Real Estate ISAC Information Sharing and Analysis Center

Serving the Commercial Facilities Sector

TLP GREEN: Limited disclosure, restricted to the community. Sources may use **TLP GREEN** when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share **TLP GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP GREEN** information may not be released outside of the community.

21 February 2018

DENIAL OF SERVICE

IN BRIEF: The most common attack method that springs to mind when someone mentions of Denial of Service (DoS) attempts is usually Distributed Denial of Service (DDoS). These words strike fear in the heart of some who wonder if their own organization could meet the threats while others have become complacent because "our DDoS mitigation provider will handle it." Not only have incidents resulting in DoS conditions risen drastically over the last five years, but the variety of tactics used by threat actors has expanded. We must remember that most incidents of denial of service still result from hardware failures, natural disasters, animals, or human incompetence. Far fewer are the result of malicious actors. However, the capabilities and infrastructure of malicious actors have expanded. This expansion is enabled by a growing supply chain of software and services available to adversaries with intent who previously lacked the capability but could afford to pay someone to carry out their objectives. The impact to reservation systems, multimedia streaming services, e-commerce transactions, securities trading, banking, and ticket sales can exceed millions of dollars per hour (or less) of downtime. The impact to security systems, emergency response systems, and ICS systems such as those found in building management or operational IoT devices could be harm to people or loss of life.

KEY TAKEAWAYS & RECOMMENDATIONS:

- DoS conditions result from a variety of unintentional and malicious acts.
- The tactics of a threat actor may not result in the intended impact.
- DDoS can take many forms.
- DoS has been combined with other methods to serve a wider variety of motives.
- While DoS is often addressed as a network resilience issue, not all incidents originate or impact operations over the network.

BACKGROUND. A Denial of Service (DoS) occurs when legitimate users are prevented from accessing information or services. By targeting a computer or its network connection, or the computers and network of the sites one wishes to use, an attacker may be able to prevent individuals or organizations from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer. Distributed Denial of Service (DDoS) may use one's computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of a computer. He or she could then force that computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including that one, to launch the denial-of-service attack.

Before we address the tactics of our adversaries and possible mitigations for DoS and DDoS attacks, we must remember that the most common causes of service outages are still general hardware failures, power outages, natural disasters or animals. Accidental human actions or mistakes (or failures to act) remain near the top of that list. Malicious attacks have not yet become a prominent cause for service outages on the Internet. This does not mean that could not change in the future.

A Quick Guide published by US-CERT in 2014 gives an example of different DDoS attack tactics based on a model of networking called the OSI model. The model has 7 layers that represents the component functions needed for two or more computers to communicate and exchange data over a network. It should be noted that the OSI model is a figurative model. There are no actual "layers" to networking. The model is however helpful in thinking about all the services, equipment, and software needed for remote systems to connect and exchange data.

