Cyber Incident
Response Scenario

DDoS Attack

SCS AGENCY INSURANCE

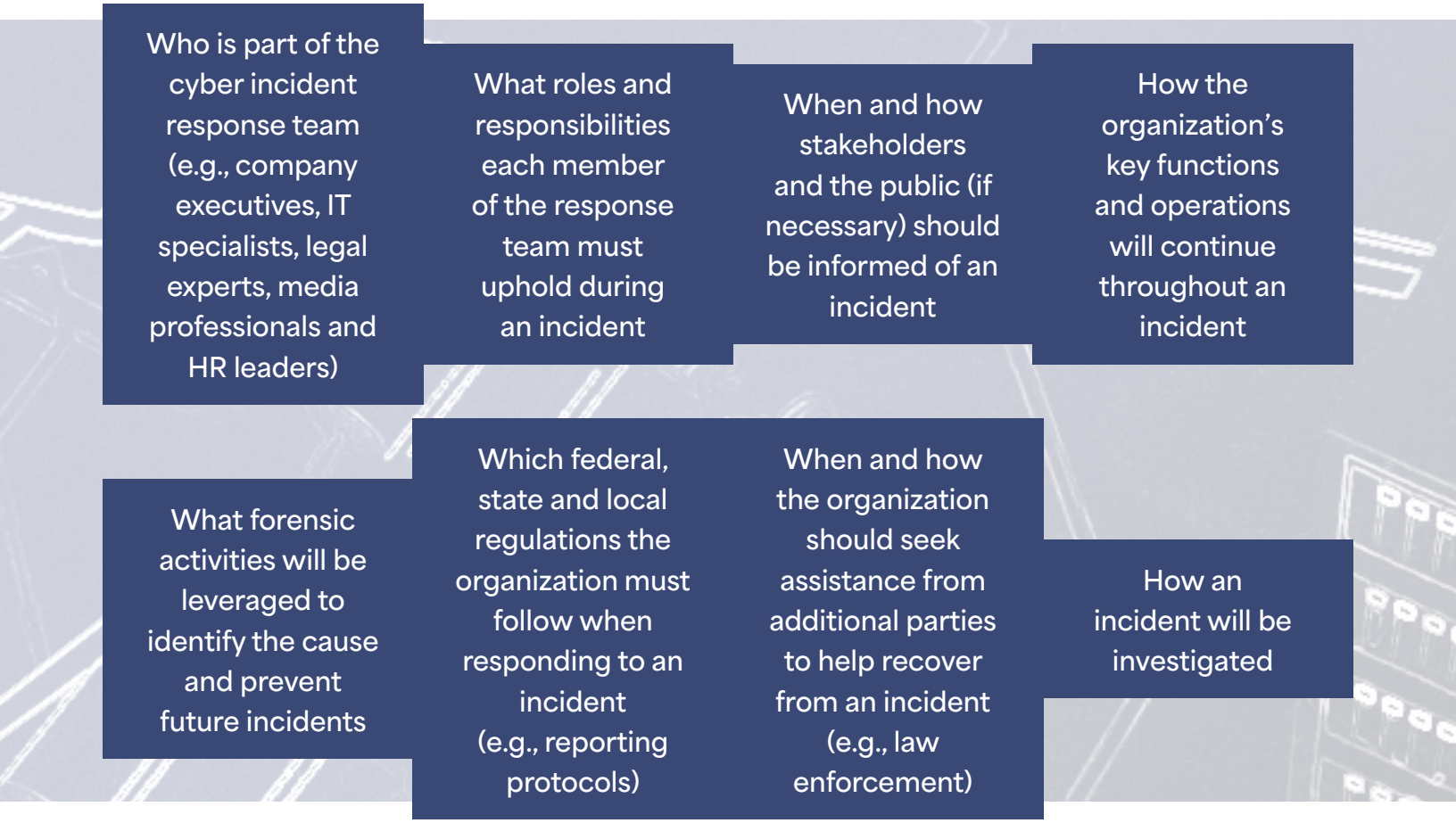
Introduction

The way an organization responds to a cyber incident can make or break its operational, financial and reputational stability.

