Before a Cyber Attack or Intrusion Educate the organization's senior management about cyber threats and risk management. Review and adopt risk management practices found in guidance such as the National Institute of Standards and Technology Cybersecurity Framework. Identify mission critical data and assets (<i>i.e.</i> , your 'Crown Jewels') and institute tiered security measures to appropriately protect those assets. Create an actionable incident response plan. Test the plan up-to-date to reflect changes in personnel and structure. Develop relationships with relevant law enforcement and other agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident. Test the plan up-to-date to reflect changes in personnel and structure. Institute basic cybersecurity procedures, such as a patch management program. Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Have procedures in place that will permit lawful network monitoring. Ensure legal counsel is familiar with legal issues associated with cyber incidents. Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan. Ouring a Cyber Attack or Intrusion "Imaging" the network. Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch. Minimize continuing damage consistent with your cyb	Cyber Incident Preparedness Checklist		
Educate the organization's senior management about cyber threats and risk management. Review and adopt risk management practices found in guidance such as the National Institute of Standards and Technology Cybersecurity Framework. Identify mission critical data and assets (<i>i.e.</i> , your "Crown Jewels") and institute tiered security measures to appropriately protect those assets. Create an actionable incident response plan. Develop relationships with relevant law enforcement and other agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident. Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Have procedures in place that will permit lawful network monitoring. Ensure legal counsel is familiar with legal issues associated with cyber incidents. Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan. During a Cyber Attack or Intrusion Maintize continuing damage consistent with your cyber incident response plan. Collect and preserve data related to the incident period of ongoing attacks. Consistent with your incident response plan. Collect and preserve data related to the incordent set of of morganization. In incident by Imaging" the network. Keeping records of o			
Review and adopt risk management practices found in guidance such as the National Institute of Standards and Technology Cybersecurity Framework. Identify mission critical data and assets (i.e., your "Crown Jewels") and institute tiered security measures to appropriately protect those assets. Create an actionable incident response plan. Test the plan up-to-date to reflect changes in personnel and structure. Develop relationships with relevant law enforcement and other agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident. Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Have procedures in place that will permit lawful network monitoring. Ensure legal counsel is familiar with legal issues associated with cyber incidents. Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan. During a Cyber Attack or Intrusion Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch. Minimize continuing damage consistent with your cyber incident response plan. Collect and preserve data related to the incident by "Imaging" the network. Keeping all logs, notes, and other records. Keeping all logs, notes, and other records. Recordi			
Institute of Standards and Technology Cybersecurity Framework. Identify mission critical data and assets (<i>i.e.</i> , your "Crown Jewels") and institute tiered security measures to appropriately protect those assets. Create an actionable incident response plan. Test the plan by conducting exercises. Develop relationships with relevant law enforcement and other agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident. Test the plan up-to-date to reflect changes in personnel and structure. Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Have procedures in place that will permit lawful network monitoring. Ensure legal counsel is familiar with legal issues associated with cyber incidents. Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan. "Imaging" the network. Collect and preserve data related to the incident particularly whether it is a malicious act or a technological glitch. "Imaging" the network. Minimize continuing damage consistent with your cyber incident response plan. "Imaging" the network. Collect and preserve data related to the incident personnel and personnel molecular. "Imaging" the network. Keeping records of ongoing attacks. Do not Use compromised systems to communicate. "Hack back" or intrud			
Identify mission critical data and assets (<i>i.e.</i> , your "Crown Jewels") and institute tiered security measures to appropriately protect those assets. Create an actionable incident response plan. Develop relationships with relevant law enforcement and other agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident. Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Have procedures in place that will permit lawful network monitoring. Ensure legal counsel is familiar with legal issues associated with cyber incidents. Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan. During a Cyber Attack or Intrusion Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch. Minimize continuing damage consistent with your cyber incident response plan. Collect and preserve data related to the incident hyperiate management and personnel systems to communicate. Imaging" the network. Keeping records of ongoing attacks. Consistent with your incident response plan. During a Cyber Attack or Intrusion Make an initial assessment of the scope and nature of the incident personnel policies	Review and adopt risk management practices found in guidance such as the National		
tiered security measures to appropriately protect those assets. Test the plan by conducting exercises. Create an actionable incident response plan. Test the plan by conducting exercises. Keep the plan up-to-date to reflect changes in personnel and structure. Exercises. Develop relationships with relevant law enforcement and other agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident. Image: Comparison of the comparincident records. Co			
Create an actionable incident response plan. Test the plan by conducting exercises. Evelop relationships with relevant law enforcement and other agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident. Keep the plan up-to-date to reflect changes in personnel and structure. Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Have procedures in place that will permit lawful network monitoring. Ensure legal counsel is familiar with legal issues associated with cyber incidents. Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan. Imaging? During a Cyber Attack or Intrusion "Imaging?" the network. Make an initial assessment of the scope and nature of the incident particularly whether it is a malicious act or a technological glitch. "Imaging?" the network. Collect and preserve data related to the incident by "Imaging?" the network. Imaging?" the network. Consistent with your incident response plan, notify Use compromised systems to communicate. Imaging?" the network. Department of Homeland Security. Other possible victims. Department of Homeland Security. Imaging?" the network. Consistent with your incident response plan, not	Identify mission critical data and assets (<i>i.e.</i> , your "Crown Jewels") and institute		
