Cyber Incident Preparedness Checklist		
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.e.*, 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.	
	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).		
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 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.	
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 your incident response plan.		