COMPROMISED COMPUTER NETWORK INCIDENT WORKSHEET

1. Organization Information	
Organization Name:	
Organization Address:	
Name of Person Reporting:	
Name of Network Administrator:	
Name of CISO:	
Name of CIO/Executive Level Decision Maker:	
Date of Report:	

2. What type of network compromise occurred? (please select all that apply)			
☐ Reconnaissance	☐ Malware	☐ Data Exfiltration	☐ Other (please describe)

3. What equipment has been impacted?	
Type:	
Manufacturer:	
Model Number:	
Serial Number:	

4. What operating system(s) was (were) installed on the equipment at the time of the intrusion?					
OS:		OS:		OS:	
Version:		Version:		Version:	
Time Zone:		Time Zone:		Time Zone:	

5. Are/Were software patches regularly installed?		
☐ Yes	☐ No	☐ Unknown

6. Does your network utilize any virtual machines or cloud services?		
☐ Yes – If so, which ones?	☐ No	☐ Unknown

7. Is remote connectivity enabled on your network?		
☐ Yes – Please select all that apply	☐ No	☐ Unknown
☐ SSH – Please provide which version:		
☐ Telnet – Please provide which version:		
☐ RDP – Please provide which version:		
☐ VPN – Please provide which version:		
☐ Other – Please provide type and version:		

8. Does your organization use any web services?	
☐ Yes – Please list all services in use	☐ No

9. Please list all domain names associated with your network.

10. Please provide your server's DHCP address.

11. Does your organization maintain DCHP logs?		
☐ Yes – If so, where?	☐ No	☐ Unknown

12. Does your organization maintain web server logs?		
☐ Yes – If so, where?	☐ No	☐ Unknown

13. Please provide your organization's network DNS address.		
Is it internal or external to your organization?		
☐ Internal	☐ External	☐ Unknown

14. Please list the range of your organization's IP addresses.
Of these, how many does your organization own and/or use?

15. Does your organization maintain any data backups?		
☐ Yes – If so, where?	☐ No	☐ Unknown

16. What terminal services are/were running on the impacted equipment?

17. What ports are/were enabled on the impacted equipment?

18. Does your organization own or operate any Wi-Fi access points?		
☐ Yes	☐ No	☐ Unknown
If so, are they active or passive?		
☐ Active	☐ Passive	

19. Do you suspect the unauthorized intrusion on your network to be the result of a current or former employee?	
☐ Yes	☐ No

20. Are your employees informed of the limits of their acceptable use and privileges on your network?		
☐ Yes	☐ No	☐ Unknown

21. Are employees given any instructions related to the cessation of their network use and privileges when they leave employment or are terminated?		
☐ Yes	☐ No	☐ Unknown

22. Has your organization taken any steps to mitigate the impact of the intrusion?		
☐ Yes – if so, please describe	☐ No	☐ Unknown

23. To the best of your ability, please quantify your estimated financial loss as a result of this incident.*	
Equipment Loss:	
Equipment Repairs:	
New Equipment:	
New Software:	
Employee Overtime:	
Consulting Costs:	
Reputation Degradation:	
Customer/Business Loss:	

