Deloitte.

Building Resilience to Denial-of-Service Attacks

Building resilience to denial-of-service attacks

Traditionally, organizations have relied on disaster recovery (DR) solutions to provide protection from technology disruptions, but recent incidents have highlighted how ill- equipped these methods are in supporting recovery from cyber incidents.

Recently there has been a significant increase in distributed denial-of-service (DDoS) incidents. These incidents are proving to be some of the largest technology disruptions in recent years, impacting network connectivity for organizations around the world. The methods used were similar to any other DDoS attack: the target was inundated with massive amounts of traffic to overwhelm its infrastructure—often leveraging Internet of Things (IoT) devices to carry out the attack.

The attack crippled the target's Domain Name System (DNS) services which disrupted business and revenue streams for many companies, including large digital businesses. Traditionally, organizations have relied on DR solutions to provide protection from technology disruptions, but this event highlighted how ill-equipped these methods are in supporting recovery from cyber incidents.

Traditional DR has been around for over 40 years. It emerged from the need to protect mainframe environments from physical disruption and was appropriate for this task. Today's digital economy is drastically different in several important respects:

Emergence of digital business
Some of the high-profile organizations that suffered disruptions as a result of the DDoS attacks are businesses heavily dependent on technology. For many such companies, disruption of information technology (IT) services can directly correlate to lost revenues.

Growing interconnectivity
With the exponential adoption of cloud, mobility, IoT, and Big Data technologies, networks are becoming increasingly critical to businesses. These same technologies also widen the threat landscape; DDoS attacks turn everyday connected devices into a robotic army of attackers.

Zero downtime expectations
The increased reliance of society on technology creates an "always-on" expectation on the part of customers and business partners. In this particular case, the multi-hour disruption in network services was justifiably unacceptable to many.

Extensive reliance on third parties
Reliance on an internet service or cloud provider may be one of the most evident dependencies, but for many organizations, these are likely not the only external points of potential failure. Digital ecosystems are growing and major disruptions can occur through multiple avenues.

Rise in cyberattacks
Rapidly evolving cyber threats require innovative approaches to protect businesses. DDoS attacks are not new, but the ways these attacks are orchestrated change every day.

What's wrong with traditional network defense and recovery?
As technology continues to revolutionize business and as threats to business operations become more complex, legacy solutions are proving increasingly costly, outdated and insufficient. While considered "front line" defenses, traditional DDoS prevention solutions are incapable of mitigating against large-scale attacks and can provide a false sense of security. Utilizing carriers to deflect traffic not only blocks DDoS-based traffic but also blocks legitimate traffic that otherwise should not be blocked. Firewalls are typically programmed to allow access to traffic utilizing some of the same ports and protocols that are most commonly exploited by attackers. Furthermore, the placement of most firewalls within the network tends to be too far downstream to stop many attacks. Attackers also tend to introduce malicious traffic by spoofing the registered IP addresses of the targeted network, further limiting the effectiveness of firewalls and router- based access control lists.

Traditional DR solutions are focused on addressing physical disruptions and employ redundancy as a foundation.

For networks, this often means having "active" and "backup" circuits. Cyberattacks are logical, targeted, and potentially persistent in nature— meaning the redundancy-based approach not only fails to provide a recovery capability, but can actually serve to propagate the attack to backup circuits.

In the case of DDoS attacks, infrastructure may be recovered to an alternate site, but the applications, database, and server configurations often require that the alternate data center maintain production network configurations. The result is a rerouting of the DDoS traffic to the alternate facility. DDoS is an attack against logical

While considered "front line" defenses, traditional DDoS prevention solutions are incapable of mitigating against large-scale attacks and can provide a false sense of security.

resources, not the physical infrastructure. Since DR does nothing to address the capacity of resources, it does nothing to address DDoS. Further, the active-backup model requires maintenance of backup circuits in parallel with active circuits, a practice that has been shown to be difficult for many companies to reliably maintain. In many cases, when the active circuit fails, failover does not work because the backup circuit has been misconfigured or is not functioning.The result is a failed recovery and potentially a full site or network disruption.

How do digital disruptions such as DDoS attacks impact businesses?

