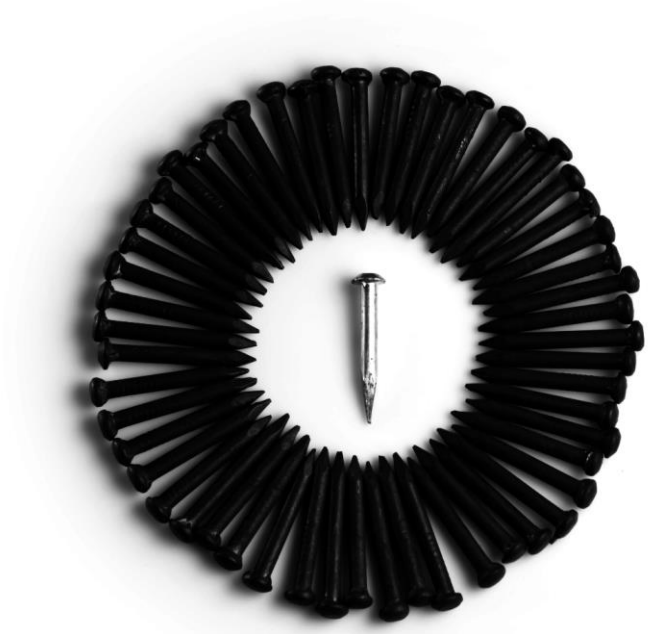
Deloitte.



Fighting back after a denial-of-service attack

Summary diagnosis of the October 21 denial-of-service attack

In the context of an uptick in distributed denial-of-service (DDoS) incidents, one of the largest DDoS attacks ever witnessed, carried out against Dynamic Network Services (Dyn),[1] a company that provides core Internet services for a variety of corporate websites. The method used was similar to any other DDoS attack; the target—Dyn, in this case—was inundated with massive amounts of redundant traffic to overwhelm its infrastructure, inhibiting its ability to provide normal services. Besides being among the largest attacks of its type, it is a game-changer for two reasons:

1. It turned everyday household internet-connected devices—also known as Internet of Things (IoT) devices—into a robotic cyber army of attackers;
2. By disrupting a single entity, it caused rippling disruption to many others.

The attack crippled access to large websites, including Netflix, PayPal, Spotify, and Twitter, by disrupting Dyn's Domain Name Service (DNS) services. The incident underscores that the fast-growing IoT broadens the risk profile for enterprises, and that in today's hyperconnected environment, an organization need not be the direct target of an attack to suffer significant business disruption or damage.

Enterprises need to invest in capabilities to be truly *secure*, constantly "sense" risks and be *vigilant* against potential attacks, and be *resilient* as an organization to contain the damage from cyber incidents and resume business operations rapidly. The fundamentals required to reduce and mitigate the broadened risk exposure have not really changed—but they likely need to be applied to a new scope of infrastructure, and to extend beyond the reaches of traditional corporate structures.

Staying ahead of the curve

IoT devices may soon penetrate many facets of our lives, and business trends are likely to lead to greater interdependency between entities. The characteristics of these advances that make them valuable from a business perspective also present significant risks.

Following are some immediate steps leaders can take to get ahead of DDoS attacks and other risks associated with these trends.

