
# DDoS Attacks: Mitigation and Response Techniques to Minimize Downtime

# Presenters

- Eric McIntyre
  - Senior Director, DNS Business
  - CloudFloorDNS

- Vincent Geffray
  - Senior Director Product, IT Alerting
  - Everbridge

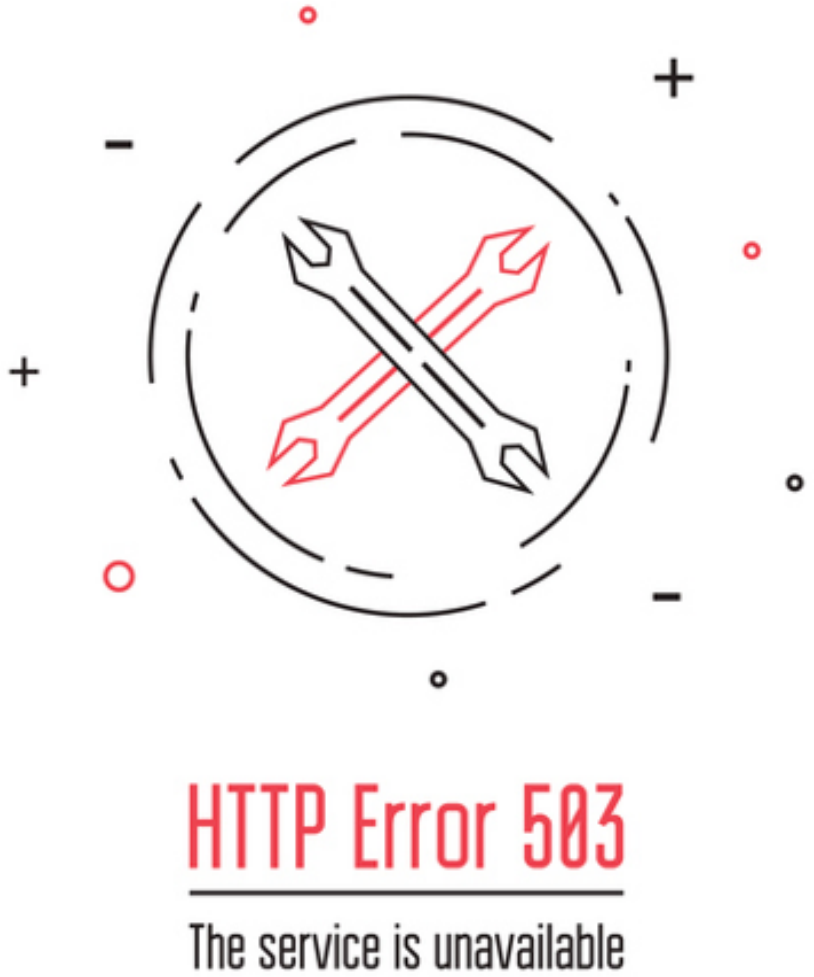
# What is a DDoS Attack?

+ A DDoS attack is a threat to your digital business

+ DDoS stands for (D)istributed (D)enial (O)f (S)ervice – designed to cripple or take down online services to effectively stop them from serving legitimate customers

+ Can be launched in a variety of ways and multiple attacks of different types at the same time

+ A DDoS Damages ability to serve customers, sell online, provide information to potential customers, effectively doing severe damage to your brand




CloudFloorDNS™
AN EVERBRIDGE SOLUTION

# DDoS Attacks are Growing

+ 64% of companies saw 2+ types of attacks, 32% 1 type of attack
+ Attacks are growing in size, avg size in Q1 2016 was 19.37Gbps
+ 41% of the attacks on companies were over 10Gbps
+ 182% increase in Qtr over Qtr since Q2 2015

Source: Verisign, DDoS attack stats, Q1 2016

+ 125.36% increase in Attacks from Q1 2015 to Q1 2016
+ 137.5% increase in Attacks over 100Gbps
+ 22.47% increase in Attacks from Q4 2015 to Q1 2016
+ 7.96% increase in Duration of Attacks -16.14 hours

Source: Akamai, State of The Internet, Q1 2016


CloudFloorDNS™
AN EVERBRIDGE SOLUTION

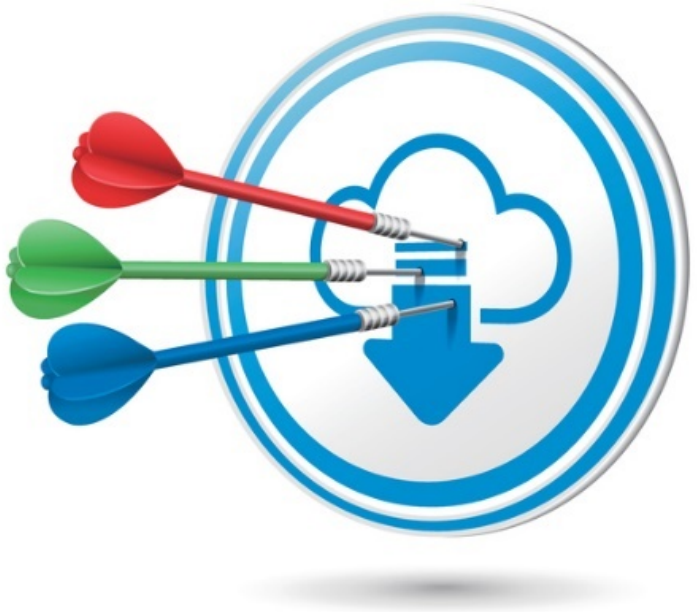
# Why do DDoS Attacks Happen?