In the event of a poor response, an organization may encounter various consequences—including the exposure of sensitive data, compromised technology, widespread business disruptions, disgruntled stakeholders, lost customers and diminished market value. Fortunately, organizations can mitigate these damages through proper cyber incident response planning.

A cyber incident response plan establishes steps to ensure timely remediation amid cyberattacks and keep related losses to a minimum. Effective response planning requires coordination across an organization.

A solid response plan should outline the following:



For cyber incident response plans to be successful, they should address a number of attack scenarios so that organizations can be ready to handle any type of attack and protect themselves from large-scale losses. One of the most important scenarios to include in a cyber incident response plan is a distributed denial-of-service (DDoS) attack. This type of attack occurs when a cybercriminal attempts to interrupt an online service by flooding it with fake traffic. Specifically, a cyber-criminal may utilize an interconnected group of hijacked devices (also called a botnet) to send countless requests to a company's servers, overwhelming various aspects of its IT infrastructure and forcing the business to temporarily halt its operations or go completely offline.

DDoS attacks typically originate from disgruntled employees, business competitors or nation-state actors who may be seeking to enact revenge, cause chaos or gain a competitive advantage. In any case, these attacks often lead to widespread outages and financial losses for impacted organizations. Keep reading for an example of a DDoS attack scenario and a summary of how a cyber incident response plan can address this scenario.For cyber incident response plans to be successful, they should address a number of attack scenarios so that organizations can be ready to handle any type of attack and protect themselves from large-scale losses. One of the most important scenarios to include in a cyber incident response plan is a distributed denial-of-service (DDoS) attack. This type of attack occurs when a cybercriminal attempts to interrupt an online service by flooding it with fake traffic. Specifically, a cybercriminal may utilize an interconnected group of hijacked devices (also called a botnet) to send countless requests to a company's servers, overwhelming various aspects of its IT infrastructure and forcing the business to temporarily halt its operations or go completely offline. DDoS attacks typically originate from disgruntled employees, business competitors or nation-state actors who may be seeking to enact revenge, cause chaos or gain a competitive advantage. In any case, these attacks often lead to widespread outages and financial losses for impacted organizations. Keep reading for an example of a DDoS attack scenario and a summary of how a cyber incident response plan can address this scenario.

Attack Scenario

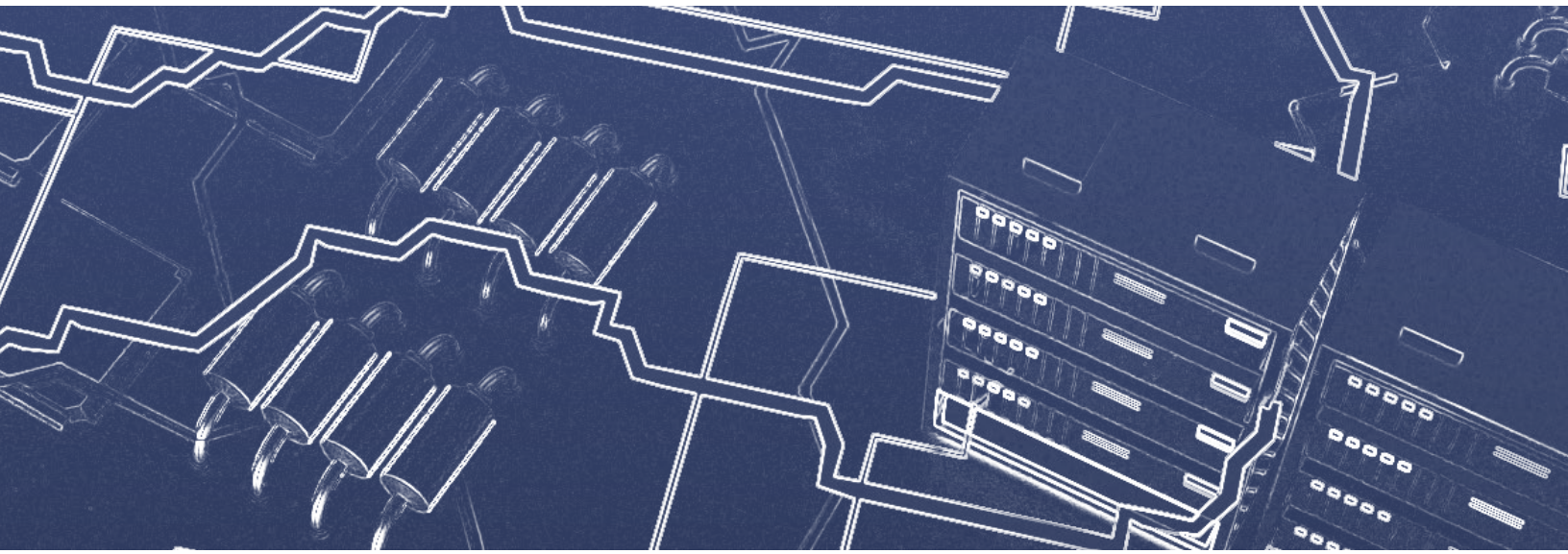
On Wednesday morning, a small online retailer launched a new product on its website and decided to draw attention to this occasion with a **companywide sale**.

