OCTOBER 2015

# NEUSTAR DDOS ATTACKS & PROTECTION REPORT: NORTH AMERICA & EMEA

## THE CONTINUOUS RISK TO DIGITAL BRANDS


neustar®

# CONTENTS

# INTRODUCTION

## IN THIS REPORT:

**U.S. AND EMEA: PROTECTION NEEDS INCREASE AS THE THREAT BECOMES CONTINUOUS**

In the summer of 2015, Neustar surveyed 760 managers and directors, CSOs, CIOs, CTOs, and others in the security and IT fields to learn how companies in North America and the EMEA region (Europe, the Middle East, and Africa) encounter and defend against DDoS attacks. Key industries sampled were financial services (17% of respondents), retail (17%), and technology (15%). In North America, 73% of participating companies generated $1B+ in annual revenue. In EMEA, 51% generated €400M a year.

**The findings show a clear trend: businesses are shifting from dealing with isolated DDoS attacks to managing a continuous threat, one with compounding impact.** The danger is defined by the sheer number of companies attacked, how many are attacked repeatedly, and the damage to brand reputations.

For the past couple of years, Neustar has provided two separate reports for North America and EMEA. Now we present a consolidated report, in which 760 executives and professionals from around the world share their experiences in contending with DDoS attacks.

## 50% OF NORTH AMERICAN AND EMEA COMPANIES ATTACKED

Half of all companies surveyed were attacked either in 2014 or early 2015.

## 83% ATTACKED REPEATEDLY

Over 8 in 10 businesses attacked suffered more than one DDoS attack. 54% were hit 6+ times.

## Over 1/3 DISCOVERED MALWARE

36% found malware or viruses as a result of DDoS attacks.

## 1 IN 4 EXPERIENCED THEFT OF DATA OR FUNDS

DDoS attacks aren't a mere nuisance; they plunder the bottom line.

## 1 IN 5 WERE ALERTED TO ATTACKS BY CUSTOMERS, PARTNERS, OR OTHER THIRD PARTIES

Result: Those attacked were the last to know and suffered damage to their brands.

The following section examines the risks in more detail.