+ Targeted – Your Business is a specific target – this can be the result of a disgruntled employee, customer or possible ransom attempt

+ Vertical Market – Certain Vertical Markets are more prone to attacks than others. High concentration of attacks on the following industries: IT/SaaS/Cloud, Financial, Entertainment and Public Sector

+ Bad Luck – Your organization is hosted on a DNS Provider, Web Server or other Cloud Service that happens to share resources with a targeted domain or service

+ Diversion – Attackers Divert attention with DDoS in order to distract Network and Security Personnel while attacking other resources



CloudFloorDNS™
AN EVERBRIDGE SOLUTION

# What happens during an Attack

+ Website, Email, API's, SaaS services and other online and cloud services can be degraded, offline or slowed to a crawl

+ Online Ordering and other customer facing apps and sites go offline

+ Attacks can last from minutes to many hours, many factors involved

+ You can't prevent an attack, its simply a matter of when it will happen to you. Preparation is key!

CloudFloorDNS™
AN EVERBRIDGE SOLUTION

# Types of DDoS Attacks

+ Volumetric Attacks – Flooding the pipes or consuming the Bandwidth. UDP and ICMP/PING Floods

+ Application Level Attacks – Targeting specific application
  Tends to be more Expensive, Difficult but targets specific applications

+ Amplification attacks are very common on services such as DNS and NTP, SSDP and other common protocols. Small query's result in big responses, clogging resources and the pipe

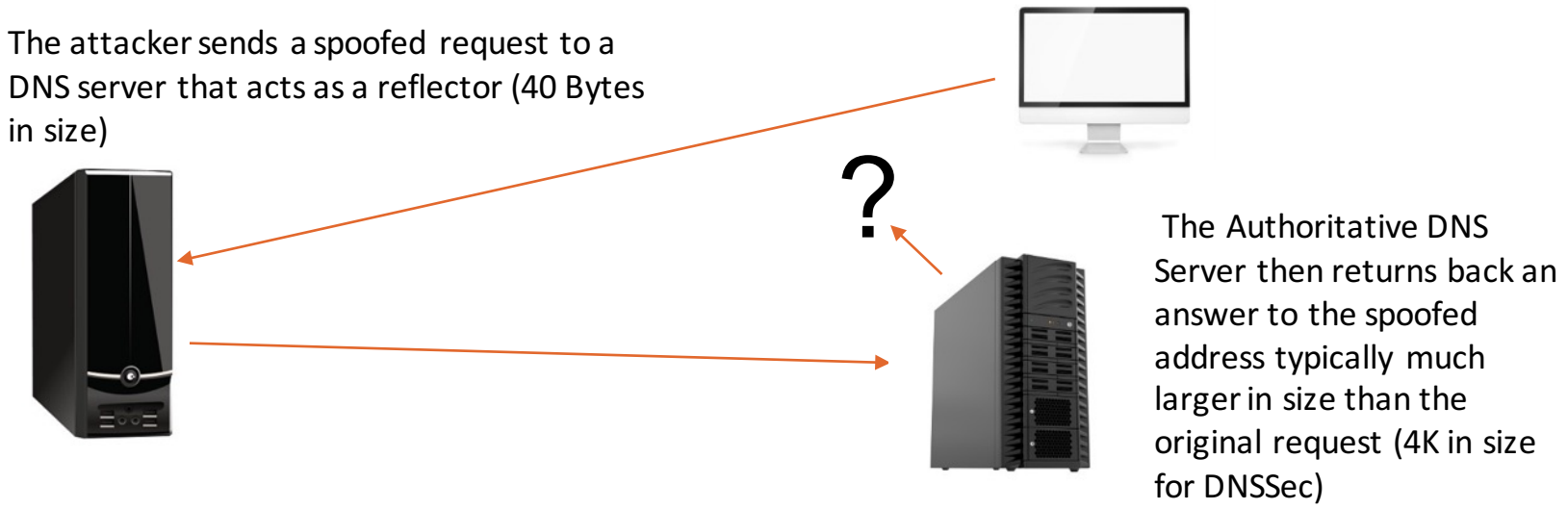
+ State Exhaustion attacks – or Protocol attacks
  Takes advantage of flaws in protocols, such as the Ping of Death which causes a buffer overload


CloudFloorDNS™
AN EVERBRIDGE SOLUTION

# Types of DDoS Attacks (Amplification)

+ Amplification attacks tend to be more common – Attacking DNS one very common type of Amplification Attack.

  Using UDP it's easy to spoof the source of the IP, attackers spoof the IP and send small requests that return a larger reply – hence Amplifying the original request by a certain factor.

