WINTERS-OLIVER
INSURANCE AGENCY, INC.

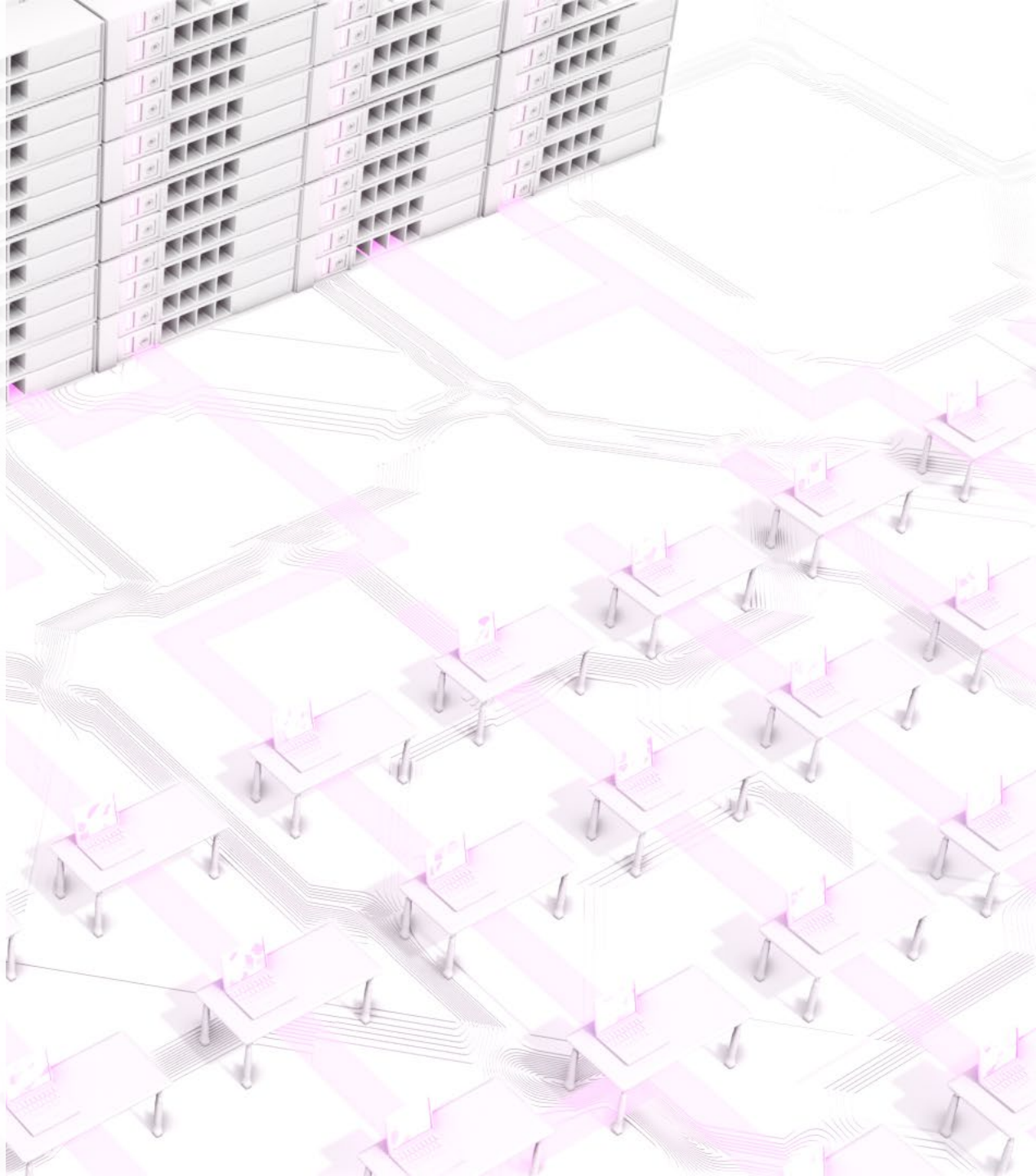
Cyber Case Study

provided by Winters-Oliver Insurance Agency

The Mirai DDoS Attack on Dyn

In October 2016, Dyn—a domain name system (DNS) provider for many well-known internet platforms—was targeted in a distributed denial-of-service (DDoS) attack. The incident was one of several major DDoS attacks in 2016 that stemmed from the Mirai botnet.

