Name: Kanchan Chopde
CSC 5372 Principles of Cyber Security
Winter 2024

Project 1
Federal-Distributed-Denial-Of-Service-CTEP-Situation-Manual

Assuming a hypothetical situation where our financial institution experienced DDos attacks, following report will give details on actions our agency takes upon receiving a CISA DDoS Advisory and examines our agency's baseline planning efforts. It also explores how our organization handles indicators of a DDoS attack, confirmation of an attack, mitigation, and monitoring and recovery efforts.

Module 1

Upon increased distributed denial-of-service (DDoS) activity targeting both U.S. and foreign government entities, in module 1 we will explore different aspects of our financial institutions operational resilience.

In a hypothetical scenario we consider that in 2024 our financial institution experienced the highest number of Distributed Denial-of-Service (DDoS) attacks. In this attack a victim's server is overwhelmed with fake connection requests, and the attack surface is diverse, comprising of banking IT infrastructures, customer accounts, payment portals, etc.

Network resources have a finite limit to the number of requests that they can service simultaneously. In addition to the capacity limit of the server, the channel that connects the server to the Internet will also have a finite bandwidth. Whenever the number of requests exceeds the capacity limits of any component of the infrastructure, the level of service is likely to suffer in one of the following ways:

- The response to requests will be much slower than normal.
- Some users' requests may be totally ignored.

The cybersecurity team, including security analysts, incident responders, and threat intelligence analysts, would be the primary recipients of this information within the organization. Depending on the severity of the threat, executive leadership may also be informed.[1]

The most useful cyber threat information includes indicators, tactics, techniques, and procedures (TTPs), security alerts, threat intelligence reports, and recommended security tool configurations. Organizations benefit from sharing cyber threat information internally and externally to enhance their security posture.
Additionally, Information Sharing and Analysis Organizations (ISAOs) play a crucial role in improving cybersecurity by facilitating the sharing of threat information among organizations. Establishing trust among members is essential for effective information sharing within ISAOs.[2]

In financial organizations, information is disseminated to relevant parties both internally and externally through various channels and mechanisms. Here are some ways information is disseminated externally

within financial organizations:

1. **Corporate Websites**: Financial organizations disseminate information for investors on their corporate websites, providing transparency and important updates.[3]
2. **Embedded Financial Analysts**: Firms utilize connected analysts within their private networks to disseminate information about relationship-based transactions. These analysts help verify transactions, leading to more accurate forecasts and lower forecast dispersion.[4]
3. **Communication with External Parties**: Relevant information resulting from assessments conducted by external parties is communicated to the board of directors, ensuring that key stakeholders are informed.[5]
4. **Standards for Economic and Financial Statistics Dissemination**: Financial organizations adhere to standards for the dissemination of economic and financial statistics to ensure accurate and timely information sharing.[6]
5. **Organizational Information Dissemination Within Collaborative Networks**: Utilizing digital communication tools within collaborative networks facilitates external communication and information dissemination, enhancing organizational success.[7]

Internally, financial organizations disseminate information through various channels and methods to ensure effective communication within the organization. Here are some ways information is disseminated internally within financial organizations:

1. **Company Apps and Channels**: Financial organizations utilize customized apps and cloud-based communication tools like Google Workspace, Slack, and internal intranet software networks to disseminate news, budget information, updates, and staff changes internally. These tools facilitate real-time communication among employees, enhancing collaboration and efficiency.[8]
2. **Project Management Software**: Internal teams in financial organizations use project management software to share project ideas, coordinate efforts, assign tasks, set priorities, and communicate feedback. These tools help streamline project workflows, improve data access, and enhance overall team performance.[8]
3. **Social Media Connections**: Social media platforms are increasingly used as internal communication tools within financial organizations. Employees utilize platforms like Twitter, Facebook, and LinkedIn to share ideas, ask work-related questions, solve problems, and improve work relationships. Social media serves as a powerful tool for information dissemination and enhancing employee engagement.
4. **Traditional Communication Tools**: Financial organizations also rely on traditional communication tools like face-to-face interactions, email, newsletters, memos, flyers, posters, press releases, and company websites to disseminate important information internally. These methods ensure that employees stay informed about company updates, changes, and announcements.[8]

In response to an advisory like the one presented in the scenario, where CISA releases information about increased DDoS activity targeting government entities, there are several actions that our

organization can take:

1. **Review and Implement Mitigations**:
    - Review the tactics, techniques, and procedures (TTPs) utilized by threat actors targeting government entities through DDoS attacks. Implement the mitigations provided in the advisory to protect your organization's network environment.[9]
2. **Enhance Cybersecurity Resilience**:
    - Refer to the Capacity Enhancement Guide and DDoS Guidance for Federal Agencies released by CISA, FBI, and MS-ISAC. These resources offer proactive steps to reduce the likelihood and impact of DDoS attacks. Consider adopting recommended contract vehicles and services for DDoS protection and mitigations.[10]
3. **Stay Informed and Educate Staff**:
    - Stay informed about the latest cybersecurity threats and advisories. Educate staff members on the risks associated with DDoS attacks and ensure they are aware of best practices for detecting, responding to, and recovering from such incidents.
4. **Conduct Security Testing**:
    - Regularly test your organization's cybersecurity incident response plan (CIRP) and DDoS response plan through exercises and simulations. Evaluate the effectiveness of these plans in addressing DDoS attacks and incorporate lessons learned from recent tests into future planning.[11]
5. **Collaborate with Industry Partners**:
    - Engage with industry partners, such as CISA, FBI, MS-ISAC, and other relevant organizations, to share information, best practices, and insights on combating DDoS attacks. Collaborative efforts can strengthen cybersecurity defenses and enhance incident response capabilities.[12]

By taking these actions in response to the advisory on increased DDoS activity targeting government entities, our organization can bolster its cybersecurity posture, mitigate risks associated with DDoS attacks, and enhance its readiness to detect, respond to, and recover from such incidents effectively.

DDoS Protections in Terms of Service Agreements with Outsourced Service Providers:

In our organization's Terms of Service agreements with outsourced service providers like ISPs, MSPs, or CSPs, the following DDoS protections are included:

1. **Cloud-Based DDoS Protection**:
    - Cloud service providers (CSPs) like Amazon Web Services, Microsoft Azure, and Rackspace offer DDoS protection services as add-ons to existing contracts. These services can help mitigate DDoS attacks by leveraging the CSP's infrastructure and expertise.[13]

2. **Outsourcing to Specialized Providers**:
    - Some cloud service providers may outsource DDoS protection services to specialized providers like Cloudflare or Imperva. This outsourcing allows for cost-effective high-capacity infrastructure that can be shared among multiple customers.[13]
3. **Bespoke DDoS Protection Profiles**:
    - Larger public cloud service providers offer optional per-customer DDoS protections for an additional fee. These protections provide customized profiles, in-depth analysis, and alerting capabilities tailored to the customer's organizational structure and requirements.[14]

When it comes to our financial institution, the organization take additional protections against attacks such as:

1. **Disseminate Audit Reports**:
    - Disseminate and communicate audit reports to all interested parties within the organization, ensuring transparency and accountability.[15]
2. **Implement Cybersecurity Directives**:
    - Adhere to cybersecurity directives issued by CISA, such as Binding Operational Directives (BODs) and Emergency Directives (EDs), to enhance cybersecurity resilience and compliance with federal requirements.[16]
3. **Collaborate with External Parties**:
    - Communicate relevant information resulting from assessments conducted by external parties, such as the FBI, to the board of directors. This collaboration ensures that key stakeholders are informed about potential threats and necessary actions.[17]
4. **Review Capacity Enhancement Guides**:
    - Review Capacity Enhancement Guides provided by CISA for Federal agencies, focusing on actionable recommendations and best practices to reduce cybersecurity risks. Implement relevant guidance to strengthen defenses against DDoS attacks and other cyber threats.[18]

Gaps or Limitations in Coverage:

Some gaps or limitations in coverage that may exist include:

1. **Limited Flexibility with Outsourced Protection**:
    - Outsourcing DDoS protection to a single vendor may limit flexibility in choosing solutions best suited for specific attacks and mitigation strategies.[19]
2. **Poor Analytics and Visibility**:
    - Outsourced services may lack detailed analytics on the nature of attacks, making it challenging to understand the impact of an attack and prevent future incidents

effectively.[19]

By considering these additional protections and addressing potential gaps in coverage, our agency can strengthen its defenses against DDoS attacks and enhance its overall cybersecurity resilience.