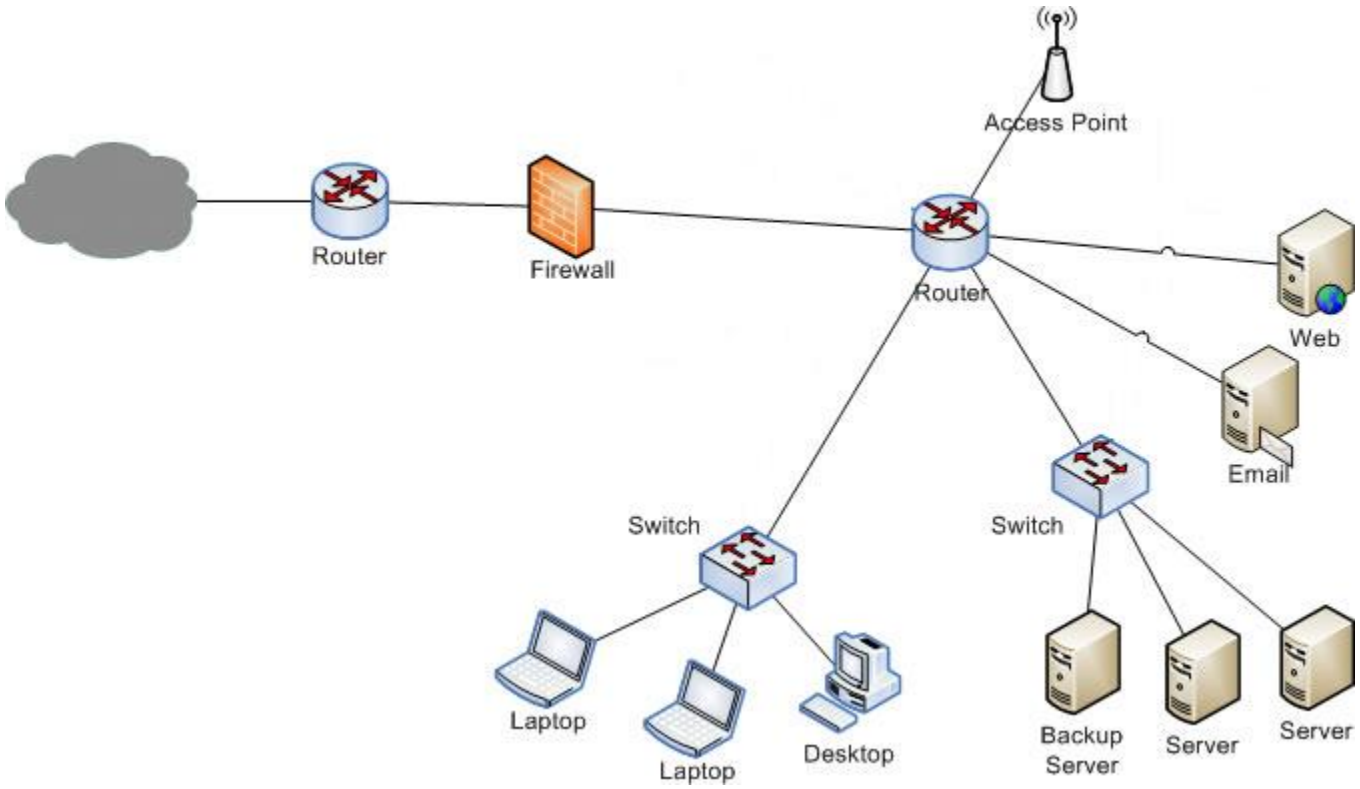
**** We understand that an intrusion event can, regrettably, result in an array of costs and financial losses to your company. We also understand that it can sometimes take weeks or months to determine the full scope of those costs/losses. We seek that information, as you are able to provide it, because it is relevant to a criminal investigation. It is particularly important in determining the sentence that we will seek, assuming a successful prosecution and conviction.***

24. Please provide a diagram and narrative description of your network architecture and configurations that lists the location (city/state/country) of all servers and users on the network (see example).

25. Please provide the relevant usernames and passwords for all equipment impacted by the intrusion.

RESOURCES

1. Example diagram of network architecture and configurations.



2. Points of Contact	
Federal Bureau of Investigation, Seattle – Cyber Task Force	206-622-0460 seattle.ctf@ic.fbi.gov
United States Attorney's Office, Western District of Washington	206-553-7970
United States Attorney's Office, Eastern District of Washington	509-353-2767
Infragard	https://www.infragard.org
Internet Crime Complaint Center (IC3)	http://www.ic3.gov

NOTICE: This worksheet is intended to provide a baseline for reporting a computer network incident to the FBI. It is not exhaustive; however, it attempts to address the core elements of information that are most valuable to investigators in light of legal precedent and commonly used technologies. This document is not legal advice, and any best practices developed from it do not necessarily guarantee successful detection, investigation, and prosecution of adversaries.