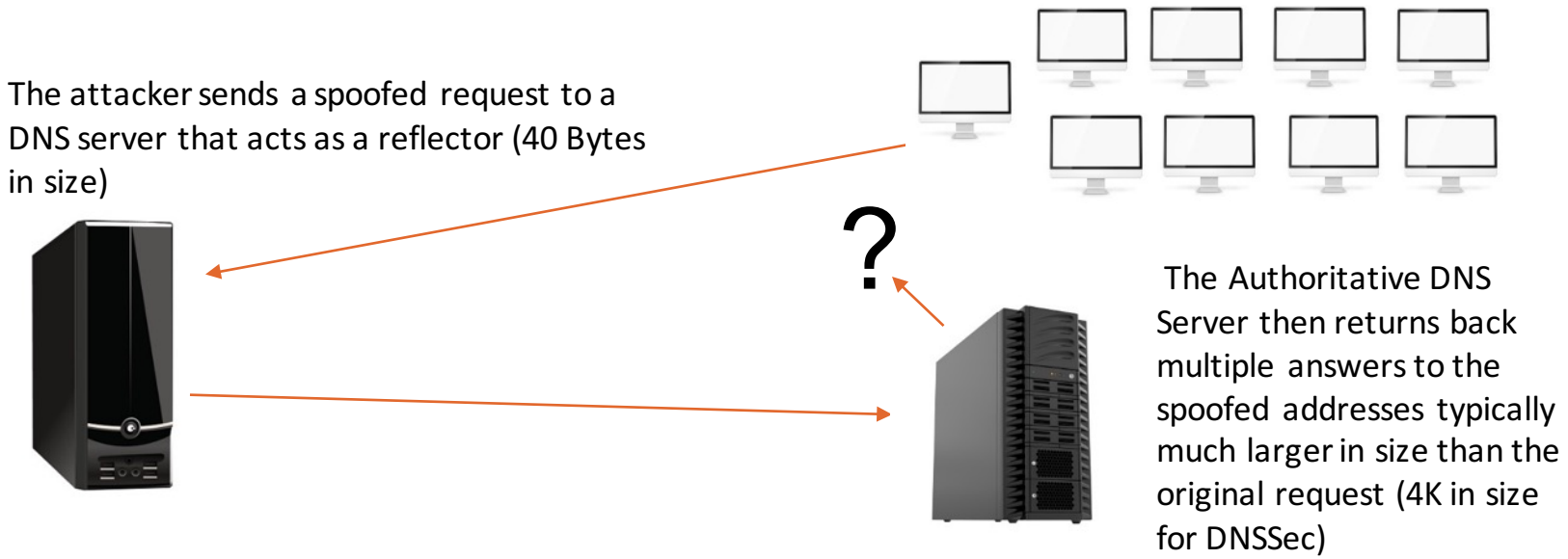



CloudFloorDNS™
AN EVERBRIDGE SOLUTION

# Amplification Attacks (Using Botnet)

+ Amplification attacks are typically launched using a Botnet – a large gathering of compromised systems controlled by hackers and available for "rent"

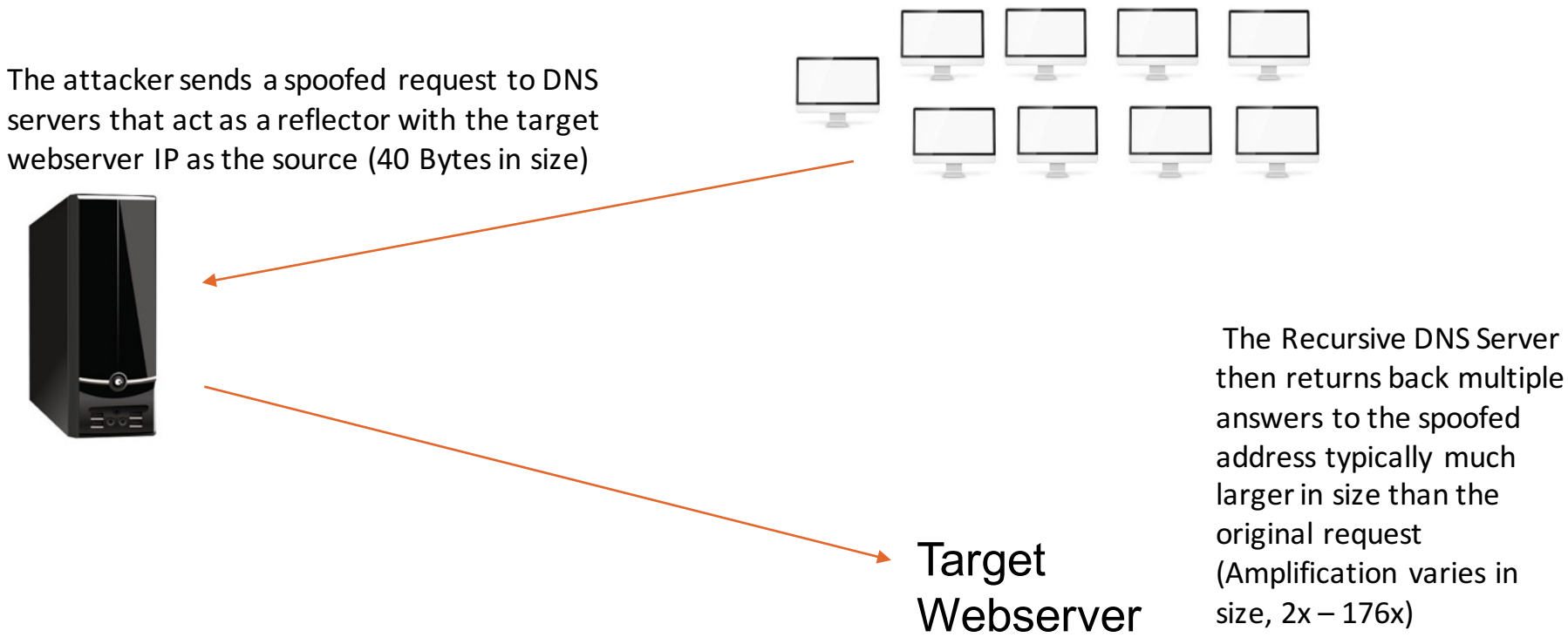
  The Botnet simply increases the requests and spoofed IP's and helps clog the pipe with useless data




