of an outage increases exponentially with the length of the outage. For example, 40% of businesses surveyed reported that a 72 hour outage would put their survival at risk.[5] Such impacts that extend beyond the period of the outage itself can be accounted for as lost future business. Table 2 (page 5) illustrates this generic approach to estimating the cost of DDoS induced outages using an example of a business fully reliant on its IDC and with $50M in annual revenue.

Modeling the Financial Impact of Attacks

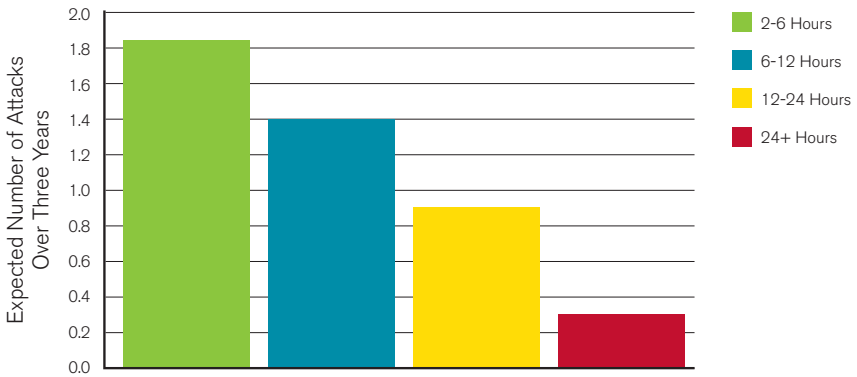

Figure 4: Modeling the Financial Impact of Attacks

Attack Duration Hours	**Operations** # hours x # staff x cost/person/hour	**Help Desk** # hours x calls/hour x cost/call	**Lost Current Revenue** Enterprise revenue per hour x outage duration x % business loss	**Loss of Future Business** Present value of 1 year lost growth	**Total Cost per Attack**
2-6	4 x 4 x $75	4 x 25 x $20	$50m/8760 x 4	0% x $50m x 2.49	$ 26,031
6-12	9 x 4 x $75	9 x 25 x $20	$50m/8760 x 9	0% x $50m x 2.49	$ 58,570
12-24	18 x 4 x $75	18 x 25 x $20	$50m/8760 x 18	.25% x $50m x 2.49	$ 428,390
24+	30 x 4 x $75	30 x 25 x $20	$50m/8760 x 30	.5% x $50m x 2.49	$ 817,773

Table 2: Modeling Cost of Outages Due to DDoS

Attack Duration Hours	**Expected Number of Attacks Over 3 Years**	**Cost per Attack**	**Expected Cost Over 3 Years**
2-6	1.9	$ 26,031	$ 49,459
6-12	1.4	$ 58,570	$ 81,998
12-24	0.9	$ 428,390	$ 385,551
24+	0.3	$ 817,773	$ 245,320
TOTAL EXPECTED COST			**$ 762,327**

Table 3: Three Year Expected Cost of DDoS Attacks

Combining the DDoS attack risk profile with attack cost estimates produces the expected cost over three years, as shown in Table 3.

This cost can now be compared to the alternative of investing in a high quality DDoS defense system, which can be expected to eliminate the extraordinary expenses of dealing with DDoS attacks through traditional methods (e.g., black holing customer traffic, removing domains, etc.). The cost of an effective DDoS protection system is generally a function of mitigation capacity—that is, how much attack traffic the device can handle. This example assumes that a system capable of mitigating 2.5 Gbps is sufficient and can be purchased for $100K. Annual ongoing ownership costs (e.g., support, maintenance, internal operations, etc.) are about 25% of the purchase price.

Using the data above, Table 4 shows the final results of the three year net present value (NPV) and ROI of the investment (not including residual value of the equipment).

Choice of the DDoS protection solution matters. As explained in Arbor Networks' white paper entitled "The Growing Need for Intelligent DDoS Mitigation Systems", traditional perimeter security products, such as firewalls and intrusion prevention systems (IPS), are unable to address the DDoS threat to availability. To realize the projected benefits of deploying a DDoS defense solution, due diligence is needed on the part of the technical staff when selecting a solution.