Attack Possibilities by OSI Layer

OSI Layer	Protocol Data Unit (PDU)	Layer Description	Protocols	Examples of Denial of Service Techniques at Each Level	Potential Impact of DoS Attack	Mitigation Options for Attack Type
Application Layer (7)	Data	Message and packet creation begins. DB access is on this level. End-user protocols such as FTP, SMTP, Telnet, and RAS work at this layer	Uses the Protocols FTP, HTTP, POP3, & SMTP and its device is the Gateway	PDF GET requests, HTTP GET, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)	Reach resource limits of services Resource starvation	Application monitoring is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDoS attacks
Presentation Layer (6)	Data	Translates the data format from sender to receiver	Uses the Protocols Compression & Encryption	Malformed SSL Requests -- Inspecting SSL encryption packets is resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server	The affected systems could stop accepting SSL connections or automatically restart	To mitigate, consider options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in protected memory on a secure bastion host
Session (5)	Data	Governs establishment, termination, and sync of session within the OS over the network (ex: when you log off and on)	Uses the Protocol Logon/Logoff	Telnet DDoS-attacker exploits a flaw in a Telnet server software running on the switch, rendering Telnet services unavailable	Prevents administrator from performing switch management functions	Check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability
Transport (4)	Segment	Ensures error-free transmission between hosts: manages transmission of messages from layers 1 through 3	Uses the Protocols TCP & UDP	SYN Flood, Smurf Attack	Reach bandwidth or connection limits of hosts or networking equipment	DDoS attack blocking, commonly referred to as blackholing, is a method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. Black holding is typically deployed by the ISP to protect other customers on its network from the adverse effects of DDoS attacks such as slow network performance and disrupted service
Network (3)	Packet	Dedicated to routing and switching information to different networks. LANs or internetworks	Uses the Protocols IP, ICMP, ARP, & RIP and uses Routers as its device	ICMP Flooding - A Layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth	Can affect available network bandwidth and impose extra load on the firewall	Rate-limit ICMP traffic and prevent the attack from impacting bandwidth and firewall performance
Data Link (2)	Frame	Establishes, maintains, and decides how the transfer is accomplished over the physical layer	Uses the Protocols 802.3 & 802.5 and it's devices are NICs, switches bridges & WAPs	MAC flooding -- inundates the network switch with data packets	Disrupts the usual sender to recipient flow of data -- blasting across all ports	Many advances switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations; allow discovered MAC addresses to be authenticated against an authentication, authorization and accounting (AAA) server and subsequently filtered
Physical (1)	Bits	Includes, but not limited to cables, jacks, and hubs	Uses the Protocols 100Base T & 1000 Base-X and uses Hubs, patch panels, & RJ45 Jacks as devices	Physical destruction, obstruction, manipulation, or malfunction of physical assets	Physical assets will become unresponsive and may need to be repaired to increase availability	Practice defense in-depth tactics, use access controls, accountability, and auditing to track and control physical assets

The Quick Guide also explains different types of DDoS attack traffic. For simplicity most DDoS attacks fall into one of three major categories: volume based attacks, protocol attacks, and application attacks.

Possible DDoS Traffic Types	
HTTP Header	HTTP headers are fields which describe which resources are requested, such as URL, a form, JPEG, etc. HTTP headers also inform the web server what kind of web browser is being used. Common HTTP headers are GET, POST, ACCEPT, LANGUAGE, and USER AGENT. The requester can insert as many headers as they want and can make them communication specific. DDoS attackers can change these and many other HTTP headers to make it more difficult to identify the attack origin. In addition, HTTP headers can be designed to manipulate caching and proxy services. For example, is it possible to ask a caching proxy to not cache the information.
HTTP POST Flood	An HTTP POST Flood is a type of DDoS attack in which the volume of POST requests overwhelms the server so that the server cannot respond to them all. This can result in exceptionally high utilization of system resources and consequently crash the server.
HTTP POST Request	An HTTP POST Request is a method that submits data in the body of the request to be processes by the server. For example, a POST request takes the information in a form and encodes it, then post the content of the form to the server.
HTTPS Post Flood	An HTTPS POST Flood is an HTTP POST flood sent over an SSL session. Due to the use of SSL it is necessary to decrypt this request in order to inspect it.
HTTPS POST Request	An HTTPS POST Request is an encrypted version of an HTTP POST request. The actual data transferred back and forth is encrypted.
HTTPS GET Flood	An HTTPS GET Flood is an HTTP GET flood sent over an SSL session. Due to the SSL, it is necessary to decrypt the requests in order to mitigate the flood.
HTTPS GET Request	An HTTPS GET Request is an HTTP GET Request sent over an SSL session. Due to the use of SSL, it is necessary to decrypt the requests in order to inspect it.
HTTP GET Flood	An HTTP GET Flood is a layer 7 application layer DDoS attack method in which attackers send a huge flood of requests to the server to overwhelm its resources. As a result, the server cannot respond to legitimate requests from the server.
HTTP GET Request	An HTTP GET Request is a method that makes a request for information for the server. A GET request asks the server to give you something such as an image or script so that it may be rendered by your browsers.
SYN Flood (TCP/SYN)	SYN Flood works by establishing half-open connections to a node. When the target receives a SYN packet to an open port, the target will respond with a SYN-ACK and try to establish a connection. However, during a SYN flood, the three-way handshake never completes because the client never responds to the server's SYN-ACK. As a result, these "connections" remain in the half-open state until they time out.
UDP Flood	UDP floods are used frequently for larger bandwidth DDoS attacks because they are connectionless and it is easy to generate protocol 17 (UDP) messages from many different scripting and compiled languages.
ICMP Flood	Internet Control Message Protocol (ICMP) is primarily used for error messaging and typically does not exchange data between systems. ICMP packets may accompany TCP packets when connecting to a sever. An ICMP flood is a layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth.
MAC Flood	A rare attack, in which the attacker sends multiple dummy Ethernet frames, each with a different MAC address, Network switches treat MAC addresses separately, and hence reserve some resources for each request. When all the memory in a switch is used up, it either shuts down or becomes unresponsive. In a few types of routers, a MAC flood attack may cause these to drop their entire routing table, thus disrupting the whole network under its routing domain.