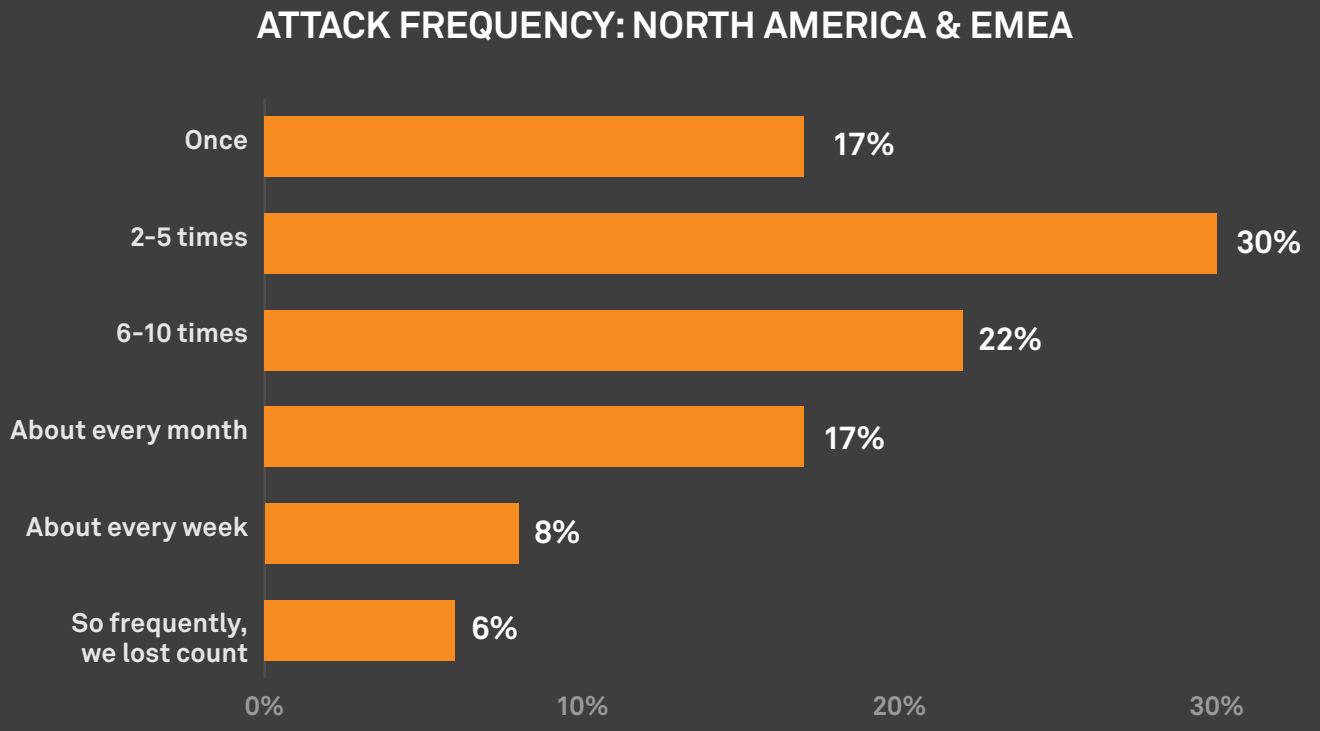
# ASSESSING RISK

**DDoS attackers are persistent. Most companies they target suffer multiple strikes.**

**Not If, Not When, But How Often**

## **83%** OF COMPANIES WERE **ATTACKED REPEATEDLY**. **54%** WERE **ATTACKED 6+ TIMES**.

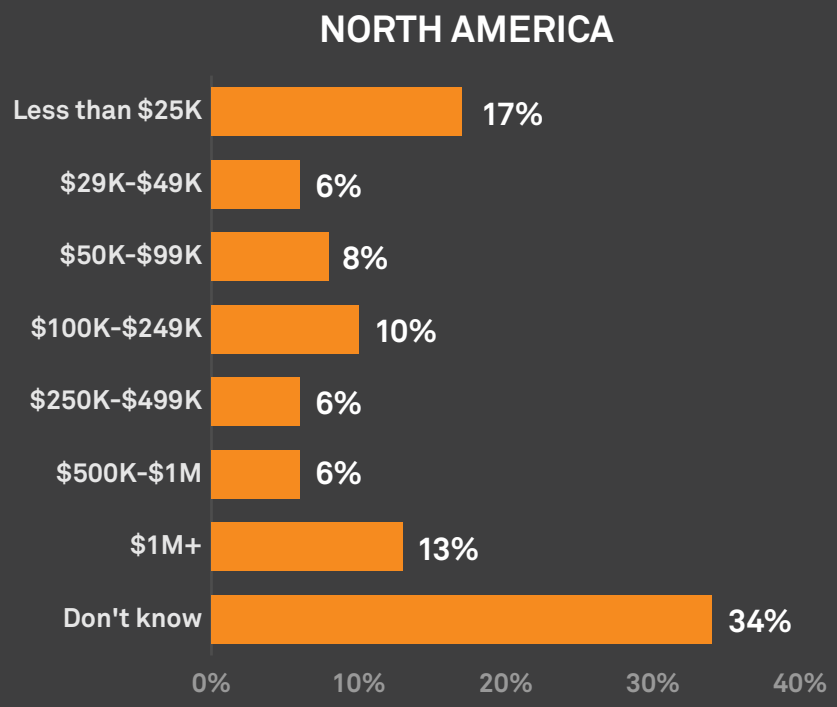
DDoS attacks are typically not an isolated incident. Companies hoping they'll just go away meet a sobering reality: most targets are hit again and again.

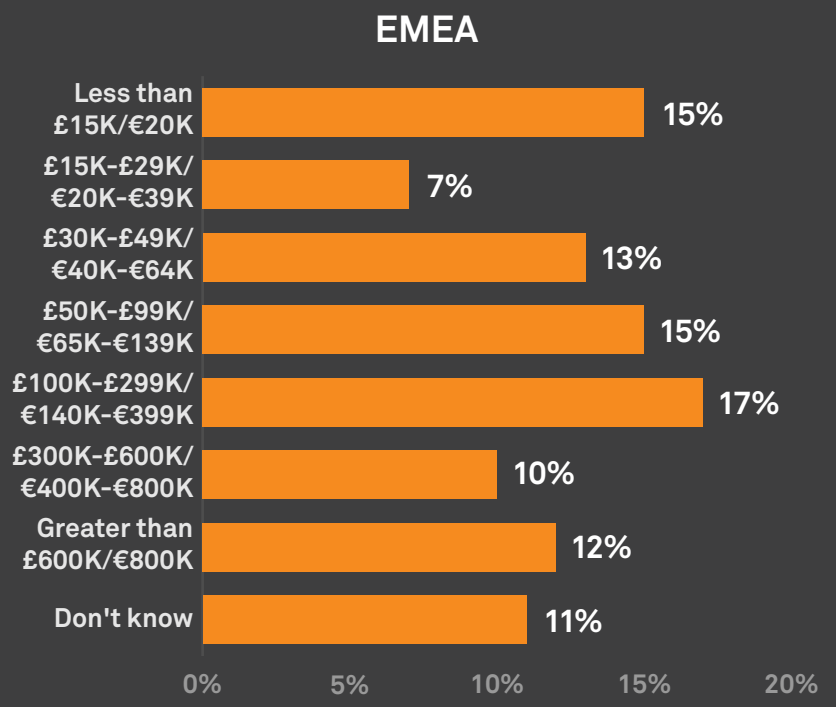


## BIG MONEY IS AT STAKE

North American and EMEA businesses perceive DDoS as a grave danger—44% say the threat is now bigger, while 45% say it's as large as the year before. Potential revenue losses are one key reason why.

### HOURLY REVENUE LOSSES DUE TO OUTAGES AT PEAK TIMES



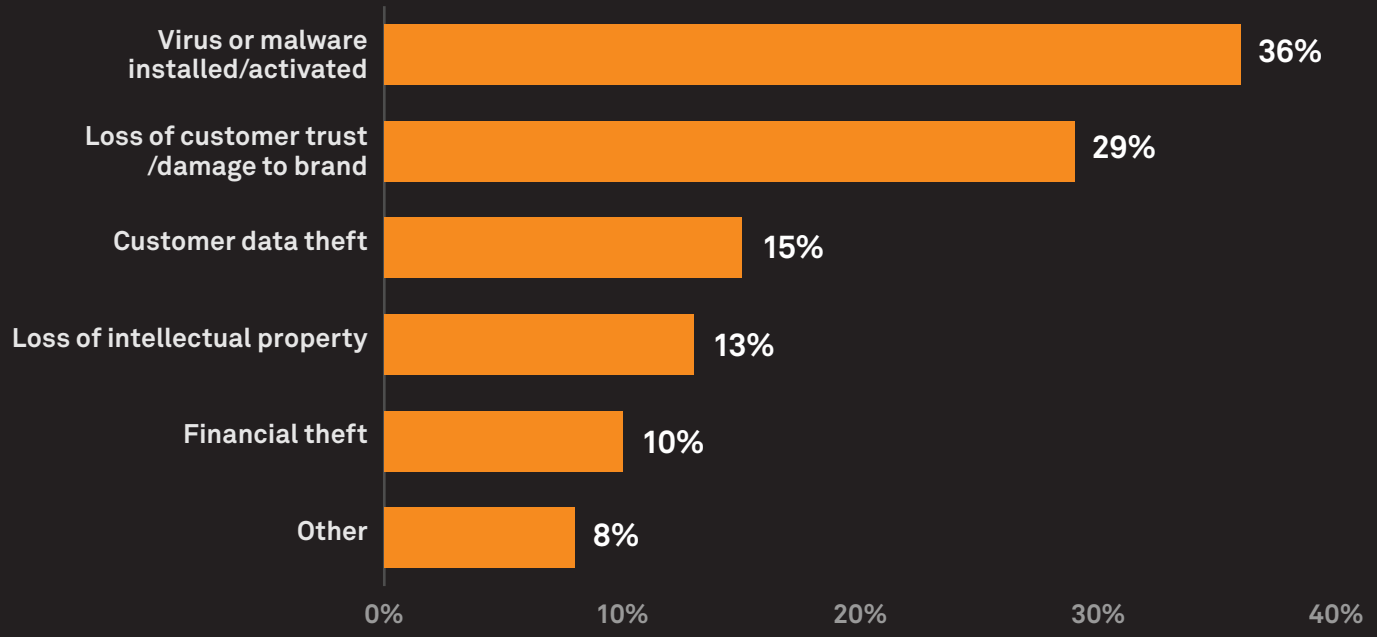

**In North America, 35% would lose over $100K per hour in a peak-time DDoS outage.**

**In EMEA, 39% would lose over €100,000 per hour in a peak-time DDoS outage.**

**The Tip of the Blade**

## OVER **1 IN 3** DDOS ATTACKS PLANT **MALWARE** OR A **VIRUS**. NEARLY **40%** OF TARGETS EXPERIENCE **THEFT**.

### RESULTS OF DATA BREACH OR THEFT SUFFERED AS A RESULT OF 2014 DDOS ATTACK: NORTH AMERICA & EMEA




*Multiple responses allowed.

