WHITE PAPER

# HOW TO ANALYZE THE BUSINESS IMPACT OF DDOS ATTACKS

*Top 3 Things to Think About to Mitigate the Damage*

# THE INEVITABILITY OF CYBERATTACKS

Distributed denial of service (DDoS) attacks continue to threaten the ongoing operations of businesses everywhere. It doesn't matter what industry you are in, where you are located, or if you are big or small, the threat of a DDoS attack is a very real part of your organization's reality.

The proliferation of the Internet of Things (IoT), which hit 20 billion devices in 2017 and is expected to include 75.4 billion devices by 2025,[1] has exacerbated the DDoS threat. Most of these devices, if not all, have vulnerable web, mobile, and cloud interfaces, unprotected storage, unencrypted communications, insecure pairing procedures, and even hardcoded backdoors that make them easy targets for hackers to exploit and leverage for their own purposes.

**IOT EXPLOSION**

**20 BILLION**
IoT devices hit by 2017

**75.4 BILLION**
IoT devices expected by 2025

We've already seen attackers use botnets, made up of IoT devices that have been compromised, to perpetrate massive DDoS attacks – Mirai, Wirex, and Reaper, to name a few. 38% of IT decision makers say their company has suffered a DDoS attack over the past twelve months.[2]

If you've been lucky enough to dodge the DDoS bullet, congratulations! However, the time may come when you're caught in a DDoS attack's crosshairs and we want to make sure you're prepared. To ensure you are taking appropriate security measures and deploying effective DDoS protection, you should understand all the potential repercussions a cyberattack can have on your business.

This white paper takes you through the top three impacts of a cyberattack, so you can better quantify the impact a DDoS attack can have on your business.

[1] https://appinventiv.com/blog/8-statistics-prove-iot-will-become-massive-2018
[2] https://www.a10networks.com/sites/default/files/resource-files/A10-TPS-GR-The_New_Threat_The_IoT_DDoS_Invasion.pdf

## *MAKING SENSE OF CYBERATTACK COSTS*

We've all seen the statistics on the costs of cyberattacks. By 2021, it's estimated cybercrime damages will cost the world $6 trillion annually.[3] But what do these numbers really entail and how do they apply to you?

The answer isn't straightforward. One of the best ways to understand what a cyberattack could cost your business is to try to quantify all the potential impacts. For this, we can look at what insurers look at as a guide to assessing what a cyberattack could do if it infiltrates and disrupts your business.

Industry watchers put the cyber insurance market between $1.3 billion[4] to $3 billion back in 2016. Assuming a compound annual growth rate (CAGR) of almost 28% for six years, experts put the future of cyber insurance at $14 billion, globally, by 2022.[5] This is quite a big leap, but not unexpected, since the risks of a wide variety of cyberattacks continue to persist and the damages when an attack, like a DDoS attack, is successful continue to grow.

### Cyber Insurance Growth Rate

**$3 BILLION**

Market in 2016

**$14 BILLION**

Market expected in 2022

Supplemental cybersecurity and identity theft coverage only became a regular part of the insurer's annual statutory financial statements in 2014. Since that time, insurers have been ramping up their cybersecurity insurance offerings, and companies have been buying stand alone policies that will help them mitigate the losses associated with a cyberattack. Some industries, particularly those that deal with a lot of personal information (PI) and are heavily regulated, have been quicker on the uptake - for instance, in the U.S., approximately 78% of hospitals are secured with cyber insurance[6] - but companies of all sizes and types have been looking at what an attack could mean to their business and taking measures to ensure they are appropriately covered.

[3] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[4] https://www.insurancejournal.com/news/national/2017/06/23/455508.htm

[5] https://www.alliedmarketresearch.com/press-release/cyber-insurance-market.html

[6] https://www.alliedmarketresearch.com/press-release/cyber-insurance-market.html

## 1 DATA, DATA, DATA

First and foremost, you need to understand what you have to protect. Data has been called the "new oil" – it's what powers our connected world and fuels our businesses. So, what happens when access to your data is disrupted? What happens when a DDoS attack makes your resources unavailable and leads to a data compromise?

Some data is obviously more important than other information, but, on average, Ponemon Institute estimates every lost or stolen record costs businesses $225.[7] A complete set of credit card data (name, payment card number, expiration date, social security number, date of birth and the three-digit security code) goes for much less - $30 to $45 dollars on the black market in the U.S. and Europe - while credit card dumps (all the information on the magnetic strip of the card) go for $200 and $300 apiece.[8] Medical records can go for even more. And stolen or lost devices (smartphones, laptops, etc.) can start a bidding war on the darkweb, depending on what they contain.

> The 2017 IP Commission Report estimates the annual cost to the U.S. economy due to counterfeit goods, pirated software and theft of trade secrets exceeds $225 billion annually and might actually be as high as $600 billion.