As our example shows, the impact of DDoS attacks can vary greatly from situation to situation. In some cases, while there is disruption at the storefront, back-end business continues uninterrupted. For e-commerce businesses, the inability to maintain web connectivity could have a significant impact. For other businesses, the loss of web access may be undesirable, but it also may have no impact on revenue streams. The more reliant businesses are on technology, the greater the impact of digital disruptions is likely to be.

Given the growing adoption of network-enabled technologies, disruption of communication channels can effectively disrupt the very heart of an enterprise, bringing important business functions to a halt and irreparably damaging brand value and customer or client relationships. High-impact disruptions could include a retailer suffering major channel disruption

on Black Friday, a hospital being unable to admit patients, or an airline having to cancel thousands of flights during the holiday season.

What can organizations do?

The answer is a shift toward Cyber Resilience, which develops the ability to withstand disruptions to IT capabilities supporting critical business operations.

Disaster recovery is a contingency planning approach that assumes disruptions will occur and aims to recover from them. Cyber risk is pervasive in an organization, and the Cyber Resilience approach drives resilience across the enterprise by addressing the people, process, and technology challenges associated with traditional contingency planning methods in an attempt to deliver an always-on enterprise.

Following (on page 4) are a number of characteristics that improve overall operational resilience, most of which do not fall under the traditional DR umbrella. These characteristics are also appropriate to consider when pursuing resilience to DDoS attacks.

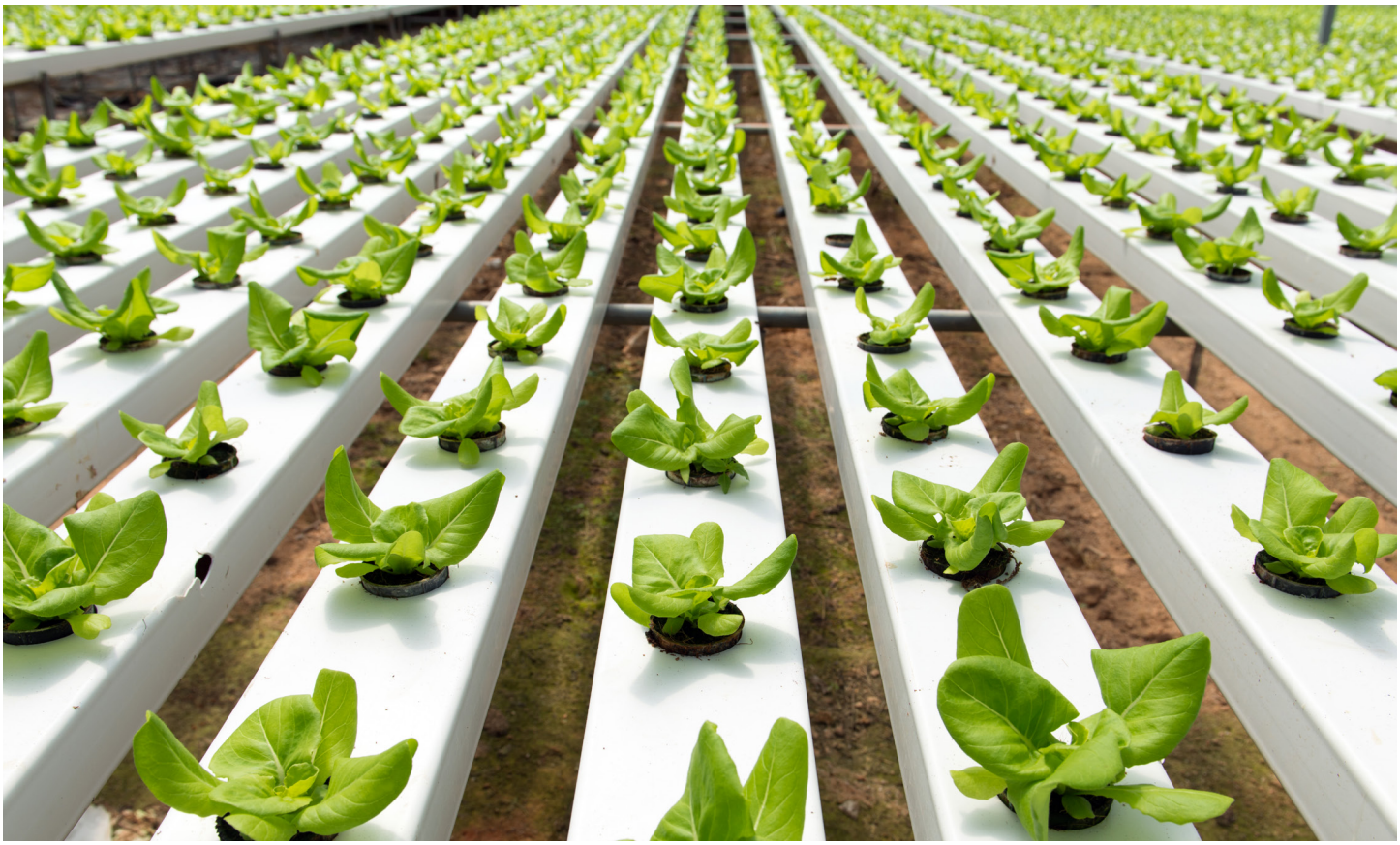
Cyber Resilience infrastructure is designed to be...