CloudFloorDNS™
AN EVERBRIDGE SOLUTION

# Amplification Attacks (DNS Attacks)

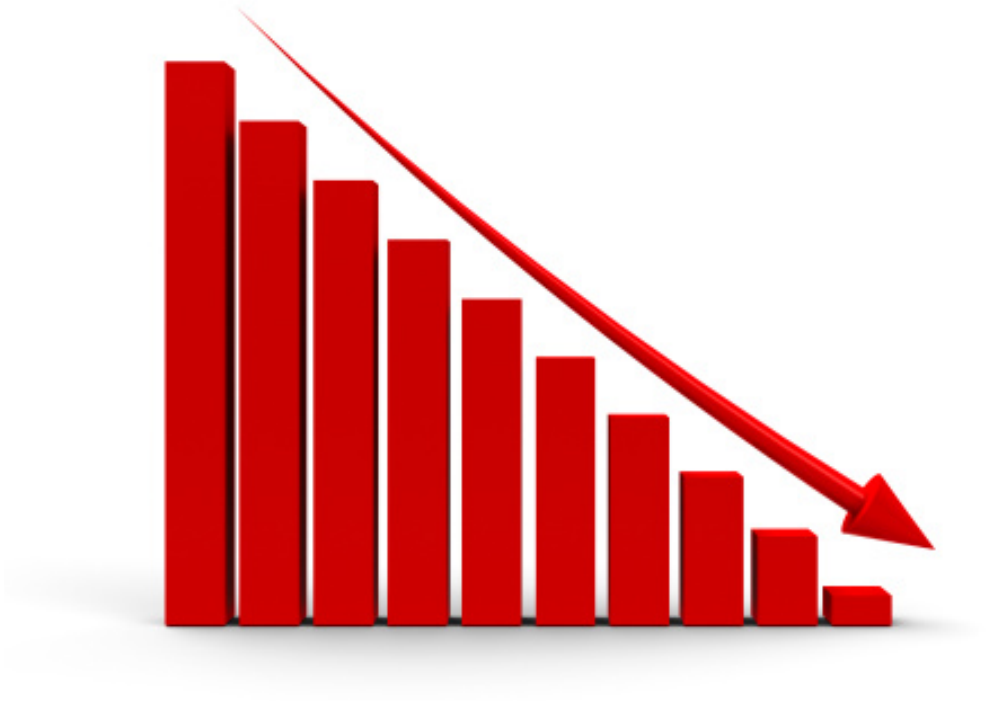
+ A DNS Amplified Reflective attack can be launched in a few different ways, this example reflects responses back to a victim website




CloudFloorDNS™
AN EVERBRIDGE SOLUTION

# Why Protect yourself against DDoS?

+ Service Outages are extremely costly!
+ Loss of Sales can cost you thousands per hour or more!
+ Loss of customers and new customer acquisition, Slow sites can be just as bad as being 100% offline
+ Damage to Brand Name and Brand Reputation



CloudFloorDNS™
AN EVERBRIDGE SOLUTION

# What to do during a DDoS Attack?

+ Have a DR/DP Plan in place BEFORE you get attacked!

+ Identify the Attack - volume and methods of Attack (MTTI)
  - What type of attack, locations, size in Gbps

+ Communication during an attack is critical!
  - Communicate Internally (operations, support, sales, mkt)
  - Communicate Externally to customers & Network Provider (Social & Email)

+ Activate Mitigation plan based on Attack, BGP Routing Adjustments, Scrubbing Traffic, Reroute Pools

+ Confirmation of Mitigation Success internally and externally

# Managed DNS can help with DDoS

+ DNS is a core part of your critical infrastructure
+ DNS on a Managed DNS provider with a global Anycast network
+ Use secondary DNS or even a tertiary DNS provider for added resiliency
+ DNS Servers using multiple TLD's (.com, .biz, .info, co.uk)
+ Use a DNS Service that has DDoS Mitigation (On or On-Demand)
+ Avoid Free DNS Services or Vanilla Website Hosting DNS

CloudFloorDNS™
AN EVERBRIDGE SOLUTION

# How CloudfloorDNS can help

+ CloudfloorDNS has a global Anycast network with 13 locations
+ Work with hosting locations on a mitigation plan and identify what is “good traffic” and “bad traffic”
+ CloudfloorDNS offers DNS Pooling (NS1.P325.CloudfloorDNS.com) for flexibility
+ Your Domain is spread across multiple TLD’s (.com, .biz, .info, co.uk) for reliability
+ Constant monitoring (Nagios, Alertsite, Thousand Eyes, Netmon) for performance
+ Network engineers adjusting announcements and traffic
+ If all Network operators implemented BCP38 it would virtually eliminate UDP IP Spoofing