This attack resulted in widespread outages across Dyn's systems, leaving various internet platforms temporarily unavailable to users throughout North America and Europe. Consequently, Dyn faced substantial business interruption issues, recovery costs and reputational damages from the attack. There are several cybersecurity lessons that organizations can learn by reviewing the details of this incident and its impact. Here's what your organization needs to know.



The Details

A DDoS attack consists of a cybercriminal aiming to disrupt a targeted server or network by flooding the victim's infrastructure with excess internet traffic. By overwhelming the victim's infrastructure with more internet traffic than it can feasibly handle, such an attack can either significantly delay server or network speeds or render these systems inaccessible until the traffic eventually subsides.

In order to generate this excess traffic, the perpetrator of a DDoS incident generally utilizes a botnet, which is a large group of internet-connected devices that have been infected with malware. This malware permits the cybercriminal to control each device within the botnet from a remote location. After establishing a botnet, the cybercriminal is then able to conduct their attack by instructing each device to overwhelm the targeted server or network with repeated requests, thus causing the victim's infrastructure to experience system performance issues or complete failure.

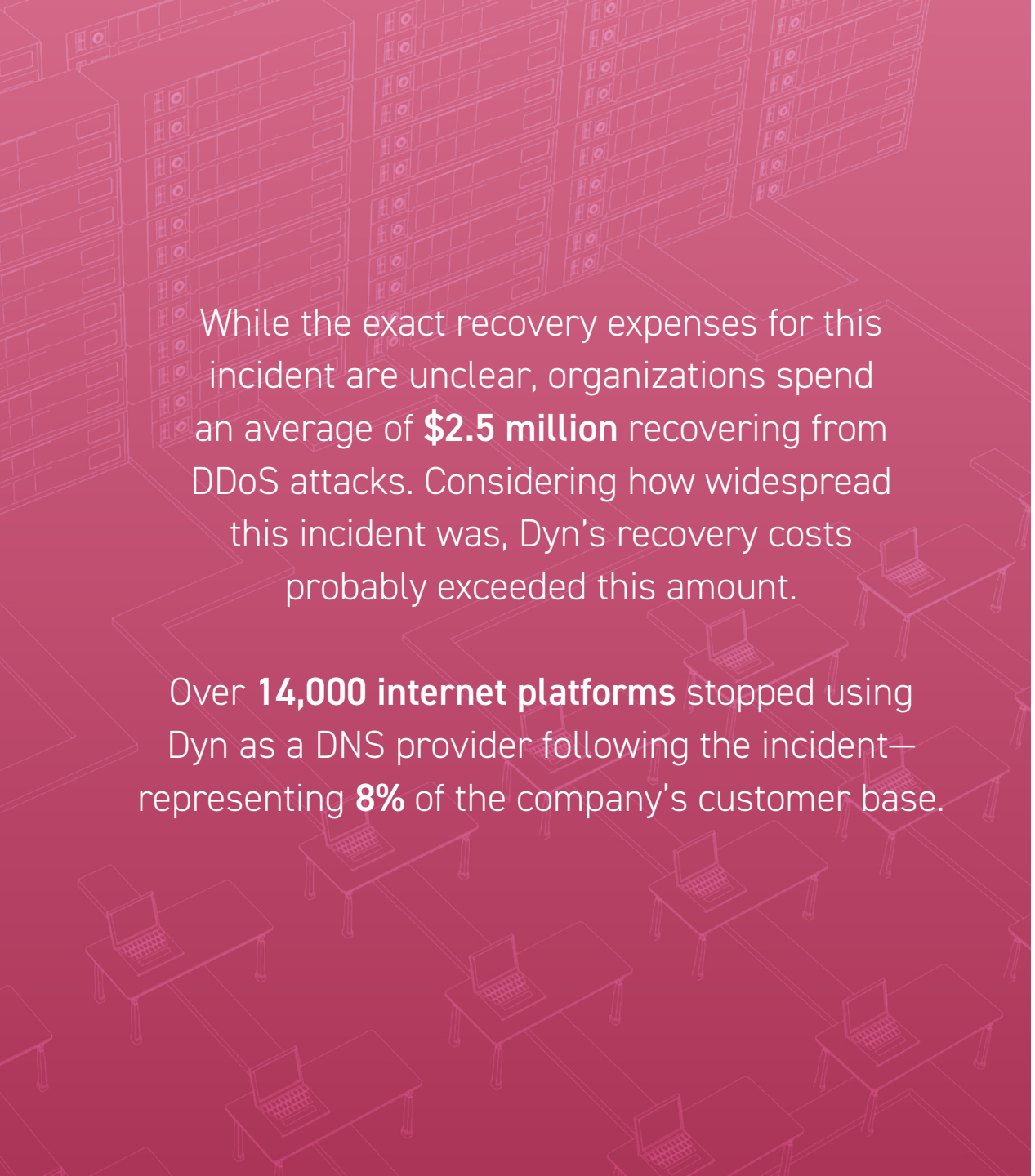
Initially, botnets only consisted of malware-infected computers, limiting the pool of devices that could be utilized in DDoS attacks and the subsequent severity of these incidents. But over time, cybercriminals began developing botnets from a range of internet-connected devices (e.g., printers, cameras and routers), increasing the potential strength of DDoS attacks in the process. Such was the case for the Mirai botnet, which was created in 2016 by three college students looking to attack various gaming servers and networks. These students established the botnet by gaining control of an estimated 145,000 internet-connected devices via malware.