While the Quick Guide is extremely helpful in giving security professionals a way to think about denial of service attacks and provides mitigation ideas for each, adversaries have improved their capabilities and combined these tactics with others. DoS and DDoS were previously thought to be the tactic used for disruption or degradation of operations or the provision of services. It was thought to be the work of activists or competitors attempting to sabotage the operations of a government agency or corporation with whom it took issue. However, the Further aiding DoS efforts is the construction and maintenance of botnets. A bot is a small automated script or set of scripts that perform simple tasks. A botnet consists of multiple network connected computers or servers that run bots. Botnets can be productive, and many are used for legitimate functions. Increasingly however, botnets have been constructed or abused to support malicious operations. Beyond botnets, as-a-service infrastructure is now available for anyone with a motive and some money. Among the infrastructure abused for DoS attacks are booter and stressor services.

A few high-profile campaigns that raised the concern of DoS/DDoS for many organizations:

- **Entertainment and Media**: In November of 2014, **Sony Pictures Entertainment** experienced a series of malicious activity attributed to North Korean government sponsored actors. The attacks ranged from DDoS to destructive malware to data theft and exposure of sensitive information. The malware that included commands and controls for the DDoS infrastructure were named DeltaAlpha, DeltaBravo and DeltaCharlie. These are all part of the North Korean HIDDENCOBRA infrastructure. That actor group is also associated with the names: Lizard Squad, Guardians of Peace, NewRomanic Cyber Army Team, IsOne, and Whois. The group has been active in a variety of activity dating back to 2007 and remains active today. Notable DDoS attacks include those on US and South Korean media, critical infrastructure, and financial organizations.
- **Entertainment and Media**: In 2015 TV5 Le Monde in France was attacked by a group claiming support for ISIS and a group claiming support for the Syrian government a short time before that. It is very common for media and entertainment firms to be targeted for disruption by organizations that resent the news reports or perspectives presented by the media or the values reflected in movies, documentaries, or TV shows.
- **Entertainment and Media**: In May of 2017, French news sites for Le Monde, Le Figaro, and L'Obs were temporarily forced offline due to an attack on their content delivery network provider, Cedexis. Other Cedexis clients including several manufacturing firms were also affected.
- **#OperationAbabil**: Actors calling themselves the Iz-ad-din-al-Qassam cyber fighters (QCF) launched DDoS attacks against financial institutions between 2012 and 2014. Each major phase of the campaign chronologically coincided with IAEA negotiations regard nuclear non-proliferation with Iran. The activity was later attributed to Iran and several Iranian nationals were indicted for the activity.
- **DDoS Attack on Spamhaus.org**:In March of 2013, Cloudflare and upstream providers mitigated what was then the most voluminous DDoS attack ever against Spamhaus.org. The website did not go down or become unresponsive during the attack. After Cloudflare measured volumes up to 120Gbps before the attackers changed their strategy and began attacking the upstream providers who measured volumes up to 300Gbps.
- **IoT**: In 2016, the Mirai malware infected millions of IoT devices using them to attack the sites belonging to cyber security journalist Brian Krebs (krebsonsecurty.com) as well as the DNS provider Dyn, and impacting Internet access in Liberia. The botnet generated the largest DDoS traffic volumes on record at the time exceeding 620Gbps to attack krebsonsecurity.com and 1.1 – 1.5Tbps to attack French web host OVH. The IoT devices affected in the latest Mirai incidents were primarily home routers, network-enabled cameras, and digital video recorders. The source code for Mirai was published in September of that year allowing anyone to abuse it to launch similar attacks.
- **IoT**: In April of 2017, ICS-CERT informed constituents about a new campaign dubbed Brickerbot. This malware exploited default and hard-coded passwords in IoT devices to permanently "brick" or render dysfunctional affected IoT devices. There were two major strains of the malware. Manual device resets to factory defaults or hardware replacement were necessary to remediate the impact of the malware.