Additional Protections and Considerations:

a. **Enhanced DDoS Protections**:

- Consider additional DDoS protections in Terms of Service agreements with outsourced service providers like ISPs, MSPs, or CSPs. Evaluate the inclusion of cloud-based DDoS protection services and specialized providers for enhanced defense against DDoS attacks.[20]

b. **Identifying Gaps or Limitations**:

- Assess gaps or limitations in coverage related to outsourced DDoS protections. Evaluate flexibility in choosing solutions, analytics capabilities, and visibility into attack patterns to address any shortcomings effectively.[20]

By taking these actions and considering additional protections against DDoS attacks while addressing gaps in coverage, our financial institution can strengthen its cybersecurity posture, mitigate risks associated with cyber threats, and enhance its overall resilience in the face of evolving security challenges.

DDoS attack detection and mitigation

For a financial institution, implementing robust methods for DDoS attack detection and mitigation is crucial to safeguarding its operations and customer data. Some automated and manual methods that our agency can consider:

Automated Methods:

1. **AI-Powered Fraud Monitoring Systems**:
    - Implement AI-powered fraud monitoring systems that can ingest and analyze large volumes of data in real-time to detect anomalies and potential DDoS attacks. AI technology can adapt to evolving threats and provide more accurate detection capabilities.[21]
2. **Real-Time Transaction Monitoring**:
    - Utilize automated systems for real-time transaction monitoring to detect suspicious activities and potential DDoS attacks promptly. Establish behavioral profiles for customers to compare against normal activity and flag any deviations for further investigation.[21]
3. **Advanced Threat Detection Solutions**:
    - Deploy advanced threat detection solutions that offer complete visibility, behavioral analytics, and continuous monitoring capabilities to detect and respond to sophisticated attacks promptly. These solutions can help identify emerging threats like zero-day attacks or AI-generated threats.[22]

Manual Methods:

1. **Employee Training and Awareness**:
    - Conduct regular security education and awareness programs for employees to enhance their understanding of cybersecurity risks, DDoS attacks, and best practices for incident response. Ensure staff are trained on identifying potential threats and responding effectively.[21]
2. **Multi-Layered Security Systems**:
    - Develop multi-layered security systems that include administrative, physical, and technical controls to protect against various types of fraud, including DDoS attacks. Implement measures like access restrictions, asset monitoring, and cross-checking of data values.[21]
3. **Internal Fraud Monitoring**:
    - Monitor internal activities closely to detect any signs of intentional or unintentional fraud by employees. Establish protocols for identifying unusual behavior, unauthorized access, or suspicious transactions that could indicate internal threats.[21]

By combining automated methods like AI-powered systems and real-time monitoring with manual approaches such as employee training and multi-layered security systems, a financial institution can strengthen its defenses against DDoS attacks effectively while ensuring the integrity of its operations and customer assets.

DDoS Attack Detection and Mitigation
Notification Recipients by Automated Detection Tools:

- In a financial institution, automated detection tools like Kentik Protect can notify designated personnel within the agency about DDoS attacks. These tools can trigger alerts to security teams, network administrators, or IT staff responsible for incident response. Notifications can be customized based on predefined thresholds or attack patterns to ensure timely and effective response.[23]

Manual Detection of DDoS Attacks:

- Manual detection of DDoS attacks in our financial institution involves monitoring network traffic for anomalies that could indicate an ongoing attack. Security analysts may analyze traffic patterns, bandwidth utilization, and server performance metrics to identify sudden spikes or unusual behavior that align with DDoS attack characteristics. Additionally, manual detection may involve reviewing logs, firewall alerts, and intrusion detection system (IDS) notifications for signs of malicious activity.[24]

c. **Frequency of System Testing**:

- The systems used for DDoS detection and mitigation in a financial institution should be regularly tested to ensure their effectiveness and reliability. These tests can vary in frequency depending on the criticality of the systems and the evolving nature of cyber threats. It is

recommended to conduct periodic testing, such as quarterly or semi-annually, to validate the performance of automated detection tools, manual monitoring processes, and incident response procedures.[25]

By ensuring that notification recipients are well-defined for automated detection tools, implementing robust manual detection processes, and conducting regular system testing, our financial institution can enhance its readiness to detect and mitigate DDoS attacks effectively, safeguarding its operations and data against potential threats.