A recent report by Neustar and The Ponemon Institute revealed that 63% of consumers distrust brands that have suffered a data breach. Even a year after a breach, over 50% of people still view the brand in negative terms.

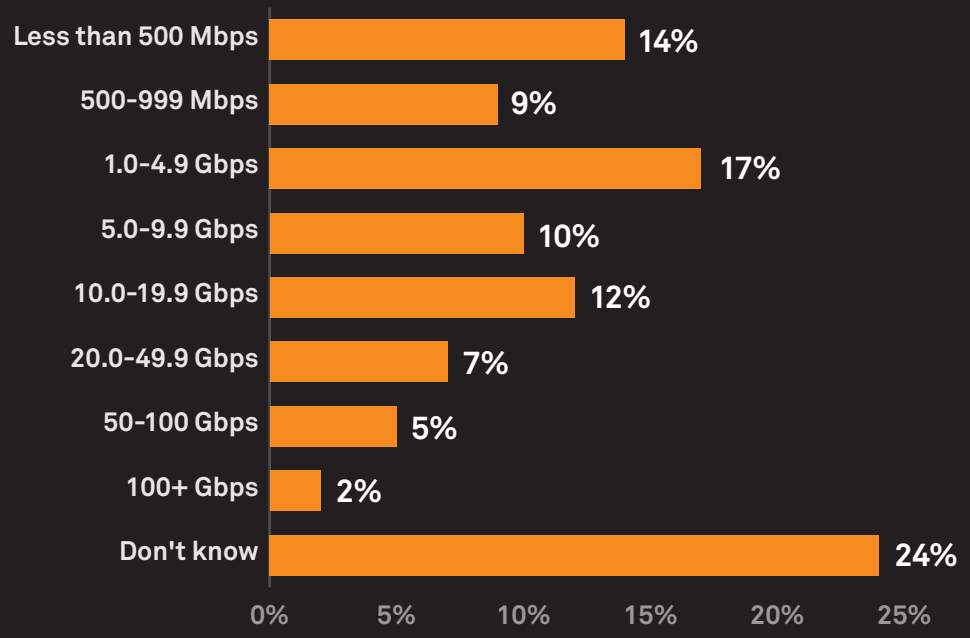
Source: "What Erodes Trust in Digital Brands," Neustar, August 2015.

**Punching Above Their Weight**

## 40% OF ATTACKS ARE UNDER 5 GBPS—NOT ENORMOUS, BUT LARGE ENOUGH TO CAUSE REAL TROUBLE.

A DDoS attack of 1 Gbps can often take down a website. Even attacks less than 1 Gbps can disrupt operations and smokescreen a greater threat like malware installation.

### ATTACK SIZE IN BANDWIDTH: NORTH AMERICA & EMEA

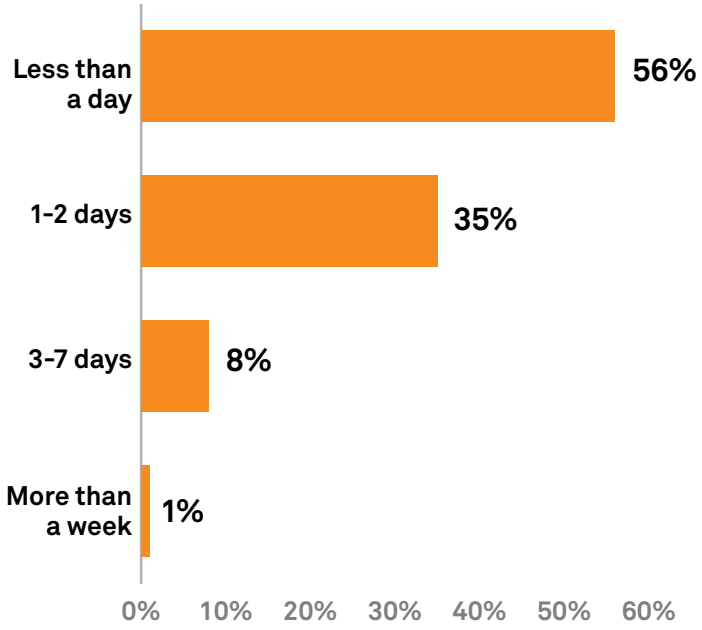



**Cancel Those Dinner Plans**

## 41% OF ATTACKS LASTED LONGER THAN A DAY.

Nearly **1 in 10 lasted from 3 days** to over a week.

### DURATION OF LONGEST ATTACK: NORTH AMERICA & EMEA



**MARK TONNESEN**
CIO and CSO, Neustar

## WHY "SMALLER" ATTACKS DESERVE MORE ATTENTION

### A Security Expert's Point Of View

Neustar's top security executive shared his thoughts on the popularity of attacks under 5 Gbps.

"If the attacker's goal isn't to cause an outage but to disrupt, he doesn't need to craft an attack of extra-large proportions. A SYN Flood attack is a good example. The attacker sends enough SYN requests to a company's system to consume server resources and stall legitimate traffic. It's a kind of 'low and slow' DDoS attack—steady and problematic, though not tsunami-like.

**"Why saturate the pipes if you can't access the network?"**

"In launching such an attack, the attacker accomplishes several things: he disrupts operations, distracts the website and security teams, and makes sure the target network is still operational—that is to say, accessible. Now the attacker can go in and plant malware or a virus, setting the stage for data theft, siphoning funds, or whatever else.

"Think about it: why saturate the pipes if you can't access the network? Doing the reverse lets attackers harass a target and set the stage for exfiltration. In this sense, a so-called smaller attack can be more dangerous than a huge one that knocks you offline but may not result in a data breach."