How much intellectual property (IP) do you hold? Do you have innovations or unique processes that give you a competitive advantage in the market? What kind of personal information (PI) do you collect or store? Note, PI in Europe is defined more broadly than the personally identifiable information (PII) covered by regulations within the United States. Understanding what access to your data means to your business is the first step in understanding how important it is to protect it.

[7] https://www.itspmagazine.com/from-the-newsroom/a-cyber-attack-costs-a-lot-more-than-you-think

[8] https://www.ontrack.com/blog/2017/02/23/black-market-data/

[9] http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

## 2 BUSINESS DISRUPTION

Qualifying the disruption a cyberattack can create is another important factor to assessing all its potential impacts on your business. There are lost opportunity costs, reductions in productivity and cycles spent investigating, documenting and recovering from the incident. Some breaches are easier than others to shut down, contain and completely remediate; on average, it takes organizations 46 days to resolve a cyberattack, at an average cost of $21,155 a day.[10]

Small businesses, who often don't have a lot of cybersecurity resources or expertise, can take days, even weeks to recover[11] ; unfortunately, some never do – 60% of small companies are out of business in six months after a cyberattack[12]. Large enterprises may be more resilient, but not by much – a report by Ponemon Institute found that 66% of organizations are not confident in their ability to recover from a cyberattack.[13]

Once an attack is remediated, there are all the ongoing post-breach activities and costs that are triggered and need to be accounted for. Some post breach expenses come from notifying customers who are affected by the attack, setting up and manning call centers, providing ongoing identity or credit monitoring services, etc. Others relate to regulatory defenses, penalties and fines that are the result of being found out of compliance with the laws and regulations that govern your industry and business operations. These costs are going up.

For example, the General Data Protection Regulation (GDPR) contains strict guidelines around the collection, use, and storage of PI. The regulations apply not just to organizations based in the EU, but any organization that processes the data of EU residents. If data is compromised due to noncompliance, companies will face fines up to €20 million (about $24.5 million) or 4% of global annual revenue for the previous financial year, whichever is higher.[14]

Summing up the operational expenses, disruptions and subsequent penalties of a cyberattack can help you put in perspective the value on preventing an attack in the first place.

[10] http://www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4

[11] https://blog.ext.hp.com/t5/BusinessBlog-en/54-days-to-recovery-The-impact-of-cyber-crime/ba-p/6720

[12] https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/

[13] https://www.techrepublic.com/article/66-of-organizations-wont-recover-after-cyberattack-study-says/; https://www.prnewswire.com/news-releases ibm-and-ponemon-study-reveals-organizations-remain-unprepared-to-respond-to-cyberattacks-300364234.html

[14] https://www.gdpreu.org/compliance/fines-and-penalties/

## 3 CUSTOMER TRUST AND VALUE

When customers choose to work or transact with you, they choose to trust you. They trust that you will protect their sensitive information and maintain the integrity of your dealings. The moment that trust comes into question, customers are hesitant to engage with you. This can hurt your business in both the long and short-term.

A quick hit to a company's stock price often follows a breach. While the company's stock price often rebounds,[15] the recovery can be a long time coming – Comparitech noted that three years after a breach, the NASDAQ ultimately outperformed companies who suffered a sizable breach by a margin of more than 40%.[16]

For breaches that involve particularly sensitive information that ultimately disrupt or damage the lives of the company's customers, those customers have been known to turn to litigation. Legal fees and settlements can easily cost companies hundreds of thousands to millions of dollars. Often the company must reimburse customers not only for past damages, but also pay for ongoing identity/credit monitoring services that shield customers from being the victim of future exploits.

**CUSTOMERS TRUST THAT YOU WILL**
**PROTECT THEM**

## MITIGATING THE DAMAGES

Cyber insurance can help mitigate the costs of a cyberattack, but one of the best ways to protect your business is to deploy effective security technologies and measures that can stop the attack in the first place or at the very least minimize its damage. Being able to demonstrate you took all precautions possible to protect your data and operations goes a long way to help you preserve your business value and customer trust.

[15] https://s2erc.georgetown.edu/sites/s2erc/files/documents/breachwriteup_pdf_final.pdf

[16] https://www.comparitech.com/blog/information-security/data-breach-share-price

## WHAT CAN YOU DO TO PROTECT AGAINST DDoS ATTACKS?

### You can deploy a DDoS defense solution that is:

- Precise, with the ability to intelligently distinguish legitimate users from attacking bots.
- Scalable, with the ability to understand the intensity and breadth of an attack, based on packets per second and millions of geographically distributed attacking agents.
- Automated, with the ability to eliminate the manual intervention often required to defend against attacks.
- Affordable, with the ability to deliver high-performance, yet be compact by design to reduce the total number of solutions needed to meet your organization's capacity requirements.

## ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com
or tweet @A10Networks.

## LEARN MORE
ABOUT A10 NETWORKS

CONTACT US
*a10networks.com/contact*

Part Number: A10-WP-21151-EN-01 JULY 2018