Edge Network Defenses for Mitigating Malicious Traffic in a Financial Institution

In order to reduce the risk of malicious traffic reaching its target while still allowing legitimate users to access agency services, a financial institution can acquire various edge network defenses. Here are some key tools and strategies that can reinforce network edge security:

1. **Traditional Network-Based Firewall**:
    - Implement a traditional network-based firewall as the first line of defense at the network edge. Firewalls permit or deny traffic based on IP address, protocol, or port number, effectively filtering out malicious traffic while allowing legitimate users to access services.[26]
2. **Intrusion Prevention Systems (IPS)**:
    - Utilize intrusion prevention systems to monitor network traffic for known malicious signatures. IPS can identify and block packets containing malicious signatures, preventing them from entering the secure side of the network and mitigating potential threats effectively.[26]
3. **Application-Layer Firewalls**:
    - Deploy application-layer firewalls that perform deep packet inspection up to Layer 7 of the OSI model. These firewalls enable administrators to block traffic based on specific applications or services being used, providing granular control over network traffic and enhancing security at the edge.[26]
4. **Network-Based Malware Protection**:
    - Implement network-based malware protection tools to defend against advanced threats at the network edge. These solutions offer additional layers of security by detecting and blocking malware-infected traffic, protecting critical assets from potential cyber attacks.[27]
5. **Cloud-Based Threat Intelligence Services**:
    - Consider leveraging cloud-based threat intelligence and sandboxing services to enhance network edge security. These services provide real-time threat intelligence, enabling proactive threat detection and response to emerging cyber threats, ensuring a robust defense mechanism against malicious activities.[27]

By incorporating these edge network defenses, including firewalls, intrusion prevention systems, application-layer firewalls, malware protection tools, and cloud-based threat intelligence services, a financial institution can significantly reduce the risk of malicious traffic reaching its target while maintaining accessibility for legitimate users to access agency services securely and efficiently.

By following the processes outlined by FISMA regulations, a financial institution can ensure that any reporting required by FISMA occurs as needed, maintaining compliance with legal standards and enhancing transparency in surveillance activities related to national security and foreign intelligence gathering.

1. **Authorization for Surveillance**:
    - Under FISMA, the Foreign Intelligence Surveillance Act (FISA) establishes procedures for surveillance and collection of foreign intelligence. The FISA Court oversees requests for surveillance warrants, ensuring compliance with legal requirements.[28]
2. **Judicial Oversight**:
    - The FISA Court reviews applications made by the U.S. Government for approval of physical search, electronic surveillance, and other investigative actions related to foreign intelligence. The court ensures that surveillance activities are conducted within legal boundaries and in accordance with constitutional principles.[29]
3. **Compliance Reporting**:
    - The Attorney General is mandated to inform the Intelligence and Judiciary Committees of the House and Senate on incidents of noncompliance with FISA Court-approved procedures by the Intelligence Community. This reporting includes details on the number of certifications and directives issued during the reporting period.[30]
4. **Procedures Approval**:
    - Within 120 days, the Attorney General must submit procedures to the FISA Court for approval on how the government will determine compliance with FISA regulations. The FISA Court reviews these procedures to ensure they align with legal requirements.[28]
5. **Oversight and Review**:
    - The FISA Court exercises oversight over surveillance activities, ensuring that proper procedures are followed and that any potential noncompliance is addressed promptly. The court's authority extends to approving surveillance warrants and overseeing intelligence investigations.[28]

Incorporating DDoS Attack Response into the CIRP in a Financial Institution

Incorporating Distributed Denial of Service (DDoS) attack response into a financial institution's Cyber Incident Response Plan (CIRP) is crucial for maintaining operational continuity and safeguarding against cyber threats. Here is how the our institution addresses the key aspects related to DDoS attacks within its CIRP:

a. Identifying and Documenting DDoS Attack Types:

- **Detection Process**: The financial institution should utilize tools for real-time detection of DDoS attacks, such as traffic analysis and anomaly detection systems.[31]
- **Response Plan**: The response plan should outline steps to identify the type of DDoS attack, including traffic analysis, distinguishing between legitimate and malicious requests, and implementing mitigation strategies like traffic filtering and rate limiting.[31]

b. Responding to and Recovering from DDoS Attacks:

- **Response Strategies**: The financial institution should activate pre-arranged response plans upon detecting a DDoS attack, including deploying automated anti-DDoS mechanisms, applying traffic filters, scaling up bandwidth, and collaborating with ISPs or cloud service providers for additional support.[31]
- **Rapid Recovery**: Rapid recovery involves adjusting network configurations, increasing network capacity if necessary, and continuous monitoring and adjustment of mitigation strategies until the attack subsides.[31]

c. Training Key Personnel on Roles and Responsibilities:

- **Role Definition**: Define roles within the incident response team, such as network engineers, security analysts, and communication coordinators, to ensure a coordinated response during a DDoS attack.[32]
- **Training Programs**: Conduct regular training sessions for key personnel to enhance their skills in recognizing DDoS attacks, understanding response protocols, and effectively executing their roles during an attack.[32]

A Cyber Incident Response Plan (CIRP) is a strategic plan developed to respond to potential computer incidents such as DDoS, data breaches etc. Our agency has exercised its CIRP against a DdoS attack. Lessons learned from such attacks emphasize the necessity of robust security measures to prevent disruptions and maintain public trust, especially in the financial services sector, which is increasingly targeted by DDoS attacks due to the potential risks they pose. Continuous monitoring, swift responses, and comprehensive cyber defense strategies to mitigate the impact of DDoS attacks on financial institutions.These actions taken to enhance incident response has helped a lot.

MODULE 2

Here we explores how our organization handles indicators of a DdoS attack, confirmation of an attack, mitigation, and monitoring and recovery efforts.

When the IT helpdesk experiences a surge in calls, several factors come into play that impact their ability to handle the increased volume effectively. One critical aspect is the average call handling time, as longer calls reduce the number of calls an agent can manage per day.
Additionally, the availability of staff plays a crucial role in managing call influxes, with an ideal throughput for agents ranging from 25 to 70 calls per day depending on various factors
The helpdesk can recognize the presence of a larger issue through various indicators and metrics that

signal potential problems within the organization.

1. **Monitoring Support Tickets**:
    - By tracking the number of support tickets opened versus solved, the helpdesk can identify trends in ticket volume and detect any sudden spikes in new tickets opened, which may indicate service delivery issues or disruptions requiring attention.[33]
    - Analyzing ticket distribution across different topics or products can help pinpoint areas that generate more tickets, highlighting potential problems with products or services that need addressing.[33]
2. **Response and Resolution Times**:
    - Monitoring response times, first response time, requester wait time, and resolution time provides insights into how efficiently issues are being addressed by the helpdesk.[33]
    - Longer response times or resolution times can indicate underlying issues that need to be addressed promptly to maintain customer satisfaction and service quality.[33]
3. **First Contact Resolution (FCR)**:
    - FCR metrics measure the percentage of tickets resolved after the first contact with a support agent, reflecting the efficiency of issue resolution processes.[33]
    - Tracking FCR rates and customer experience surveys can help identify areas where improvements are needed to enhance service quality and streamline problem-solving processes.[33]

Processes for Notifying and Escalating Issues

Establishing Communication Protocols:

- Large-scale DDoS attacks may necessitate an enterprise-level response, requiring a hierarchical structure for response coordination and communication among technical teams, management, and other stakeholders.[34]
- Implementing multiple bridge lines can facilitate effective communication during incidents, ensuring swift responses and coordination among different teams.[34]

- **Developing Incident Response Plans**:
    - Organizations should create a DDoS Response Annex within their incident response plan to outline specific processes for responding to DDoS attacks. This includes defining roles and responsibilities clearly to streamline decision-making and response efforts.[34]
    - Obtaining pre-approvals for invoking mitigation services can help expedite the response process without delays once an attack occurs.[34]
- **Engaging Service Providers**:

    - Establishing and maintaining relationships with upstream Internet Service Providers (ISPs) and DDoS mitigation providers is essential. These partners can assist in preventing system downtime during sustained DDoS attacks by sharing information and coordinating responses effectively.[34]

- **Communication Strategies**:
    - Organizations should engage channel leads, public relations teams, and develop incident notification strategies for both internal and external communications. This includes messaging for senior management, key service providers, customers, and the media to ensure transparency and timely updates during incidents.[34]

When a public-facing customer service call center experiences an influx of similar calls, several key actions can be taken:

Identifying a Bigger Issue:

- The customer service call center may realize there is a larger issue when there is a sudden surge in call volume reporting the same problem or issue, leading to overwhelmed representatives.[35]
- Signs like increased call wait times, higher abandonment rates, or recurring complaints about the same issue can indicate a systemic problem that needs attention.[35]

Notification and Escalation Processes:

- Processes for notifying and escalating the issue involve following predefined protocols that include notifying supervisors, managers, or specialized teams when call volumes exceed normal levels.[35]
- Escalation steps typically involve escalating from frontline agents to senior management if the issue persists or escalates in severity.[35]