The first DDoS attack that utilized the Mirai botnet took place on Sept. 19, 2016. This incident targeted OVH, a French internet service company. In the days following the attack, the college students posted the code for the Mirai botnet online, thus making it harder to trace the origins of the botnet back to them. In doing so, the students also gave other cybercriminals access to the botnet, paving the way for a plethora of Mirai-based DDoS attacks in the coming weeks and months.

On Oct. 21, 2016, cybercriminals leveraged the Mirai botnet to launch a DDoS attack on Dyn. The first wave of the attack began at 7 a.m., when cybercriminals commanded the devices within the botnet to send tens of millions of requests to Dyn's systems and overwhelm its infrastructure. As a result, over 50 major internet platforms serviced by Dyn became temporarily inaccessible to users throughout both the Northeastern United States and regions of Europe. Impacted internet platforms included PayPal, Twitter, Reddit, Sony, Amazon, Netflix, Spotify, Pinterest, SoundCloud, Squarespace and several major news websites.

After discovering the attack, Dyn was able to mitigate the incident and restore the impacted internet platforms in approximately two hours. However, the incident continued throughout the day as the cybercriminals launched two additional attack waves against Dyn's systems in the afternoon and evening. Nevertheless, these waves were less severe in nature and only caused minor delays for certain internet platforms. As such, Dyn was able to resolve these issues relatively quickly.

Weeks after the attack, the federal government began investigating the origin of the Mirai botnet. Although the perpetrators of the DDoS attack against Dyn remain unknown, the U.S. Department of Justice eventually identified the three college students as the creators of the Mirai botnet in December 2017. At this time, the students pleaded guilty to developing and sharing the botnet code that contributed to the Mirai-based DDoS attacks during the past year. Yet, the Mirai botnet remains active to this day—making future attacks a possibility.



While the exact recovery expenses for this incident are unclear, organizations spend an average of **$2.5 million** recovering from DDoS attacks. Considering how widespread this incident was, Dyn's recovery costs probably exceeded this amount.