Create an actionable incident response plan. Keep the plan up-to-date to reflect changes in personnel and structure. Develop relationships with relevant law enforcement and other agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident. Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable). Image: Consume that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Image: Consume that will permit lawful network monitoring. Have procedures in place that will permit lawful network monitoring. Image: Consume that will permit lawful network monitoring. Ensure legal counsel is familiar with legal issues associated with cyber incidents. Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan. During a Cyber Attack or Intrusion Imaging'' the network. Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch. Minimize continuing damage consistent with your cyber incident response plan. Collect and preserve data related to the incident by "Imaging" the network. Kceping records of ongoing attacks. Image: Consistent with your incident response plan, notify Do not Use compromised systems to communicate. "Hack back" or intrude upon ano			
plan. Keep the plan up-to-date to reflect changes in personnel and structure. Develop relationships with relevant law enforcement and other agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident. Image: Comparison of Comparison o	1		
Develop relationships with relevant law enforcement and other agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident. Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Have procedures in place that will permit lawful network monitoring. Ensure legal counsel is familiar with legal issues associated with cyber incidents. Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan. During a Cyber Attack or Intrusion Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch. Minimize continuing damage consistent with your cyber incident response plan. Collect and preserve data related to the incident by It is incident response plan, notify During a Cyber Attack or Intrusion Law enforcement. Department of Homeland Security. Other possible victims. Data preserve data related to the incident seponse Appropriate management and personnel within the victim organization. Law enforcement. Department of H			
counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident.Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable).Image: State and Stat	-		
may need in the event of an incident. Image in the event of an incident. Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable). Image incident (or ensure that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Image incident (or ensure that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Image incident (or ensure that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Image incident (or ensure that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Image incident (or ensure that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Image incident (or ensure that it is easily obtainable). Institute basic cyber Attack or Intrusion Imaging" the network. Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch. Imaging" the network. Minimize continuing damage consistent with your cyber incident response plan. Imaging" the network. Imaging" the network. Collect and preserve data related to the incident by Imaging" the network. Imaging" the network. Imaging" the network. Consistent with your incident response plan. </td <td colspan="2"></td>			
Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Have procedures in place that will permit lawful network monitoring. Ensure legal counsel is familiar with legal issues associated with cyber incidents. Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan. Institute basic cyber Attack or Intrusion During a Cyber Attack or Intrusion Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch. Minimize continuing damage consistent with your cyber incident response plan. "Imaging" the network. Collect and preserve data related to the incident by "Imaging" the network. Keeping records of ongoing attacks. Keeping records of ongoing attacks. Consistent with your incident response plan, notify Use compromised systems to communicate. Do not Use compromised systems to communicate. "Hack back" or intrude upon another network. "Hack back" or intrude upon another network. After Recovering from a Cyber Attack or Intrusion Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network. Conduct a post-incident review to identify deficiencies in planning and execution of			
is easily obtainable). Institute basic cybersecurity procedures, such as a patch management program. Have procedures in place that will permit lawful network monitoring. Ensure legal counsel is familiar with legal issues associated with cyber incidents. Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan. During a Cyber Attack or Intrusion Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch. Minimize continuing damage consistent with your cyber incident response plan. Collect and preserve data related to the incident by			
Institute basic cybersecurity procedures, such as a patch management program.Have procedures in place that will permit lawful network monitoring.Ensure legal counsel is familiar with legal issues associated with cyber incidents.Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan.During a Cyber Attack or IntrusionMake an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch.Minimize continuing damage consistent with your cyber incident response plan.Collect and preserve data related to the incident byKeeping all logs, notes, and other records.Keeping all logs, notes, and other records.Plan, notifyDo notUse compromised systems to communicate.Do notAfter Recovering from a Cyber Attack or IntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regimed control of your network.Conduct a post-incident review to identify deficiencies in planning and execution of			
Have procedures in place that will permit lawful network monitoring.Ensure legal counsel is familiar with legal issues associated with cyber incidents.Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan.During a Cyber Attack or IntrusionMake an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch.Minimize continuing damage consistent with your cyber incident response plan.Collect and preserve data related to the incident byCollect and preserve data related to the incident byMake an initial assessment of the scope and nature of of ongoing attacks.Consistent with your incident response plan, notifyDo notDo notDo notUse compromised systems to communicate. "Hack back" or intrude upon another network.After Recovering from a Cyber Attack or IntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.			