# MEASURING BUSINESS IMPACT

**DDoS attacks don't just ruin the IT department's day. They affect the call center, customer service, sales, and your brand. When attacks reoccur, the business impact adds up.**

**No Department Is Immune**

## COMPANIES **FEEL THE STING** IN CUSTOMER-FACING AREAS.

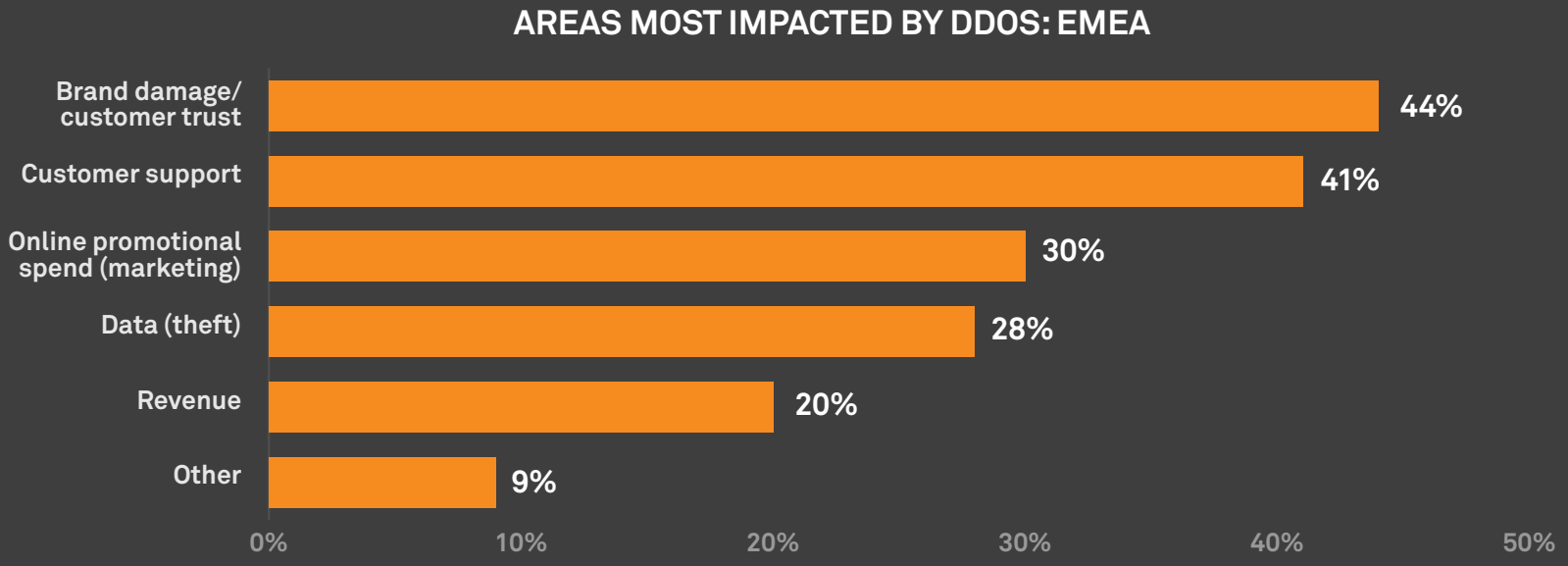
Once solely considered a security or IT problem, DDoS attacks now ripple through every part of the business.

**Top 3 Areas Affected by DDoS Attacks: NORTH AMERICA & EMEA**

1. **Customer Support (41%)**
2. **Brand Damage (35%)**
3. **Marketing/Online Promotional Spend (25%)**

*Multiple responses allowed.

## IN EMEA, THE IMPACT IS ESPECIALLY WIDESPREAD

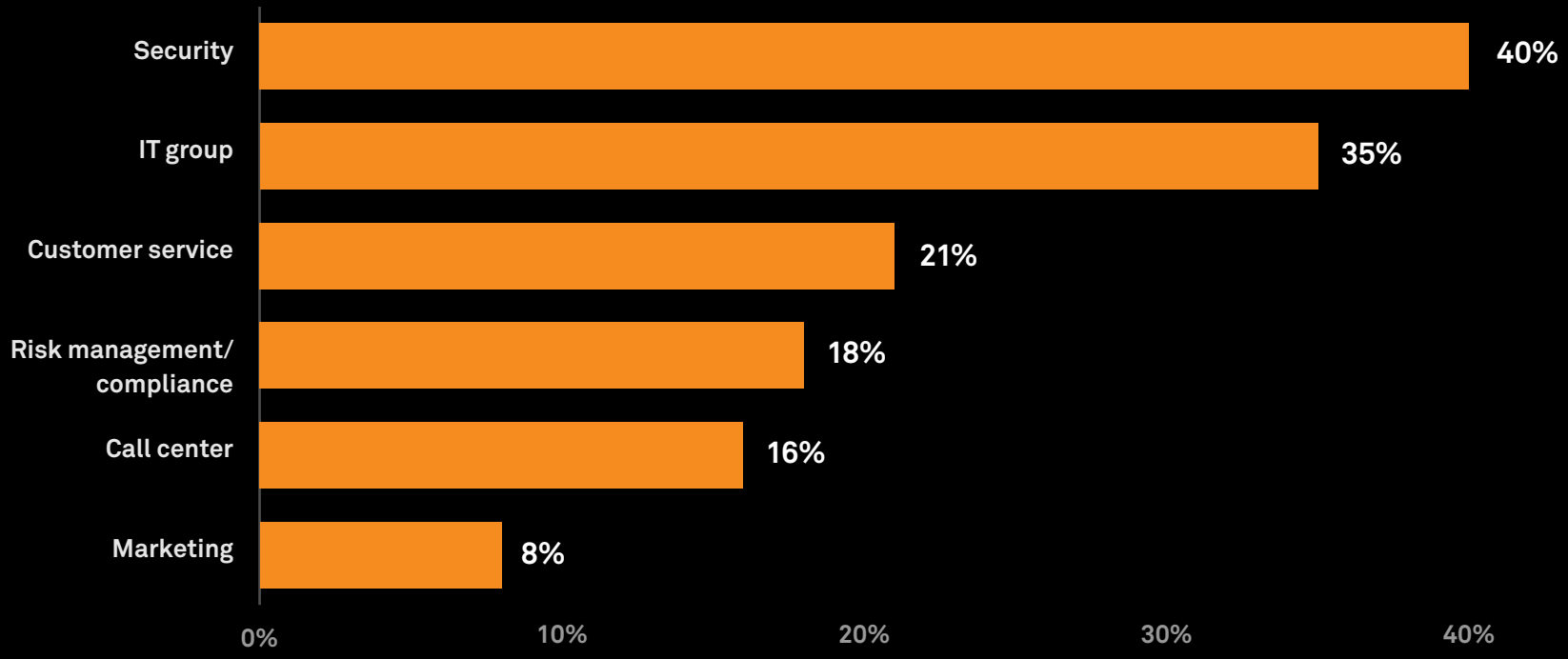



*Multiple responses allowed.