CloudFloorDNS™
AN EVERBRIDGE SOLUTION


# How to minimize the guaranteed downtime due to DDoS attacks

Vincent Geffray, @VGeffray

# The facts

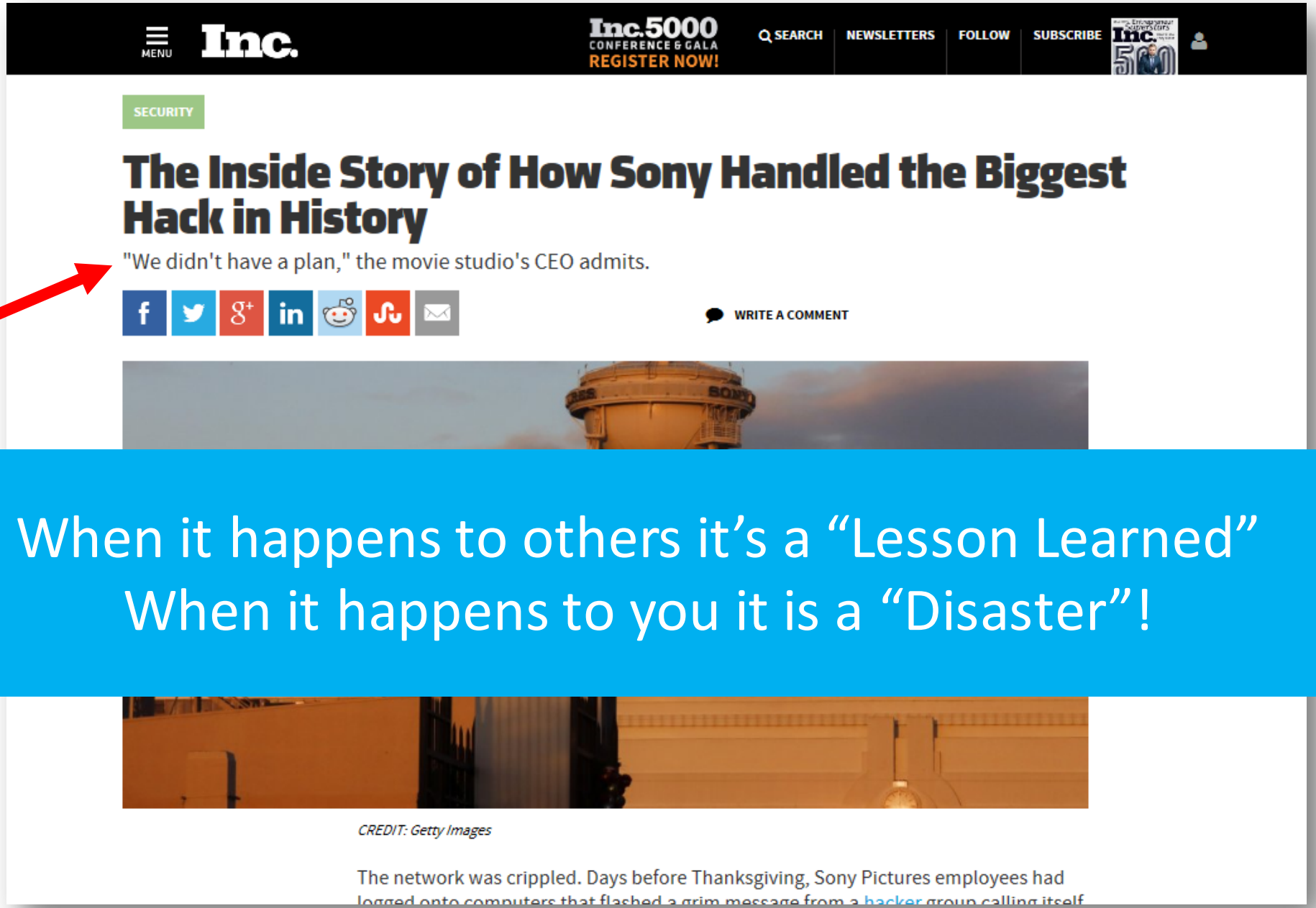
- A successful DDoS attack will shut down your operations
- For a few hours or for days
- Collateral damage after a cyberattack continues for much longer (ex. information leaks)
- A Cyberattack is an IT incident of a different nature
- Backup systems, applications and data may be infected and become useless during immediate response and recovery
- Cyberattacks can alter your RTO because production and IT assets are infected

- **32%** of org have been affected, and
- **34%** think they will during the next two years
- Only **37%** of org have a cyber incident response plan
- **61%** of CEOs are concerned about cybersecurity,

but less than half of board members request information about their organization's state of cyber-readiness