Over **14,000 internet platforms** stopped using Dyn as a DNS provider following the incident—representing **8%** of the company's customer base.

The Impact

Dyn faced a range of consequences from this cyber incident, including the following:

Business interruptions

This attack resulted in major disruptions for Dyn and the internet platforms it serviced, rendering these platforms temporarily unavailable. Although Dyn was able to mitigate the incident within two hours—which is faster than the average time it takes to resolve a DDoS attack—these interruptions were still significant. After all, DDoS attacks can cost as much as $22,000 per minute of downtime they cause, while over half of these attacks (51%) contribute to reduced revenue for targeted organizations.

Recovery costs

Apart from business interruptions, Dyn also likely incurred substantial recovery expenses from this attack. Such costs include those related to identifying the incident, mitigating its impact, investigating the cause and implementing additional cybersecurity practices to prevent future attacks. While the exact recovery expenses for this incident are unclear, organizations spend an average of $2.5 million recovering from DDoS attacks. Considering how widespread this incident was, Dyn's recovery costs probably exceeded this amount.

Reputational damages

Because it impacted several major internet platforms and involved an emerging botnet, this incident was widely publicized by the media. Despite Dyn's best efforts to mitigate the attack as quickly as possible, it still received criticism for the resulting system outages and delays. Further, some customers no longer trusted Dyn to service their internet platforms after the attack. In fact, over 14,000 internet platforms stopped using Dyn as a DNS provider following the incident—representing 8% of the company's customer base.