**The Financial Pain Is Shared, Too**

## **63%** REPORT **COST INCREASES** IN AREAS BEYOND SECURITY AND IT.

### DEPARTMENTS WITH GREATEST DDOS-RELATED COST INCREASES: NORTH AMERICA & EMEA



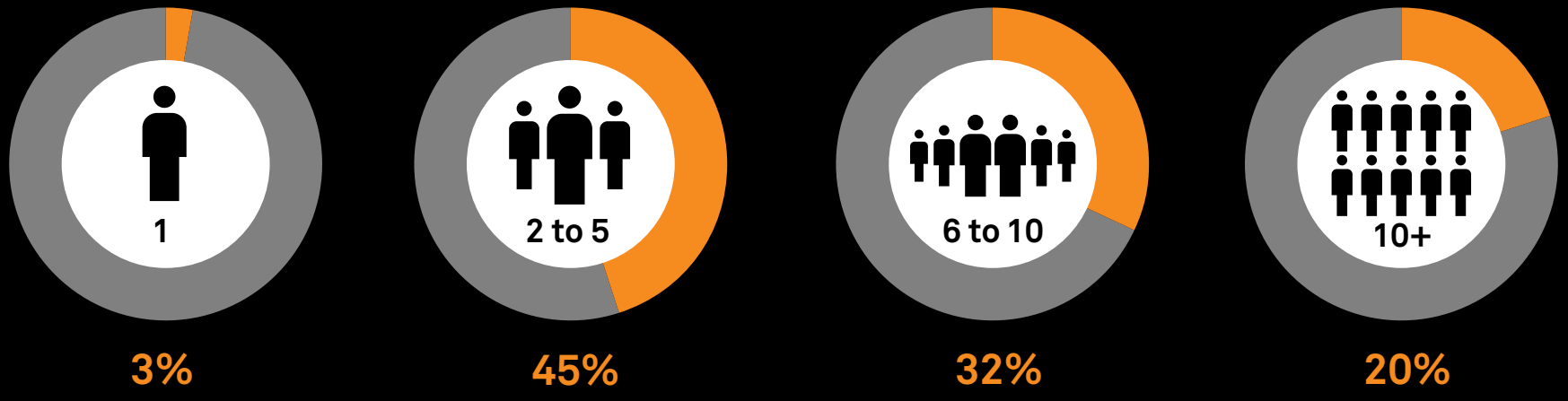

*Multiple responses allowed.

**The Impact On Staff**

## OVER **50%** OF COMPANIES USE **6+ PEOPLE** TO MITIGATE ATTACKS.

This hidden cost adds to the bottom-line impact.

### MANPOWER REQUIRED TO MITIGATE ATTACKS: NORTH AMERICA & EMEA



A Lesson from One Retailer:

# REPEAT ATTACKS = AMPLIFIED BUSINESS IMPACT.

What happens when you're hit with DDoS repeatedly? Let's examine one French retailer. Based in Paris, the company has a major e-commerce presence, with total annual revenues of €400-675 million. Peak-time revenue risk from outages: €140,000-€399,999 per hour.

**ANNUAL FREQUENCY OF ATTACKS:**

2-5 Times

**REPORTED DAMAGE FROM ATTACKS**

Customer Data Theft, Malware/Virus Insertion

**NUMBER OF STAFFERS NEEDED TO MITIGATE**

2-5

**COMBINED DETECTION AND RESPONSE TIMES**

Up To 24 Hours

## SO HOW IS THIS RETAILER RESPONDING?

Currently this business has no DDoS-specific protection, relying solely on WAFs, switches, and firewalls. Attacks take 6-12 hours to detect and another 6-12 hours to mitigate. The retailer now reports that it sees DDoS attacks as a bigger threat and plans to invest more heavily in defense.

## THE FINANCIAL IMPACT IS REAL.

Here's the estimated cost of a 24-hour attack on this retailer based on respondent data.

| IMMEDIATE COSTS | |
|---|---|
| Lost revenue | **€1,974,000** (35% revenue decrease due to cart abandonment from slow load times) |
| IT staff to mitigate attack | **€4,128** (3 dedicated staffers x €41 per hour each x 24 hours) (1 manager x €49 per hour x 24 hours) |
| **TOTAL** | **€1,978,128** |
| **IMPACT COSTS** | |
| Wasted marketing spend | **€70,000** (€350,000 campaign with 20% degradation) |
| Brand damage | **€4,020,000** (€201 per lost or stolen record x 20,000 customers - Source: Ponemon Institute's 2014 Cost of Data Breach Study) |
| Lost customers | **€626,865** (Estimated customer lifetime value of €2,645 x 711 customers) |
| Call center increases | **€41,455** (8,291 additional calls @€5 each) |
| **TOTAL** | **€4,758,320** |
| **GRAND TOTAL** | **€6,736,448** |