Agile	DNS caching solutions allow for resolution of network addressing in the face of DNS failures and outages. This potentially addresses multiple forms of DNS disruptions, including situations when DDoS attacks hammer DNS.
Surge-supporting	High-capacity, cloud-based DDoS protection services allow you to quickly reroute DDoS traffic and keep your IT resources readily available. These on-demand services quarantine traffic from suspicious IP addresses and scrub them to allow clean traffic through.
Scalable	Load-balanced front end web servers can help handle an initial onslaught of queries targeted at those environments.
Secure	Validating access to web services can winnow out malicious and robotic/automated access. Securing end user-originated traffic from internet-originated traffic supports continuity of services as organizations shift critical services to the cloud and other external sources. Software-defined WAN technologies provide secure access to enterprise and Internet-based resources through encryption, evergreen proxy, URL filtering, anti-virus protection, and other network security technologies.
Risk-sensing	Anti-DDoS appliances support quick identification and diversion of web-based queries that may be part of a DDoS attack.
Adaptive	Quickly gaining momentum is a hybrid network solution in which two different access technologies [e.g. Multi-Protocol Layer Switching (MPLS), Internet] are used to provide diverse WAN services to a particular site. Many large organizations currently employ a dual-carrier strategy in which an MPLS circuit from each carrier is terminated at each remote site to provision against potential circuit and/or carrier failure.
Modular	Software-defined WAN technologies can support network micro-segmentation, which provides the agility to failover only impacted systems and/or network segments. They allow organizations to utilize multiple enterprise circuits in a standardized fashion and even provide increased bandwidth and resiliency for remote sites with a single MPLS circuit through the deployment of an Internet circuit.
Automated	Software-defined networks provide a layer of application-aware routing and path diversity. This provides the ability to automate and proactively divert network traffic, increasing overall network resiliency based on pre-defined thresholds. It also allows organizations to replace expensive MPLS circuits with low-cost, high- bandwidth Internet circuits providing direct Internet access to remote sites.

Thriving in the network-driven digital economy

Networks underpin the digital economy; building proactive management of cyber risks into the overall business strategy is a foundation for today's high-performing organizations. The IoT, cloud, mobility, and other emerging technologies organizations are embracing offer great rewards—and the risks are manageable. As the cybersecurity landscape continues to evolve, Cyber Resilience provides a framework and pre-emptive approach to enterprise resiliency and supports a Secure.Vigilant.ResilientTM cyber program.

Cyber Resilience services provide a framework and pre-emptive approach to enterprise resiliency.



For more information please visit
www.deloitte.com/us/cyber

Contacts for Cyber Resilience

John Gelinne
Principal
Cyber Risk Services
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
jgelinne@deloitte.com

Bob Black
Principal
Technology Strategy and Architecture
Deloitte Consulting LLP
bobblack@deloitte.com

Myke Miller
Managing Director
Technology Strategy and Architecture
Deloitte Consulting LLP
mykemiller@deloitte.com

Pete Renneker
Senior Manager
Cyber Risk Services
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
prenneker@deloitte.com

Deloitte.