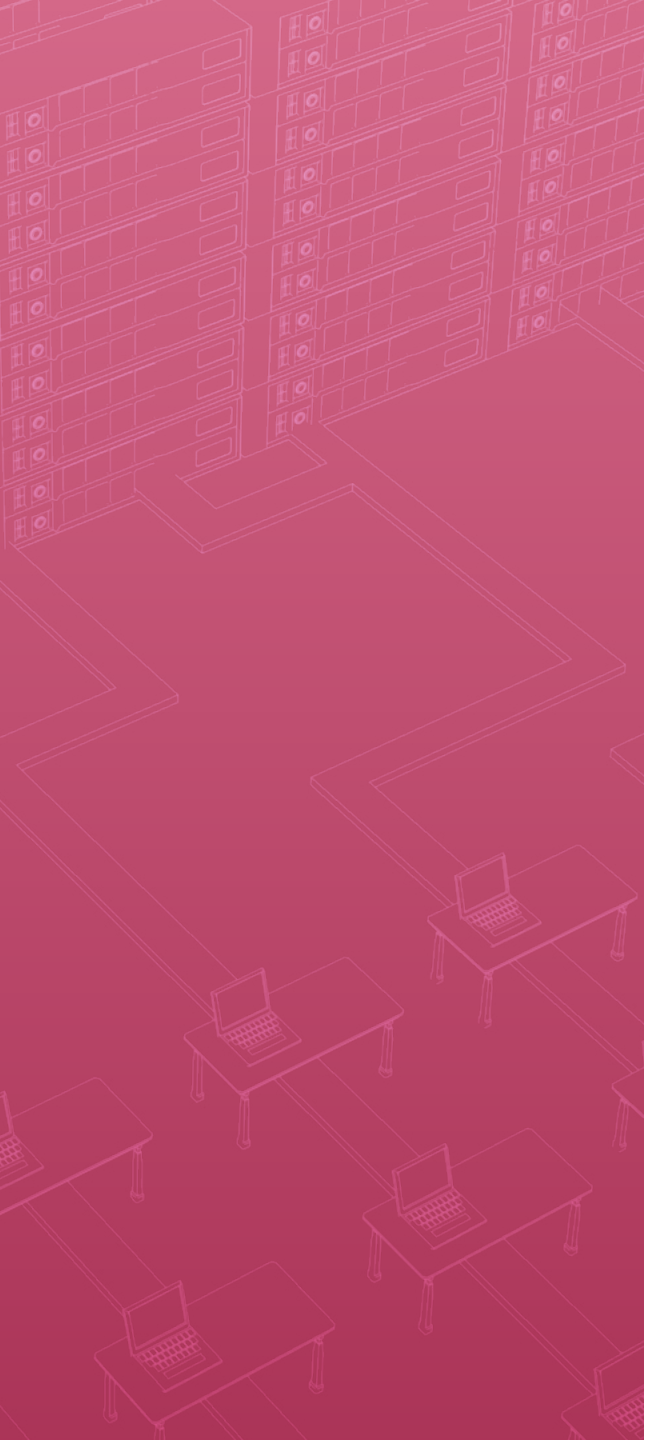
Lessons Learned

There are several cybersecurity takeaways from the Mirai DDoS attack on Dyn. In particular, the incident showcased these key lessons:

DDoS attacks are a rising threat.

As cyberattacks methods evolve, DDoS attacks have become a growing concern. What's more, these incidents are only expected to rise due to the continued proliferation of internet-connected devices. In 2020 alone, more than 10 million DDoS attacks were recorded—up from 8.5 million in 2019. While these incidents can cause issues for any organization, they can be especially devastating for those that rely heavily on their internet platforms to conduct key operations (e.g., online retailers and digital news outlets). What's worse, with harmful botnets like Mirai emerging, DDoS attacks could become increasingly severe. With this in mind, it's important to implement the following cybersecurity practices to help identify and mitigate potential DDoS attacks:

- Closely monitor internet traffic patterns for all organizational servers and networks. By establishing a baseline for these systems, it will be easier to detect excess traffic and potential DDoS attacks.
- Educate employees on the signs of DDoS attacks, including sudden changes in server or network speeds, unexpected system shutdowns and excess spam issues. Have specific procedures in place for reporting DDoS attacks.
- Make organizational servers and networks more resilient against DDoS attacks. This entails segmenting different systems to help minimize internet traffic bottlenecks and adding more bandwidth to ensure systems are equipped to handle instances of elevated traffic. In some cases, transitioning certain operations to the cloud can provide greater bandwidth



Lessons Learned (cont.)

- Install DDoS detection and prevention software on all workplace technology. Such software may include advanced firewalls, internet traffic monitoring systems and anti-DDoS hardware. Consider working with a qualified cybersecurity professional to secure additional DDoS protection.
- Contact a supervisor or the IT department if suspicious activity arises.

Cyber incident response plans make a difference.

Dyn took several hours to recover from this incident, ultimately increasing disruption concerns and compounding the overall costs of the attack. Such recovery issues highlight how essential it is to have an effective cyber incident response plan in place. This type of plan can help an organization establish timely response protocols for remaining operational and mitigating losses amid a cyber event. A successful incident response plan should outline potential cyberattack scenarios, methods for maintaining key functions during these scenarios and the individuals responsible for carrying out such functions. Additionally, the plan should address specific response procedures for upholding critical operations amid DDoS attacks, as these attacks are more likely to cause disruptions. Furthermore, the plan should discuss how to respond if DDoS attacks target supply chain members (e.g., vendors, distributors or suppliers) and key operations are subsequently disrupted. This plan should be routinely reviewed through different activities—such as tabletop exercises and penetration testing—to ensure effectiveness and identify ongoing vulnerabilities. Based on the results from these activities, the plan should be adjusted as needed.

Proper coverage can provide much-needed protection.

Finally, this attack made it clear that no organization—not even a major DNS provider—is immune to cyber-related losses. That's why it's crucial to ensure adequate protection against potential cyber incidents by securing proper coverage. Keep in mind that standard cyber insurance policies may not provide sufficient protection for losses resulting from cyber-related business interruptions, such as those that often accompany DDoS attacks. To protect against such disruptions, it may be necessary to obtain certain policy endorsements or additional, specialized coverage. It's best to consult a trusted insurance professional when navigating these coverage decisions.

For more risk management guidance and insurance solutions, **contact us today.**