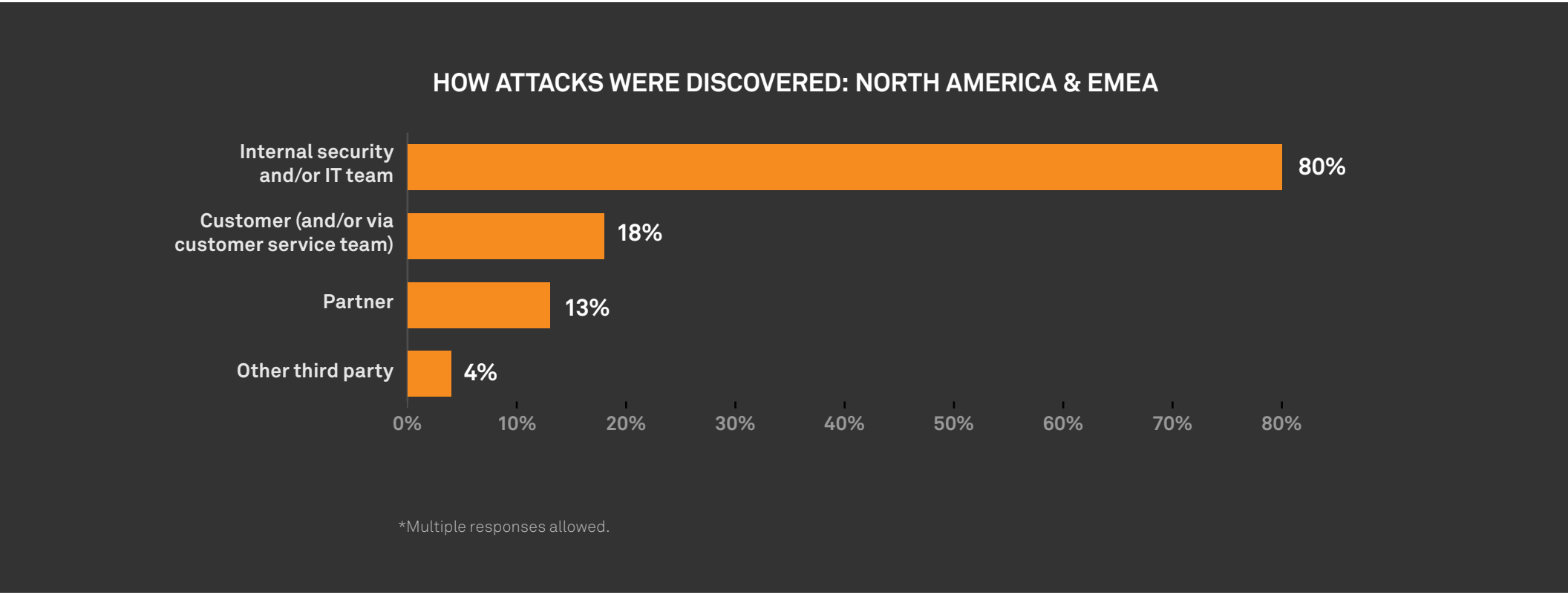
**Multiplied 2-5 times** to account for repeat attacks...
And the **grand total** potentially **= €13,472,896 to €33,682,240**

Attacks tend to vary in their business impact, so in real life of course these figures could be lower. Much depends on whether the target company upgrades its protection.

**Ouch.**

## **1 IN 5** BUSINESSES WERE **ALERTED** TO DDOS ATTACKS **BY A CUSTOMER, PARTNER, OR OTHER THIRD PARTY**.

When surprises like this happen, it's bad news for the brand.




*Multiple responses allowed.

In EMEA, 36% of the 200 firms attacked were notified of the attack by a third party. Of those, 79% (4 out of 5) experienced a breach that also involved theft.