Aggregating Network Disruptions:

- To aggregate network disruptions from the IT helpdesk and customer service call center, agencies can use centralized incident management systems that consolidate data from various sources for a comprehensive view of ongoing disruptions and their impact.[35]
- Integration of monitoring tools and incident reporting mechanisms allows for real-time tracking and correlation of network disruptions reported by different departments, facilitating effective response coordination.[35]

Confirming a DDoS Attack:

- **Indicators of a DDoS Attack**: To confirm a DDoS attack, your financial institution agency should monitor for signs like network latency, high processor and memory utilization, sluggish performance, high network traffic, or the inability to access websites.[36]
- **Contact Technical Professionals**: Once a DDoS attack is confirmed, the agency should contact appropriate technical professionals such as Internet Service Providers (ISPs) to gain a better understanding of the attack and take steps to block DDoS threat actors.[37]

Determining DDoS Attack Type:

- **Understanding Attack Patterns**: Your agency can determine the type of DDoS attack by analyzing traffic patterns, attack vectors used, and the impact on network performance during the attack.[38]
- **Leveraging Botnets**: DDoS attacks often leverage botnets—hijacked devices connected over the internet to generate overwhelming traffic from multiple attacking machines.[38]

Mitigating Cascading Effects:

- **Monitoring Network Assets**: To mitigate cascading effects of a DDoS attack, it's crucial to monitor other network assets for secondary attacks and update the DDoS response plan to enhance future response capabilities.[36]
- **Creating Baselines**: Establishing baselines of regular network activity helps in pinpointing future attacks promptly and developing proactive strategies to prevent disruptions.[36]

Additional DDoS-Specific Actions in the CIRP

Here are the additional DDoS-specific actions included in the Continuity of Operations Incident Response Plan (CIRP):

- **Actions Included**:
    - Ensuring all identified High Value Assets (HVAs) are assessed for vulnerabilities and exposure to the internet.
    - Enrolling all publicly exposed assets in CISA's Cyber Hygiene Services and verifying appropriate configurations of existing monitoring tools.
    - Conducting at least one agency-level DDoS tabletop exercise using the CISA DDoS Tabletop Exercise Package.[39]
- **Implementation**:
    - These actions are typically implemented by Federal Civilian Executive Branch (FCEB) agencies as part of their cybersecurity measures to enhance resilience against DDoS attacks.[39]

To continue monitoring and mitigating other cyber-attack vectors during a DDoS attack, your agency can leverage the following resources and strategies:

Technical and Personnel Resources:[36]

- **Technical Tools**: Utilize network monitoring tools, intrusion detection systems, and DDoS protection services to detect and mitigate various cyber threats concurrently.
- **Personnel Expertise**: Engage cybersecurity professionals with expertise in threat detection, incident response, and network security to manage multiple attack vectors effectively

Mitigating Other Attack Vectors:

- **Continuous Monitoring**: Maintain continuous monitoring of network traffic, system logs, and security alerts to identify and respond to any suspicious activities beyond the DDoS attack
- **Proactive Measures**: Implement proactive security measures such as regular vulnerability assessments, patch management, and access controls to prevent exploitation of vulnerabilities during a DDoS attack

Federal Notification Requirements and Process

- **Internal Notification**: Federal agencies should promptly notify their top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or information technology department within one hour of identifying a potential compromise to the confidentiality, integrity, or availability of a federal information system.[40]
- **External Notification**: Incidents involving federal Executive Branch civilian agencies must be reported to the National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Emergency Readiness Team (US-CERT) with the necessary data elements within one hour of identification.[40]

Notifying Upstream Service Providers

- **Engagement with ISPs**: Organizations experiencing a DDoS attack should engage with their Internet Service Provider (ISP) to understand the attack better and potentially block DDoS threat actors.[41]
- **Sharing Attacking IP Address**: Providing the attacking IP address to the ISP can help in enabling firewall settings and denying specific types of network traffic to reduce the risk of being used as a reflector in the attack.[41]

.