Ensure legal counsel is familiar with legal issues associated with cyber incidents. Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan. During a Cyber Attack or Intrusion Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch. Minimize continuing damage consistent with your cyber incident response plan. Collect and preserve data related to the incident by Keeping all logs, notes, and other records. Keeping records of ongoing attacks. Consistent with your incident response plan, notify Do not Use compromised systems to communicate. "Hack back" or intrude upon another network. After Recovering from a Cyber Attack or Intrusion Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.			
Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan. Image: Construct on the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch. Minimize continuing damage consistent with your cyber incident response plan. Imaging" the network. Collect and preserve data related to the incident by "Imaging" the network. Keeping all logs, notes, and other records. Keeping records of ongoing attacks. Consistent with your incident response plan, notify Law enforcement. Department of Homeland Security. Other possible victims. Do not Use compromised systems to communicate. "Hack back" or intrude upon another network. "Hack back" or intrude upon another network. After Recovering from a Cyber Attack or Intrusion Intrusion Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network. Conduct a post-incident review to identify deficiencies in planning and execution of			
its incident response plan. During a Cyber Attack or Intrusion Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch. Minimize continuing damage consistent with your cyber incident response plan. Collect and preserve data related to the incident by "Imaging" the network. Keeping all logs, notes, and other records. Keeping records of ongoing attacks. Consistent with your incident response plan, notify Appropriate management and personnel within the victim organization. Law enforcement. Department of Homeland Security. Other possible victims. Other possible victims. Do not Use compromised systems to communicate. "Hack back" or intrude upon another network. "Hack back" or intrude upon another network. After Recovering from a Cyber Attack or Intrusion Intrusion Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network. Conduct a post-incident review to identify deficiencies in planning and execution of			
During a Cyber Attack or IntrusionMake an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch.Minimize continuing damage consistent with your cyber incident response plan.Collect and preserve data related to the incident by"Imaging" the network.Keeping all logs, notes, and other records.Keeping records of ongoing attacks.Consistent with your incident response plan, notifyAppropriate management and personnel within the victim organization.Law enforcement.Department of Homeland Security.Other possible victims.Do not"Hack back" or intrude upon another network.After Recovering from a Cyber Attack or IntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.Conduct a post-incident review to identify deficiencies in planning and execution of			
Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch.Interfact the incident is a malicious act or a technological glitch.Minimize continuing damage consistent with your cyber incident response plan.Integration of the incident response plan.Collect and preserve data related to the incident byIntegring" the network.Keeping all logs, notes, and other records.Keeping records of ongoing attacks.Consistent with your incident response plan, notifyAppropriate management and personnel within the victim organization.Law enforcement.Law enforcement.Department of Homeland Security.Other possible victims.Do notUse compromised systems to communicate."Hack back" or intrude upon another network."Hack back" or intrude upon another network.After Recovering from a Cyber Attack or IntrusionIntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.Conduct a post-incident review to identify deficiencies in planning and execution of			
whether it is a malicious act or a technological glitch.Imaginal glitch.Minimize continuing damage consistent with your cyber incident response plan.Collect and preserve data related to "Imaginal" the network.Imaginal" the network.Collect and preserve data related to the incident by"Imaginal" the network.Imaginal" the network.Keeping all logs, notes, and other records.Keeping records of ongoing attacks.Imaginal" the victim organization.Consistent with your incident response plan, notifyAppropriate management and personnel within the victim organization.Imaginal" the victim organization.Law enforcement.Department of Homeland Security.Imaginal" the possible victims.Do notUse compromised systems to communicate.Mack back" or intrude upon another network.Imaginal" the work.After Recovering from a Cyber Attack or IntrusionImaginal use sure the intruder has been expelled and you have regained control of your network.Imaginal use sure the intruder has been expelled and you have regained control of your network.			