everbridge IT ALERTING

*Source: PWC - Global Economic Crime Survey 2016*

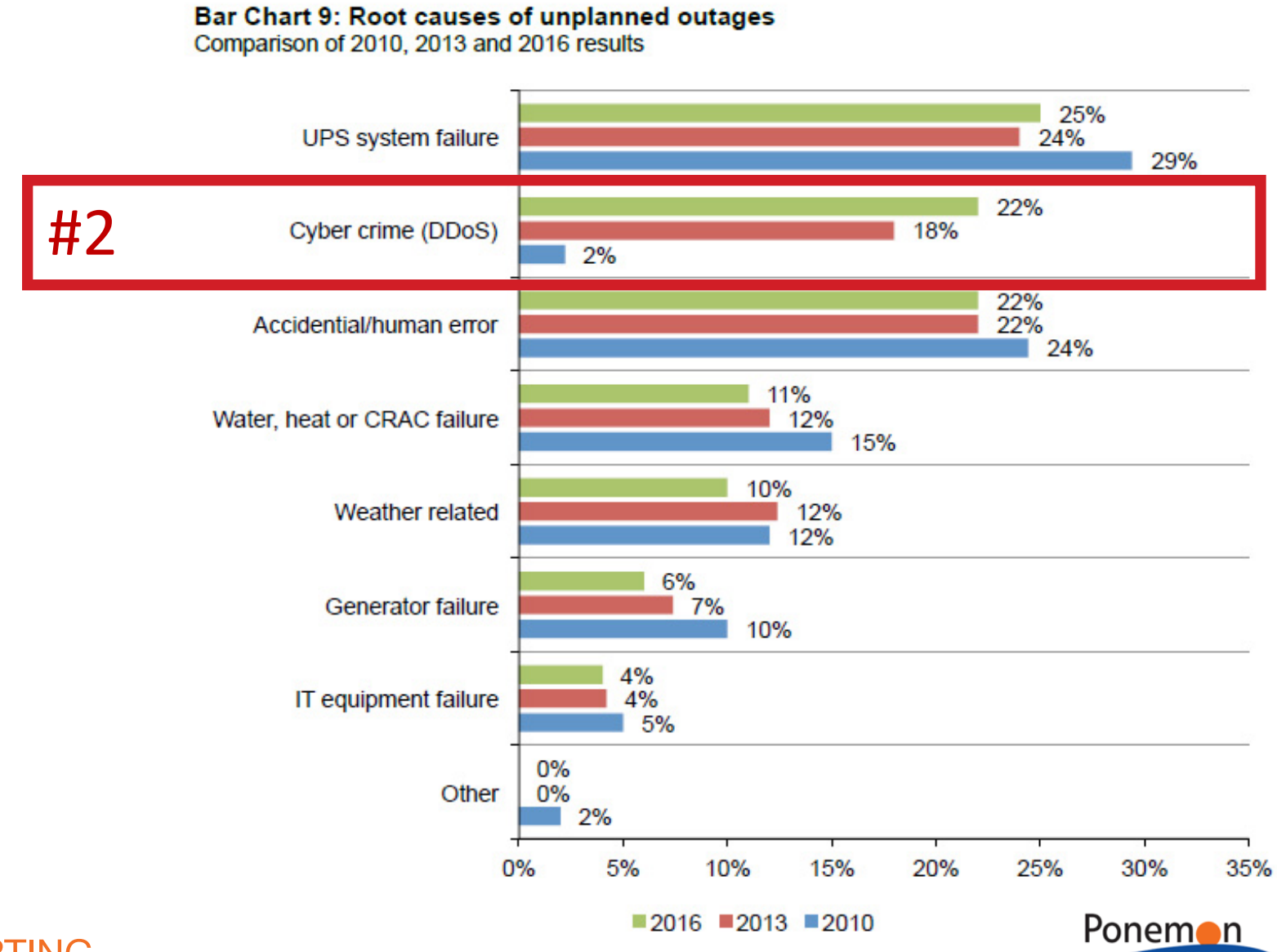



When it happens to others it's a "Lesson Learned"
When it happens to you it is a "Disaster"!

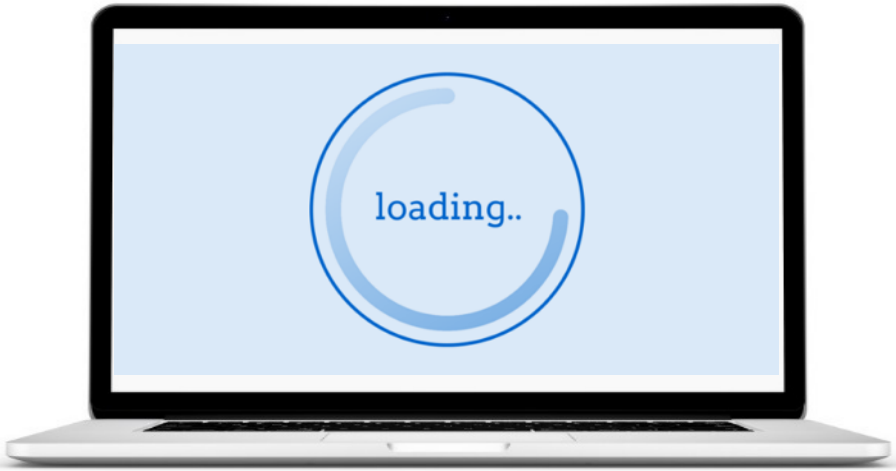
everbridge
IT ALERTING

http://www.inc.com/associated-press/sony-ceo-call-to-google-got-interview-out.html