Additional Capabilities and Agreements

Agency Requirements and Collaborations:

- **Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA)**: If your agency relies on another agency, having an MOU/MOA in place ensures clear guidelines and responsibilities for collaboration.[42]
- **Third-Party Vendor Contracts**: Establishing contracts and activation processes with third-party vendors is crucial. Testing these processes ensures readiness for potential cyber incidents.[42]

Federal Guidelines and Resources:

- The Cybersecurity and Infrastructure Security Agency (CISA) has released guidelines to enhance the nation's cybersecurity, including improving incident response capabilities, threat

information sharing, and cybersecurity standards across federal agencies.[43]

- These guidelines emphasize the importance of proactive steps to reduce the impact of Distributed Denial-of-Service (DDoS) attacks, such as identifying critical assets, enrolling in DDoS protection services, and developing response plans.[36]

Reduced staffing around the holiday season can significantly impact agency response efforts. Here's how your organization can address staffing deficiencies and implement contingency plans:

Overcoming Staffing Deficiencies:

- **Internal Maximization**: Encourage internal staff to work additional shifts or assignments before resorting to external agencies, leveraging technology like marketplace apps to facilitate staff engagement.[44]
- **Build Internal Agency**: Establish an internal agency within your organization to provide premium pay and flexibility for existing staff, reducing reliance on external agencies and optimizing workforce utilization.[44]

Contingency Plans for Surge Staffing Requirements:

- **Vendor-Neutral Model**: Engage multiple staffing agencies to reduce reliance on a single provider, ensuring competitive bill rates and quick response times for securing staff.[44]
- **International RN Strategy**: Implement an international RN strategy to access candidates from various countries, reducing premium labor costs and enhancing workforce diversity.[44]

By maximizing internal resources, establishing internal agencies, adopting vendor-neutral models, and implementing international RN strategies, your agency can effectively address reduced staffing challenges during the holiday season and ensure continuity in response efforts.

Transition to Recovery and Post-Incident Phases

When does the Recovery phase of an event begin? What activities are involved in the Recovery phase of an event? The Recovery phase begins when hospital incident command determines that the event is de-escalating or over, allowing for the initiation of de-mobilization and recovery activities. These activities involve assessing critical elements of operation and ensuring safe, normal operations.[44]

Decision to Transition to Recovery Phase

The decision to transition to the recovery phase is made when the hospital incident command determines that the event is de-escalating or over, signaling a shift towards recovery activities.[44]

Communicating Incident Recovery Status

Incident recovery status is communicated to internal and external partners/stakeholders through clear and consistent messaging. Communication is crucial during recovery to keep all parties informed about progress and next steps.[45]

Conducting Post-Incident Review

Post-incident reviews are conducted by the agency to evaluate response actions, identify strengths,

weaknesses, and areas for improvement. These reviews are essential for learning from past incidents and enhancing future response strategies.[46]

Incorporating Lessons Learned into Continuous Improvement Planning

Lessons learned and areas for improvement identified during post-incident reviews are incorporated into the agency's continuous improvement planning. This process ensures that insights from past incidents are used to enhance preparedness and response capabilities.[46]

To increase the resilience of your organization against future DDoS attacks, consider implementing the following changes based on the provided search results:

1. **Utilize Cloud-Based DDoS Mitigation Solutions**:
    - Implement cloud-based DDoS mitigation solutions to benefit from dedicated staff for quicker response times, high network bandwidth, and automated replication options to maintain services during attacks.[47]
2. **Engage with Managed Service Providers (MSPs)**:
    - Consider partnering with MSPs specialized in cybersecurity to actively monitor network traffic, detect attacks, and redirect harmful traffic away from your network. MSPs offer expertise, advanced technologies, 24/7 monitoring, and quick response capabilities to mitigate attacks effectively.[47]
3. **Conduct Post-Incident Analysis**:
    - After a DDoS attack, analyze the impact by identifying targeted assets, attack methods used, duration of the attack, financial losses incurred, and any reputational damage. Monitor network assets for unusual activity and assess the damage to understand the impact on your organization.[48]
4. **Maintain Transparency and Communication**:
    - Verify if third-party DDoS mitigation providers fulfill their service level agreements (SLAs) and communicate transparently with all stakeholders about the attack's impact, mitigation steps taken, recovery status, and additional security measures being implemented.[48]
5. **Build Cyber Resilience**:
    - Shift towards Cyber Resilience by developing the ability to withstand disruptions to IT capabilities supporting critical business operations. This approach addresses people, processes, and technology challenges associated with traditional contingency planning methods to deliver an always-on enterprise.[48]

REFERENCES:

1. **https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf**

2. **https://www.csoonline.com/article/567485/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html**