Just over a week ago, the 2018 Pyeongchang Olympic website was down for about 12 hours beginning during the opening ceremonies for the 2018 games. The DoS resulted from a decision to take the server down for remediation purposes. As more details have emerged a malicious attack was launched against the Olympic infrastructure using a wiping tool that self-propagates through a network. The attack was in planning for several months as emerging data indicates an IT provider for the games was compromised along with credentials for some of the sites and infrastructure. The malware was contained, and the systems and network remediated with little impact to the Olympic systems or network.

Now, DoS and DDoS are used to provide a smoke screen for other activities such as intrusion and data theft. One example of this is the DirtJumper campaign quite familiar to financial institutions. Another example is the Dyre or Dyre Wolf malware that used DDoS traffic to hide unauthorized wire transfers. DoS tactics are also used to create race conditions to intercept user credentials or perform session hijacking techniques. To complicate matters, DoS can result from the attempted exploitation of many vulnerabilities. In one case, an intruder's attempts to guess username/password combinations for one firm's FTP server caused a denial of service condition. The bandwidth of the frequent guesses

exceeded the capacity of the network connection and the server was unable to respond to legitimate attempts at access. Fortunately, it could not respond to the unauthorized access attempts, either. Another significant evolution is the use of DDoS in extortion campaigns. Both activists and financially motivated criminals are now using the threat of DDoS to influence decision making and behavior or to collect ransom payments from intended victims. Crypto currency mining programs that use up vast amounts of system resource can simulate a denial of service condition (or even cause one directly). Beware of that possibility as this is the latest type of malware used by financially motivated criminals. For those who are intentionally investing resources in crypto currency mining, be sure to pay careful attention to system configuration, network bandwidth, and memory resources so the mining program does not overtax a system or network of systems.

In addition to the exploitation of ICS and IoT devices, adversaries have also compromised cyber-physical emergency response capabilities and have begun to research and test attack methods for non-traditional Internet technologies. For example, several call centers including 911 call centers have experienced disruption in the form of telephone denial of service or TDoS. TDos can take advantage of the use of data networks for video conferencing, phone calls, or other multimedia use. Telephones themselves have been compromised or protocols for data exchange abused.

Other ways to cause DoS conditions result from physical destruction like cutting network cables, or physically damaging network devices. Jamming radio frequencies or introducing other types of interference can prevent the communications via wireless means. Preventing access or the ability to repair a device can also result in a denial of service. That is achieved by overwriting device firmware or removing or changing administrative accounts or credentials. Other ways to prevent customers from accessing services are to redirect traffic away from a merchant's site by tampering with DNS architecture, hijacking domain names, or other public identifiers.

With the increased adoption of shared infrastructure such as public cloud services, attacks on others can result in outages of the service provider which can impact any other client organization.

MITIGATION. Considerations must be applied to consider one's organization as the target victim as well as prevent abuse of that organization's assets from becoming part of an attacking botnet.