# What are the Root Causes of an unplanned outage?



# Frustrated Customers




everbridge
IT ALERTING

| Service Desk | IT Security, IT and Business Continuity |
| --- | --- |

Revenue Loss

Bad publicity, Brand Damage

Customer Retention Risk

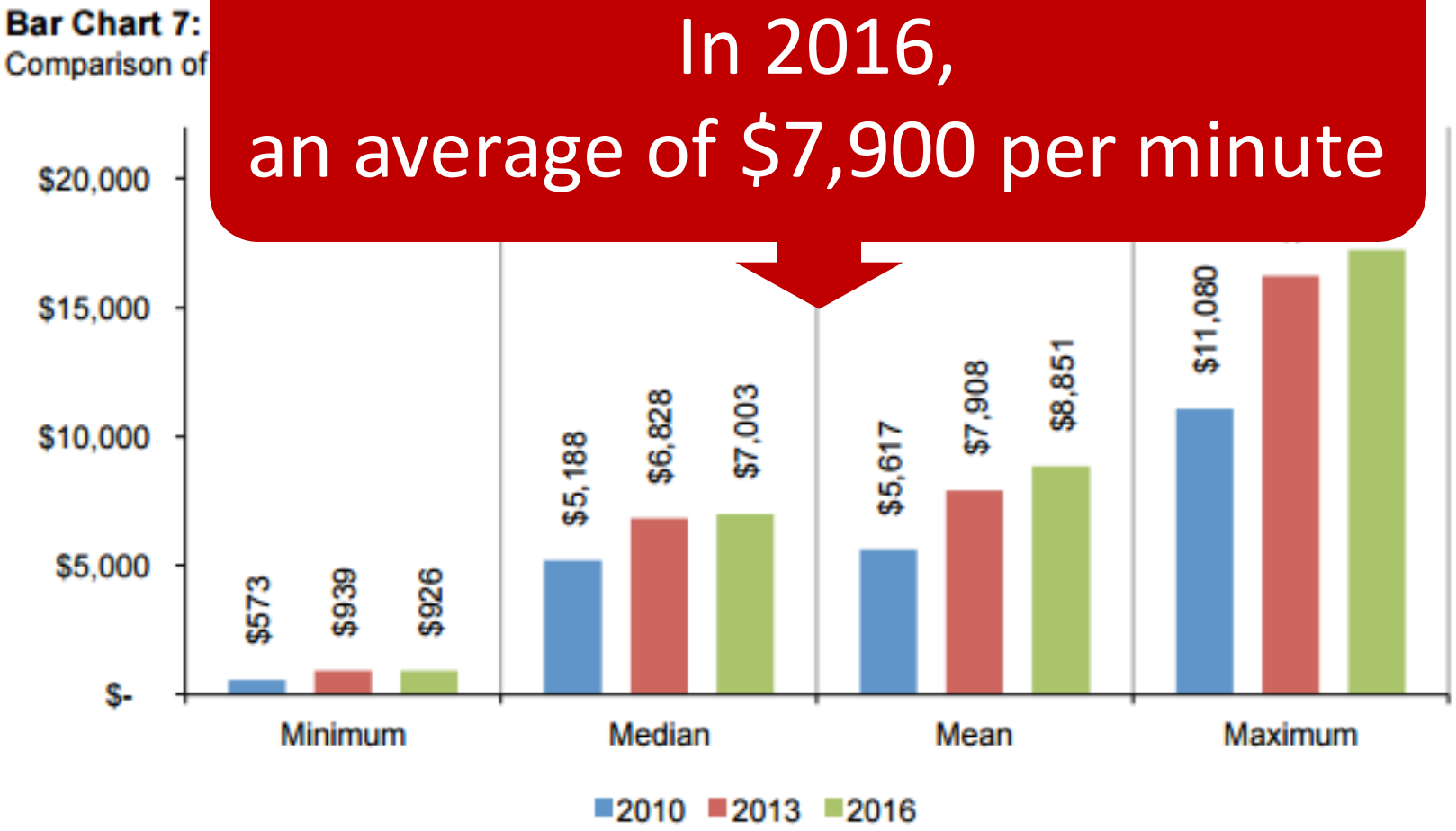
Legal Consequences

# An unplanned outage is a Business issue

everbridge
IT ALERTING

# What's the cost of an unplanned data center outage?

In 2016,
an average of $7,900 per minute




everbridge
IT ALERTING

Ponemon INSTITUTE

# The clock is ticking

everbridge
IT ALERTING

# #1 Unlike at Sony Pictures, have a plan

- Ensure you've defined:
  - a prevention plan,
  - an incident response plan and
  - a communication plan
- Cyberattack response strategy into the BC/DR Plans
- Train your teams on how to respond