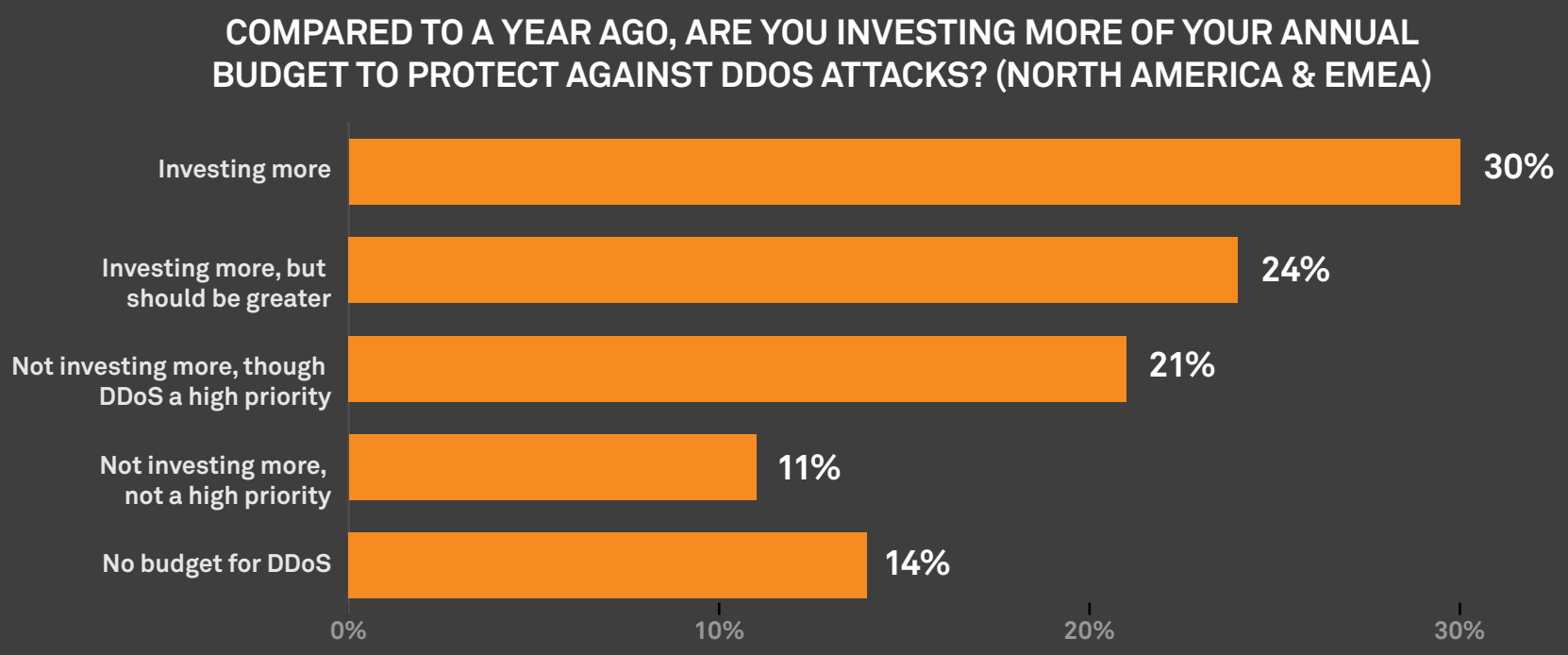
# UNDERSTANDING PROTECTION TRENDS

**In both regions, mitigation investment is rising.**

**Attackers Have Your Attention**

## 54% OF COMPANIES ARE INVESTING MORE IN DDOS PROTECTION.

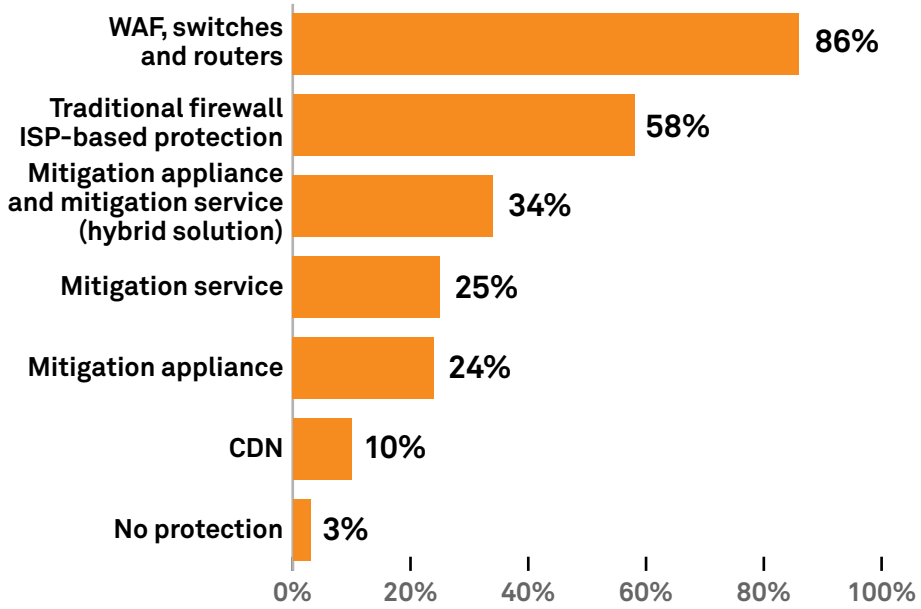
Nearly 1 in 5 businesses are not only investing more but believe their investment should be even greater.



**Clinging To What They Know**

# MORE THAN 60% OF BUSINESSES STILL MITIGATE WITH TOOLS NOT PURPOSE-BUILT FOR DDOS.

## TYPES OF DDOS PROTECTION USED: NORTH AMERICA & EMEA




*Multiple responses allowed.

**However, in EMEA the story changes.**

Facing more frequent attacks:

- 46% of EMEA businesses use best-in-breed hybrid protection
- 40% rely on a third-party service
- 33% use a mitigation appliance

## DDOS-SPECIFIC DEFENSES ARE ON THE RISE (2015 v. 2014): NORTH AMERICA & EMEA

**34%**

20%

**DDoS Hybrid Solution**
**(mitigation appliance and service)**
34% (up from 20%)

**25%**

14%

**DDoS Mitigation Service**
25% (up from 14%)

**24%**

15%

**DDoS Mitigation Appliance**
24% (up from 15%)

**Learn From Those Who Got Hit The Most**

## HYBRID ADOPTION IS EVEN GREATER AMONG COMPANIES THAT HAVE BEEN ATTACKED.

**67%** of companies attacked now use hybrid protection. Again, over half of those companies were hit **6+ times in a year**

**67%**

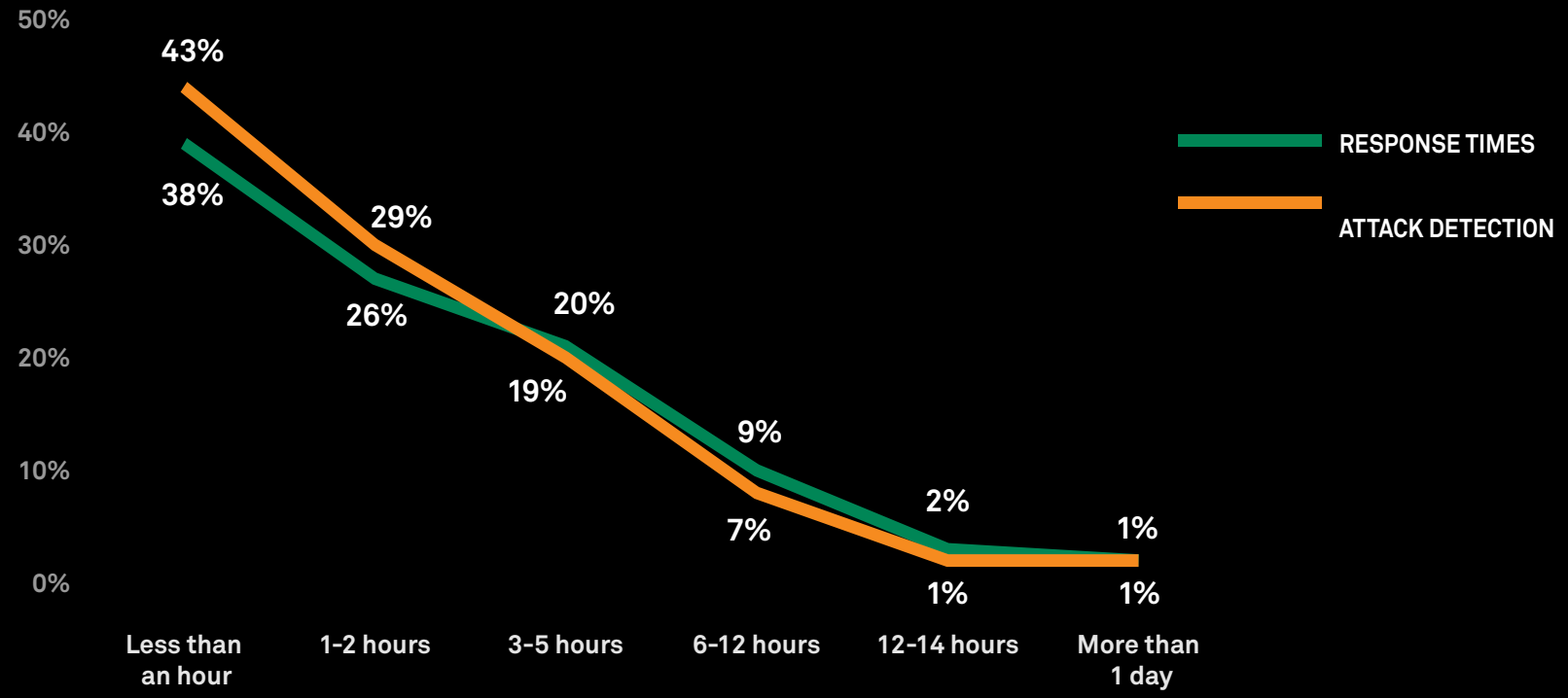
As companies experience multiple attacks and absorb impact and cost increases throughout their operations, the hybrid combination of DDoS appliance and cloud-based mitigation is emerging as the defense of choice. With hardware to block Layer 7 (application) and short-lived attacks, and cloud-based capacity to scrub higher volumes of malicious traffic, businesses with hybrid protection are faster in detecting and responding to attacks.