	ROI
Initial Investment	$100,000
Year 1 Return—Ownership Costs	$229,109
Year 2 Return—Ownership Costs	$229,109
Year 3 Return—Ownership Costs	$229,109
NPV (@10% Discount Rate)	$427,054
ROI	587%
Payback	5.2 Months

Table 4: NPV and ROI of a DDoS Defense Solution

Modeling Risk

In addition to modeling the best estimate of ROI as shown above, it also useful to model the upside and downside risks of investing in DDoS protection. In a McAfee survey of enterprises representing a variety of business sectors, respondents estimated on average that 24 hours of downtime from cyber attack would cost their organization $6.3M.[3] In short, organizations have a strong financial interest in protecting against losses that result from major attacks.

Figure 5 uses the example model from the previous section to show the breakeven point and financial sensitivity for protecting specifically against the risk of major attacks that result in extended outages (24+ hours). The graph depicts the three year cost of extended outages as a function of attack frequency and compares that to the fixed three year cost of DDoS protection. The breakeven point in this case is a frequency of one major outage every 15 years. Also significant is the difference between the upside and downside risk. The graph shows that the cost of not being able to effectively address DDoS attacks rises very steeply as frequency goes up; thus, the cost exposure of underestimating attack frequency is very high. In contrast, if the actual frequency is less than expected, the cost exposure of having overinvested in DDoS protection is gradual, bounded by the amount invested and further offset by the benefits of being able to mitigate shorter duration attacks. Finally, the graph illustrates how the investment in DDoS protection replaces a highly uncertain and steep cost curve with a flat, predictable and relatively low cost curve. This is clearly a more desirable operating model for financial managers.

Three Year Cost of Major Attacks Causing Outages of 24 Hours or More

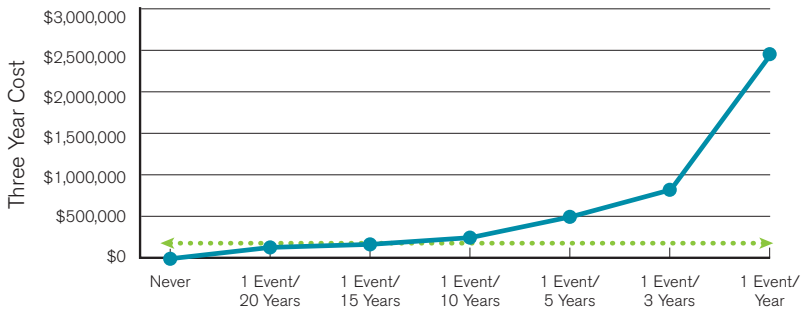

Figure 5: Three Year Cost of Major Attacks Causing Outages of 24 Hours or More

Conclusion

DDoS attacks on Internet data centers (IDCs) are common and pose a risk to the financial health and stability of IDC-based businesses.

Modeling costs and risks of these attacks provides a useful tool for evaluating the benefits of investing in sound DDoS protection. Arbor Networks has been protecting Internet-based businesses from DDoS longer than any other vendor and is the clear market leader.

For more information and tools visit Arbor Networks at www.arbornetworks.com or contact Arbor at www.arbornetworks.com/contact.

References

[1] *Worldwide Infrastructure Security Report,* Arbor Networks, January 2010.

[2] *The Trends and Changing Landscape of DDoS Threats and Protection,* Forrester Consulting, July 2009.

[3] *In the Crossfire: Critical Infrastructure in the Age of Cyber War,* Authors: Stewart Baker, distinguished visiting fellow at CSIS and partner at Steptoe & Johnson; Shaun Waterman, writer and researcher, CSIS; George Ivanov, researcher, CSIS; McAfee, 2010.

[4] *Modeling the Economic Incentives of DDoS Attacks: Femtocell Case Study,* Vicente Segura and Javier Lahuerta, Department of Network and Services Security, Telefonica I+D.

[5] *Ontrack–2001 Cost of Downtime Survery Results,* 2001.

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

Europe
T +44 207 127 8147

Asia Pacific
T +65 6299 0695

www.arbornetworks.com

ARBOR® NETWORKS

WP/DDoSPROT/EN/0612