3. Dissemination of information for investors at corporate Web sites - ScienceDirect

4. https://publications.aaahq.org/accounting-review/article-abstract/95/2/257/4232/Information-Dissemination-through-Embedded?redirectedFrom=fulltext

5. https://www.unifiedcompliance.com/products/search-controls/control/07117/

6. https://www.imf.org/external/np/sta/dsbb/1996/030896.pdf

7..https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1993&context=gscis_etd

8.https://work.chron.com/tools-disseminating-workplace-information-11070.html

9.https://www.cisa.gov/news-events/alerts/2024/02/15/cisa-and-ms-isac-release-advisory-compromised-account-used-access-state-government-organization

10.https://www.cisa.gov/news-events/alerts/2022/10/28/joint-cisa-fbi-ms-isac-guide-responding-ddos-attacks-and-ddos-guidance-federal-agencies

11.https://www.cisa.gov/sites/default/files/2023-03/formal_response_to_cisa_cybersecurity_advisory_committee_recommendations_june_2022%20%282%29.pdf

12.Response to CISA Advisory (AA24-060B) - AttackIQ

13. Cloud DDoS protection: What enterprises need to know | TechTarget

14.Best DDoS Protection and Mitigation Services 2024 (cloudzenpartners.com)

15.Disseminate and communicate the audit report to all interested personnel and affected parties identified in the distribution list. | Simplifying Compliance Management | UCF (unifiedcompliance.com)

16.Cybersecurity Directives | CISA

17.Federal Bureau of Investigation - Wikipedia

18.Capacity Enhancement Guides for Federal Agencies | CISA

19.**Automated, Accurate, Flexible DDoS Detection and Mitigation | Kentik Blog**

20.CISA and MS-ISAC Release Advisory on Compromised Account Used to Access State Government Organization | CISA

21. Fraud Management in Banking: Detection, Prevention & More – Hitachi Solutions (hitachi-solutions.com)

22. Protecting Your Assets: Why Financial Services Firms Need Advanced Threat Detection (mixmode.ai)

23.Detect and Mitigate DDoS | Solutions | Kentik

24.DDoS Detection | Kentik

25.Fast DDoS Detection and Prevention | FastNetMon

26.What tools can reinforce network edge security? | TechTarget

27.Comprehensive DDoS Protection | Edge

28.The Foreign Intelligence Surveillance Act of 1978 (FISA) | Bureau of Justice Assistance (ojp.gov)

29.FISA FISC Lawyer in Boston | FISC Court | Dhar Law LLP

30.Special Report: A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks (Full Report) (justice.gov)

31.Emergency Procedures To Responding To DDoS Attacks (redswitches.com)

32.6 Tips to Train Your Team for DDoS Attacks (linkedin.com)

33.12 help desk metrics to measure support performance (zendesk.com)

34. distributed-denial-of-service-ddos-attacks-march-2021.pdf (aha.org)

35.Does an Influx of Calls Overwhelm Your Call Center? Here’s Why. (atsg.net)

36.CISA, FBI, MS-ISAC Publish Guidelines For Federal Agencies on DDoS Attacks - Infosecurity Magazine (infosecurity-magazine.com)

37.CISA, FBI, MS-ISAC Provide Guidelines For DDoS Incident Response (healthitsecurity.com)

38.U.S. Agencies Release Guidelines for DDoS Attacks (secureworld.io)

39.Capacity Enhancement Guide: Additional DDoS Guidance for Federal Agencies (cisa.gov)

40.US-CERT Federal Incident Notification Guidelines (cisa.gov)

41.CISA, FBI, MS-ISAC Provide Guidelines For DDoS Incident Response (healthitsecurity.com)

42.National Cybersecurity Protection System | CISA

43.Executive Order on Improving the Nation's Cybersecurity | CISA

44.When does the Recovery phase of an event begin? What activities are involved in the Recovery phase of an event? - Emergency Preparedness (calhospitalprepare.org)

45.Rural Community Recovery after an Emergency or Disaster - RHIhub Toolkit (ruralhealthinfo.org)

46.phe.gov/Preparedness/planning/mscc/healthcarecoalition/chapter3/Pages/establishingprocedures.aspx

47.Defending against distributed denial of service (DDoS) attacks – ITSM.80.110 - Canadian Centre for Cyber Security

48.us-building-resilience-to-denial-of-service-attacks.pdf (deloitte.com)