**Security Practices: Accountability is Tightening**

Some businesses still roll the dice and take little or no action against DDoS attacks. However, as attackers use DDoS to launch more lethal action such as data theft and malware infestation, authoritative bodies are holding corporate executives to account. Fines and terminations are already a reality. Heavier enforcement, brought about by broadened regulatory power, is gaining the attention of business decision-makers. For example, in the area of data security alone, the U.S. Federal Trade Commission has reached more than 50 settlements with companies over poor security practices.  Recent court judgments have only extended the governance and authority of the FTC to hold organizations accountable.

Source: Federal Trade Commission Business Center, "Start with Security: A Guide for Business," https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

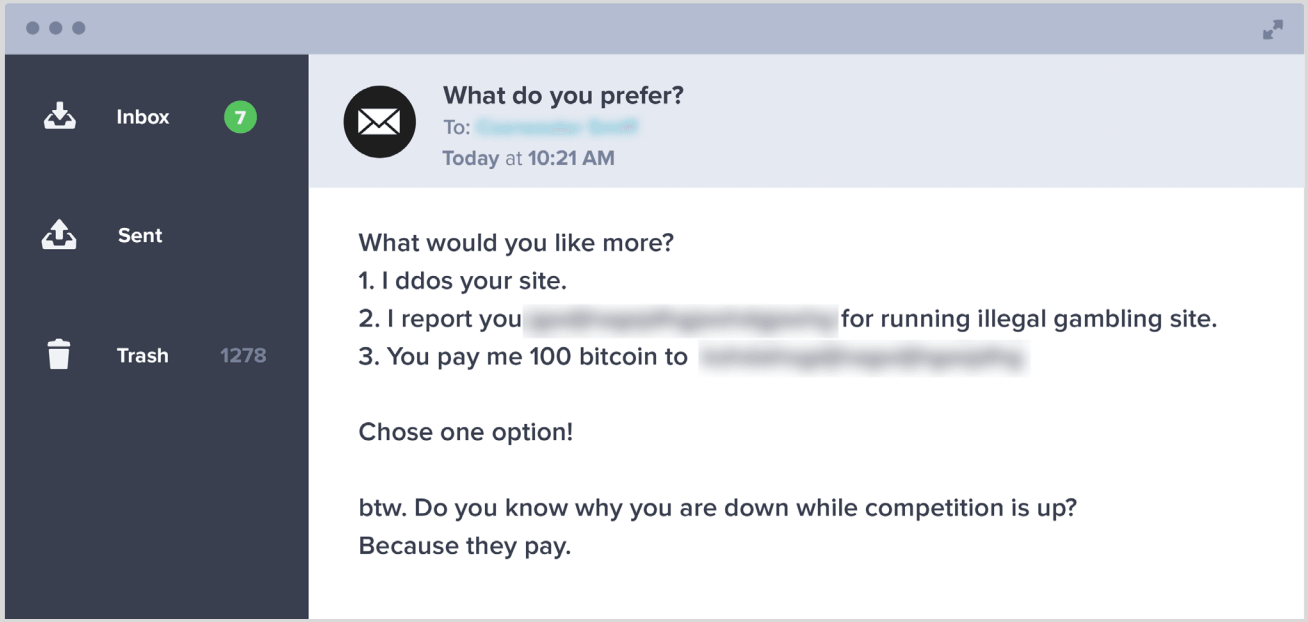
## ATTACK DETECTION AND RESPONSE TIMES: NORTH AMERICA & EMEA



# “PAY UP OR ELSE...”
## DDOS FOR RANSOM IN THE AGE OF DIGITAL CURRENCY.

The plot is old, but the methods are 21st century. On what seems like a typical Wednesday, your website suddenly goes offline. Shortly thereafter, an email pops up that claims responsibility and demands a form of digital currency in return for business as usual.

In slightly redacted form, here’s one ransom note.



The site, your job, and the profitability of your company are now held hostage. If your company is like 41% of those surveyed in this study, every hour of downtime during peak business means revenue losses greater than $100,000. Every minute counts. Going to law enforcement, while a good idea, takes time. And since the last victimized company paid, the precedent has been set.

**What Should You Do?**

Your options are limited: If you pay, your website will return online, but there's no guarantee you won't be attacked again—and ordered to pay more. If you don't cough up, your website remains offline, social media starts to buzz, and your brand reputation suffers. Either way, the hacker claims victory.

The other option is fighting back with a DDoS mitigation solution. If you have a solution in place—and it's purpose-built to protect against a variety of attacks— your odds of success are better. If you don't yet have a solution, it's a different cost to incur.

In the final analysis, you have to answer this question: which cost is more palatable, tomorrow as well as today?

# SUMMARY

## 5 KEY TAKEAWAYS FROM THIS REPORT

1. **It's not if, not when, but how often:** 50% of North America and EMEA companies suffered a DDoS attack, with over 8 in 10 targeted more than once.

2. **Attackers penetrate with purpose, using DDoS as a weapon:** When attacked, 50% of companies on both sides of the Atlantic reported some form of theft (customer data, intellectual property, financial). 36% of companies were infected with malware or viruses.

3. **When caught by surprise, brands can lose credibility:** 1 in 5 attacks were discovered by customers, partners, or other third parties.

4. **"Slow and steady" can have lasting repercussions:** Rather than trying to overwhelm networks, attackers often use a "slow and low" strategy, deploying smaller attacks to disrupt and distract, install malware, steal data or funds, and tarnish the brand.

5. **Companies know the threat is real:** 54% of North America and EMEA companies are investing more in DDoS protection as compared to a year ago.

**TO LEARN MORE ABOUT DDOS PROTECTION, VISIT NEUSTAR.BIZ**

To mitigate DDoS attacks, Neustar blends expertise, proven responses, and diverse technologies. Neustar SiteProtect, our DDoS mitigation service, offers options to meet your level of risk, budget, and technical environment: cloud-based protection; on-premise, always-on hardware; or a hybrid of both, fully managed by us. SiteProtect is backed by the Neustar Security Operations Center, whose experts bring years of experience to blocking every attack.

## ABOUT NEUSTAR

Neustar, Inc. (NYSE:NSR) is the first real-time provider of cloud-based information services, enabling marketing and IT security professionals to promote and protect their businesses. With a commitment to privacy and neutrality, Neustar operates complex data registries and uses its expertise to deliver actionable, data-driven insights that help clients make high-value business decisions in real time, one customer interaction at a time. More information is available at **www.neustar.biz**.

neustar®



RPRT-DDoS-1056 09292015