Mitigations Chart

	In Case You are the Target	**Prevent Participation**

Planning	• Contact your Internet Service Provider, Content Delivery Network Provider, and Cloud Services Providers and ask about their response to DoS/DDoS or high traffic volumes?
	  ○ Discuss the possibility of a DDoS attack.
	  ○ Estimate traffic needs and future bandwidth requirements.
	• Learn What your cyber insurance policy covers in terms of DDoS mitigation/response.
	• Procure and install monitoring equipment including the ability to perform packet captures, stateful inspection, netflows, and other network behavior.
		• Install and maintain anti-virus software.
		• Install a firewall and configure it to restrict traffic coming into and leaving your computer.
		• Follow good security practices for distributing your email.
		• Applying email filters may help you manage unwanted traffic.
		• Install and maintain anti-virus software.
		• Install a firewall and configure it to restrict traffic coming into and leaving your computer.
		• Follow good security practices for distributing your email address. Applying email filters may help you manage unwanted traffic.

	• Obtain a baseline for "normal" bandwidth usage and traffic type. • Inventory all network equipment and all hardware components for critical systems – determine how soon each will require replacement. • Be sure all network equipment is included in vulnerability management and software update plans. • Ensure all systems and network appliances are included in identity and access management programs. • Assess network architecture to determine where network segmentation is feasible. • Include cloud based assets and services in all maintenance and planning activities. • Obtain DDoS mitigation services in advance of any attack. Determine what level of service is needed and what SLAs will apply to response scenarios. • Design a DDoS response playbook and include service providers in exercises to test the playbook.	• Subscribe to information sharing or commercial services that will inform you of vulnerabilities in the hardware, software, devices and firmware you use and any available or known exploitation of those items. • Monitor incoming and outgoing traffic, especially the outgoing traffic from your network connected assets. • Coordinate remediation efforts with law enforcement. If one of your assets has been recruited into a botnet, law enforcement may need some data points before you remediate the infection. Doing so can help law enforcement map criminal infrastructure and coordinate botnet takedowns. This will cripple adversary operations longer and raises the cost for attackers to maintain botnet infrastructure.

Detection	• Look for the following indicators:
	  ○ unusually slow network performance (opening files or accessing websites)
	  ○ unavailability of a particular website
	  ○ inability to access any website
	  ○ dramatic increase in the amount of spam you receive in your account
	• Use network flow to detect spoofed packets. (See the Mitigation section below for information on verifying spoofed traffic before blocking that traffic.)
	• Use network flow or other summarized network data to monitor for an unusual number of requests to at-risk UDP services.
	• Use network flow to detect service anomalies (e.g., bytes-per-packet and packets-per-second anomalies).
		Attempts to compromise assets for participation on botnets often appear as intrusion attempts rather than DoS attempts. Pay attention to the use of common software exploits or unauthorized external vulnerability scanning against your assets.
		
		In order to participate in a botnet automated scripts must be installed on the system and commands must be received. Often the bot will be asked to report back to another bot, a bot herder, or a command and control (C2) server. Watch for communication with known malicious botnet C2 systems.
		
		Monitor Internet connected hosts and devices for the creation of files, startup of new services or processes, or the injection of code or data from unusual sources. A web application firewall (WAF) can be helpful for monitoring for such changes as well as host based data integrity controls.

	• You don't generally need to receive the request responses when conducting a DoS attack. If you want to test for Denial of Service conditions yourself, we recommend that you use HEAD instead of GET requests where possible, or use the Range header with a value of 'bytes=0-0' • Certain methods of error handling are resource-intensive. If you encounter a verbose error, this might indicate that there is a large amount of computing power involved. For example, stack traces are known to be resource-intensive. • A small amount of input that leads to an exceptionally large return value is always a good place to look for DoS, especially if recursion is involved. • Whenever you encounter a DoS error, you should consider whether this is the worst impact the vulnerability might have. If there is an **Local File Inclusion**, try to read sensitive information rather than recreating a DoS. And if you can issue a limited set of commands, try to escape from the sandbox and turn it into a full RCE, instead of wasting the system's resources. This helps to more accurately calculate the risk for the developers to which you report the flaw. Should you submit your findings to a bug bounty program, it is also likely to lead to a more lucrative payout. • Detect and alert large UDP packets to higher order ports. • Detect and alert on any non-stateful UDP packets. (A simple Snort example is below. The approach will need to be customized to each environment with a whitelist and known services.) • Upstream providers should maintain updated contacts and methods with downstream customers to send alerts by network.	