Minimize continuing damage consistent with your cyber incident response plan.Imaging" the network.Collect and preserve data related to the incident by"Imaging" the network.Imaging" the network.Keeping all logs, notes, and other records.Keeping records of ongoing attacks.Imaging" the network.Consistent with your incident response plan, notifyAppropriate management and personnel within the victim organization.Imaging" the network.Law enforcement.Department of Homeland Security.Imaging" the possible victims.ImagingDo notUse compromised systems to communicate.Imaging" the work.ImagingAfter Recovering from a Cyber AttackIntrusionImagingImagingContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.ImagingImagingConduct a post-incident review to identify deficiencies in planning and execution ofImagingImagingImagingConduct a post-incident review to identify deficiencies in planning and execution ofImagingImagingImagingImaging in the planning and execution ofImaging in the planning and execution ofImagingImagingImaging in the post-incident review to identify deficiencies in planning and execution ofImagingImagingImagingImaging in the planning and execution ofImaging in the planningImagingImagingImagingImaging in the planning and execution ofImaging in the planningImaging in the planningImagingImaging in the plann			
Collect and preserve data related to the incident by"Imaging" the network.Keeping all logs, notes, and other records.Keeping records of ongoing attacks.Consistent with your incident response plan, notifyAppropriate management and personnel within the victim organization. Law enforcement.Department of Homeland Security.Do notUse compromised systems to communicate."Hack back" or intrude upon another network.After Recovering from a Cyber Attack or IntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.Conduct a post-incident review to identify deficiencies in planning and execution of			
the incident byKeeping all logs, notes, and other records.Keeping records of ongoing attacks.Consistent with your incident response plan, notifyAppropriate management and personnel within the victim organization. Law enforcement.Department of Homeland Security.Department of Homeland Security.Do notUse compromised systems to communicate. "Hack back" or intrude upon another network.After Recovering from a Cyber Attack or IntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.Conduct a post-incident review to identify deficiencies in planning and execution of			
Recepting an logs, notes, and other records.Keeping records of ongoing attacks.Consistent with your incident response plan, notifyAppropriate management and personnel within the victim organization.Law enforcement.Law enforcement.Department of Homeland Security.Other possible victims.Do notUse compromised systems to communicate."Hack back" or intrude upon another network."Hack back" or intrude upon another network.After Recovering from a Cyber Attack or IntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.Conduct a post-incident review to identify deficiencies in planning and execution of	-		
Consistent with your incident response plan, notifyAppropriate management and personnel within the victim organization. Law enforcement.Department of Homeland Security.Department of Homeland Security.Do notUse compromised systems to communicate."Hack back" or intrude upon another network.After Recovering from a Cyber Attack or IntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.Conduct a post-incident review to identify deficiencies in planning and execution of		Keeping all logs, notes, and other records.	
plan, notifywithin the victim organization.Law enforcement.Law enforcement.Department of Homeland Security.Other possible victims.Do notUse compromised systems to communicate."Hack back" or intrude upon another network."Hack back" or intrude upon another network.After Recovering from a Cyber Attack or IntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.Conduct a post-incident review to identify deficiencies in planning and execution of		Keeping records of ongoing attacks.	
Law enforcement.Department of Homeland Security.Other possible victims.Do notUse compromised systems to communicate."Hack back" or intrude upon another network.After Recovering from a Cyber Attack or IntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.Conduct a post-incident review to identify deficiencies in planning and execution of	Consistent with your incident response	Appropriate management and personnel	
Department of Homeland Security.Department of Homeland Security.Other possible victims.Do notUse compromised systems to communicate."Hack back" or intrude upon another network.After Recovering from a Cyber Attack or IntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.Conduct a post-incident review to identify deficiencies in planning and execution of	plan, notify	within the victim organization.	
Other possible victims.Do notUse compromised systems to communicate."Hack back" or intrude upon another network.After Recovering from a Cyber Attack or IntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.Conduct a post-incident review to identify deficiencies in planning and execution of		Law enforcement.	
Do not Use compromised systems to communicate. "Hack back" or intrude upon another network. After Recovering from a Cyber Attack or Intrusion Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network. Conduct a post-incident review to identify deficiencies in planning and execution of		Department of Homeland Security.	
Do not Use compromised systems to communicate. "Hack back" or intrude upon another network. After Recovering from a Cyber Attack or Intrusion Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network. Conduct a post-incident review to identify deficiencies in planning and execution of		Other possible victims.	
"Hack back" or intrude upon another network.After Recovering from a Cyber Attack or IntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.Conduct a post-incident review to identify deficiencies in planning and execution of	Do not		
network. After Recovering from a Cyber Attack or Intrusion Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network. Conduct a post-incident review to identify deficiencies in planning and execution of			
After Recovering from a Cyber Attack or IntrusionIntrusionContinue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.IntrusionConduct a post-incident review to identify deficiencies in planning and execution ofIntrusion		-	
Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network. Conduct a post-incident review to identify deficiencies in planning and execution of			
intruder has been expelled and you have regained control of your network.Conduct a post-incident review to identify deficiencies in planning and execution of			
Conduct a post-incident review to identify deficiencies in planning and execution of			