Although the retailer expected increased traffic on its website during the sale, the company's servers quickly became **overwhelmed by a sudden spike in online activity**. Within minutes, the retailer's website was flooded with hundreds of thousands of requests, far exceeding the network's usual bandwidth and causing the company's servers to lag.

As time went on, the retailer's network could no longer keep up with these excessive requests, prompting the servers to repeatedly time out and forcing the website to display an error message. With the retailer's website shut down, customers were unable to shop the sale, ultimately driving away potential business. The retailer initially assumed the website was experiencing technological issues and consulted the IT department for assistance. In an attempt to resolve these issues, several members of the IT department carefully reviewed the surge in online activity. Upon doing so, these experts discovered that the excessive requests had all **stemmed from similar devices in the same geographic area**, indicating that a cybercriminal had utilized a botnet to launch a DDoS attack. Facing major operational disruptions and lost income, the retailer needed to act fast to minimize further damage.

Response Plan Reaction

In this particular DDoS attack scenario, **a well-crafted cyber incident response plan** would guide the retailer through the following steps:



Validation and research—Once the members of the IT department shared their suspicions of a DDoS attack, the retailer promptly assessed the situation to determine whether the incident posed a genuine threat. After validating the attack, the retailer conducted additional research regarding the scope and severity of the incident by consulting its internet service provider, documenting which aspects of its IT infrastructure were affected (e.g., the company's servers, network and website), calculating potential losses and identifying possible motivators that would have led the cybercriminal

responsible for the incident to launch the DDoS attack. The retailer immediately activated its cyber incident response team and notified necessary parties (e.g., the local authorities and insurance professionals) to kickstart the investigation and insurance claims process.

Containment—At this stage, the cyber incident response team isolated the company's affected servers, network and website by taking them offline. The response team also displayed a message on the retailer's website stating that the site was temporarily down and instructing customers to come back later to shop the sale. In doing so, the response team was able to limit the cybercriminal's ability to proceed with the DDoS attack while still keeping customers engaged. During this containment, the response team also explored different methods (e.g., rate-limiting mechanisms, load-balancing solutions and traffic-scrubbing services) to help filter and divert potentially malicious online activity going forward, thus reducing the risk of the cybercriminal being able to relaunch the attack. The response team relied on offline communication methods (e.g., phone calls) throughout this process to reduce the risk of the cybercriminal intercepting any important conversations.

Recovery—Following containment, the cyber incident response team implemented its selected methods for filtering

and diverting harmful online traffic before gradually restoring the retailer's affected servers, network and website to their original functionality and allowing customers to shop the sale once again. The response team then scanned the company's larger IT infrastructure for any remaining vulnerabilities to ensure proper protection against future attacks. Once the response team addressed any ongoing vulnerabilities, it consulted with legal counsel to discuss any regulatory ramifications of the incident and determine whether any further recovery steps were necessary. Due to a prompt response, the retailer was able to recover from the DDoS attack by Wednesday evening, resulting in less than 24 hours of total downtime.