Response and Mitigation	• Before reacting to perceived DDoS threats or traffic, verify there is a malicious event. Changes in process or addition of new technology can result in a spike in traffic volume as can some periodic business activities. Improper response actions can result in a security team that causes a DoS condition to a critical business function.
	• During a DoS event, involve all necessary IT, Legal, functional, communications, security, and networking personnel. Collaborate with ISPs and business units to determine the best course of action.
	• Share information about what you are experiencing with yoru information sharing communities and law enforcement partners. If they are experiencing similar activity, it may be more efficient to determine course of action in collaboration with others. Also, ask if anyone has experienced this pattern of attack before, if so, they may have a tried and true set of mitigation steps that can speed your time to recovery.
	• Simplifying interfaces with customers and partners can ease the impact of a layer 7 attack.
	• The following steps can help mitigate a DRDoS attack:
	  ○ Use stateful UDP inspections—such as reflexive access control lists—to reduce the impact to critical services on border firewalls or border routers.
	  ○ Use a Border Gateway Protocol (BGP) to create a Remotely Triggered Blackhole, preferably in coordination with upstream providers or ISPs.
	  ○ Maintain a list of primary upstream provider emergency contacts to coordinate responses to attacks. Upstream providers should conduct mitigation in coordination with downstream customers.
		• Disconnect device from the network.
		• While disconnected from the network and Internet, perform a reboot. Because botnet malware can exist in dynamic memory, rebooting the device clears the malware.
		• Ensure that the password for accessing the device has been changed from the default password to a strong password.
		• You should reconnect to the network only after rebooting and changing the password. If you reconnect before changing the password, the device could be quickly re-infected with the botnet malware.
		• Leverage rate-limiting on routers adjacent to the firewall and Internet.
		• Leverage firewall Access Control Lists (ACLs)
		• Implement SYN proxy mechanisms
		• Limit the number of SYNs per second per IP
		• Limit the number of SYNs per second per destination IP
		• Set ICMP flood SCREEN settings (thresholds) in the firewall
		• Set UDP flood SCREEN settings (thresholds) in the firewall

	• In general, ISP network and server administrators should use the following best practices to avoid becoming amplifier nodes:
	  ○ Regularly update software and configurations to deny or limit abuse (e.g., DNS response rate limit).
	  ○ Disable and remove unwanted services or deny access to local services over the Internet.
	  ○ Use UDP-based protocols—e.g., quality of service (QoS) on switching and routing devices—to enable network-based rate-limiting to legitimate services provided over the Internet.
	  ○ Work with Customer Provider Edge manufacturers for secure configuration and software.
	• As a service provider, to avoid any misuse of Internet resources:
	  ○ Use ingress filtering to block spoofed packets
	  ○ Use traffic shaping on UDP service requests to ensure repeated access to over-the-Internet resources is not abusive.
	  ○	

Investigation and Recovery	If possible, implement packet captures during a DDoS incident. Conduct a careful inspection of all traffic and patterns to identify any other types of malicious events during the DDoS incident. If DDoS was used as a distraction or smokescreen for other activity, detection is necessary ASAP. Identify any patterns not discovered during the event and use them to refine firewall rules, proxy permissions, and other controls while reducing the false positive alerts generated by those same controls. Ensure that any assets modified during the incident or taken out of service during the incident are restored with all security and privacy controls in-tact.	It may be helpful to compare suspicious or compromised devices with a recent backup of the system (provided the backup is verified to be clean). This can help to detect changes to the configuration, data, programs, and files and help to ensure a complete remediation and recovery. Be sure to report to law enforcement and share information with industry peers so that the spread can be stopped, and further incidents can be prevented. Industry peers may also be instrumental in suggesting refinements for detection and mitigation controls thus reducing the cost of mitigation and reducing impact of security measures for business units.

Reporting and Information Sharing	• Establish regular information sharing relationships and communication with others in your sector, geographic region, especially the relevant ISAC and government partners. • If you were unable to share information during the incident, be sure to do so after a complete investigation. Update any information shared or provide a complete summary of the incident and mitigation strategies that proved effective. Others will appreciate learning from your experiences when they face similar activity in the future.	See the previous column.