**Failing to prepare is preparing to fail!**

# #2 Identify or establish one crisis response team

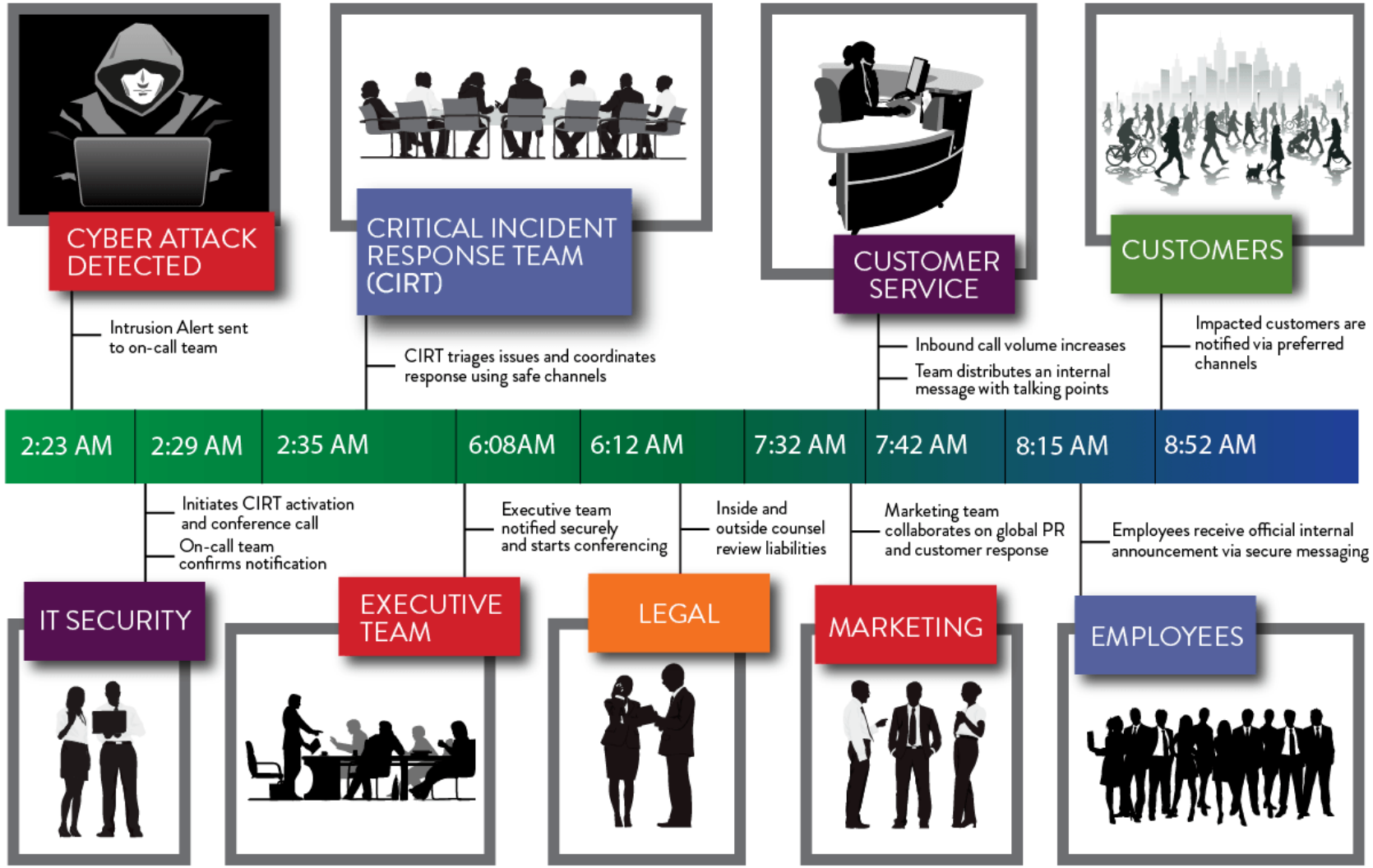

## Crisis Response Team

- Your BCM team, Major IT Incident Response team, IT Security team
- Network engineering, Application support, DB support, Middleware team, Server/infrastructure team, EMR support team
- IT security Manager
- Service Desk manager
- Customer service manager
- Change manager
- IT Service Director
- 3rd Party vendor (technical contact) – DNS provider or Web hosting
- Corporate communications, Legal, Marketing

Assign a Major Incident Manager

everbridge IT ALERTING

# #3 Identify Your Contacts and Stakeholders




everbridge
IT ALERTING

# #4 Create a Communication Strategy

- Who will you be contacting?
  - Your IT experts
  - Senior management
  - Impacted customers
- What communication system should be used?
  - Off-net system
  - Secure/encrypted communications
- How/where do you keep contact information up-to-date?
  - Individuals
  - On-call personnel
  - Static groups
  - Dynamic groups
  - Subscriptions
- How will you be communicating?
  - Text, SMS,
  - Voice, text to voice
  - Emails
  - Mobile app, etc…
- What content will be communicated, to whom ?
  - Notification templates
- What's the escalation rule if your IT experts don't respond
- How often will you be communicating during the crisis?

Like at Sony. What if your telephony network is also compromised?

everbridge
IT ALERTING

# #5 Make (Secure) Virtual Crisis Rooms Available

- You need at least 2 (secure) conference Bridges:
  - Your IT experts and security experts
  - Senior Management/Stakeholders/Business

- How will you be contacting the Stakeholders?
  - Off-net/Secure communications

- How will you be contacting Your IT experts?
  - Manually
  - From your ticketing system
  - From your Monitoring tools

everbridge
IT ALERTING

# Summary

- DDoS attacks can't be avoided and may take your operations down
- Can be disastrous on brand image and revenue
- React quickly and engage the RIGHT resources
- Have a plan
- Define a Cyber crisis response team
- Know who you will communicate with (IT/Security Staff, 3rd party vendors, Stakeholders/Exec/impacted customers…)
- Know who's on-call for each IT and security team at all time (on-call schedules and escalation)
- Know who to escalate to, if no answer
- Have the communication workflows already defined (Cycles/multi-modality)
- Be able to start multiple virtual crisis rooms (Conference bridge, secure or not)

# Engage Your IT Experts in 5 Minutes or Less with Everbridge IT Alerting


automated, multi-modal notifications • rules-based escalation • 1-click conferencing • on-call scheduling • auditing & reporting