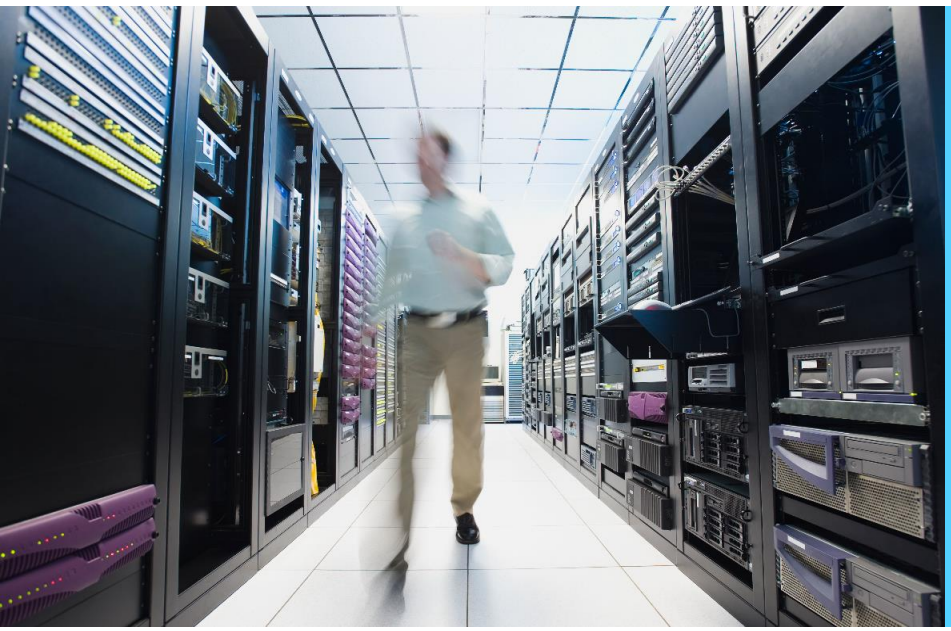
1. Protect your "extraprise." In today's world of highly digitized services, companies need to ask, Who are we dependent on? How could an attack on them impact my operations? From this broad vantage point, continue to push third-party technology and infrastructure providers to authoritatively address cyber risks. This includes third-party programs that focus on specific aspects such as secure-by-design, product security, continuous testing, and incident response from a cyber risk perspective.

2. Plan for the worst. The impact of DDoS attacks can vary greatly. In some cases, while the face of a company is disrupted, back-end business operations continue uninterrupted. Because last week's attack targeted a centralized provider, the outages it suffered cascaded downward to impact many others. Planning for a worst-case scenario should include cyber wargame simulations involving external vendors and business partners, and well thought-out monitoring and resilience strategies shaped to provide business continuity, disaster recovery, and incident response for the highly risk-sensitive parts of the business.

3. "Cyberize" innovation. Driving business performance typically means continuous change—new products and services, new customer engagement models, new business relationships, new technologies. From ideation to design to execution, innovation efforts need to consider cyber risk requirements and how to embed them through the innovation lifecycle.

4. Learn and unlearn. As malware—such as Mirai used in the Dyn attack—is publicly disclosed to help cyber teams manage threats, bad actors may take advantage of such information-sharing to create derivatives to be used to launch further, similar attacks. Even when a public incident does not directly impact an organization, its cyber team should review cyber intelligence reports to understand potential implications for both its own infrastructure and for assets and services hosted by third parties. It is important, though, to remain open-minded about the shape of future threats, and not assume that tomorrow's attacks will look like yesterday's.

5. Refresh your cyber strategy. Entities should revisit the threats and risks associated with their existing and new businesses. Those without a DDoS management strategy in place, may want to consider an accelerated program to incorporate measures to protect against such



DDoS attacks

Q2 2016 versus Q2 2015

- 129% increase in total DDoS attacks
- 151% increase in infrastructure layer (layers 3 & 4) attacks
- 276% increase in NTP reflection attacks (a record high)
- 70% increase in UDP flood attacks

Source: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2-2016-internet-security-executive-review.pdf

attacks by working with an external security solution provider. Consider investing in solutions that cover multiple potential points of failure. Solutions that allow for network resolution even in the face of DDoS attacks or DNS failures can improve resilience in multiple disruption scenarios.

6. Reinforce your guard rails. Given the proliferation of new technologies and connected devices, it is increasingly important to diligently design and implement the fundamentals around over-the-air (OTA) configuration management, network segmentation and traffic management, and security patching and monitoring to manage both risk and performance.

Risk powers performance

Dramatic news headlines and significant disruptions resulting from cyberattacks should not dissuade businesses from being innovative. Organizations can productively pursue the benefits of IoT adoption, cloud services, and digital transformation—as long as they address the associated risks.

The October 21 DDoS attack highlights the need for a *Secure.Vigilant.Resilient.*™ cyber program that perpetually adapts to new business risks and the evolution of cyberthreats.

---

[1] Dyn's statement on the incident is available at http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

Deloitte Advisory contacts

Irfan Saif
Principal
Advisory Cyber Risk Services
Deloitte & Touche LLP
isaif@deloitte.com

Emily Mossburg
Principal
Advisory Cyber Risk Services
Deloitte & Touche LLP
emossburg@deloitte.com

Arun Perinkolam, Pete Renneker, Sachin Verma, and Colin Soutar contributed to this article.