Communication—Upon completing the recovery process, the cyber incident response team worked closely with the local authorities and insurance professionals to provide any further information and documentation that would help these parties complete their investigation and resolve the associated insurance claim. At this stage, the local authorities revealed that the cybercriminal responsible for the DDoS attack was a disgruntled former employee who had intended to drive business away from the retailer during the sale. The response team also took this time to release a public statement regarding the DDoS attack and communicate directly with

any regulators or stakeholders who needed to be informed of the incident.

Post-incident analysis—Lastly, the retailer conducted a post-incident analysis. This analysis focused on where the DDoS attack originated; how it was detected; how effective the incident response plan was in handling this event; the different technical, operational and financial impacts of the incident; and whether any company failures played a role in the event. The results of the post-incident analysis ultimately guided the retailer's identification of its cybersecurity weaknesses and supported its effort to fill possible gaps with bolstered defenses. This analysis also helped the retailer make necessary updates to the cyber incident response plan, thus improving mitigation techniques for future cyber incidents and reducing related damage.

An organization's cyber incident response team typically consists of various experts and professionals across multiple fields. It's also worth noting that, depending on an organization's size and in-house resources, its response team may consist of either internal or external parties. In other words, larger organizations may have entirely in-house response teams, whereas small organizations with fewer resources may seek the assistance of third-party vendors. Regardless, before hiring any vendors to help respond to cyber incidents,

employers should consult their cyber insurers to determine whether any policy provisions include vendor-related stipulations or requirements. Some insurers mandate policyholders to work with preselected vendors that offer negotiated rates, therefore limiting associated claim costs. In this DDoS attack example, the impacted retailer had limited in-house experts due to its size and developed a response team consisting of insurer-recommended vendors.

In addition, keep in mind that although the retailer's IT department was able to detect the DDoS attack due to online traffic involving multiple devices from the same geographic location, these types of attacks don't always present themselves in this way. After all, the botnets utilized to launch DDoS attacks may consist of millions of interconnected devices located anywhere and belonging to anyone. With this in mind, employers should be aware of other possible signs of DDoS attacks, such as one or more specific IP addresses making several consecutive requests over a short period of time and traffic logs showing spikes at unexpected hours or in unusual sequences. What's more, organizations should prioritize effective threat detection technology and continuous traffic monitoring solutions; these tools are often the best way to ensure early identification of possible DDoS attacks.

Further, it's important to understand how cyber insurance may apply to losses stemming from DDoS attacks. Namely, these attacks have the potential to result in considerable business interruptions and lost income; nevertheless, securing business interruption coverage amid cyberattacks can carry challenges. Most organizations affected by cyber incidents are usually able to reinstate their key operations within hours or days, so cyber insurers often heavily scrutinize business interruption calculations and related expenses. Cyber insurers may even leverage forensic accountants to review these expenses further. Even so, organizations should note that because cyber incidents are often resolved quickly, the waiting period for business interruption coverage to kick in with cyber insurance is often shorter than that of traditional business interruption insurance. That is, the waiting period with a cyber insurance policy is typically less than 24 hours, whereas the waiting period with a business interruption policy is generally 72 hours.

Considering these concerns, it's critical for employers to consult their sales and operations teams to ensure accurate business interruption calculations and foster open communication with cyber insurance representatives to reach positive claims outcomes. The most valuable business interruption expenses to document include diminished production capabilities, operational inefficiencies caused by temporary work-

arounds, lost or canceled orders, permanent contract losses, and prolonged downtime that allowed customers or clients to purchase products and services from competitors. In this DDoS attack scenario, the retailer's business interruption coverage was triggered due to the retailer's in-depth loss documentation and the recovery process exceeding its cyber insurance policy's waiting period, yet the bulk of the insurance payout applied to the company's external vendor costs. In any case, organizations should consult trusted insurance professionals to discuss their unique coverage needs and determine how their policies will respond to DDoS attacks.

Conclusion

Organizations can adequately prepare for cyber incidents and reduce potential fallout through **proper response planning**.

Yet, it's essential to understand that response plans are always a work in progress; as operational needs change and cyber exposures evolve, response planning should follow suit. Thus, organizations can leverage several practices (e.g., tabletop exercises and penetration testing) to assess their cyber incident response plans and make adjustments over time. In doing so, organizations can remain prepared for the latest cyberthreats and successfully navigate the ever-changing digital risk landscape.

Contact us today for further risk management guidance.