



Prior to First Response

Preserving Your Options in the event of a
Malicious Cyber Incident

Law Enforcement Workgroup



STOP | THINK | CONNECT™



“Criminals are attacking small and medium-sized companies that don't have the inclination, money or expertise to prevent cybercrime.”

- Reuters Nov 24, 2009 (Bartz & Finkle)





What Options?

- Initiating an adverse Personnel Action
 - Or defending a wrongful termination or harassment action.
- Complaining to Regulators
- Bringing a lawsuit
- Referring to Law Enforcement

- All require evidence!





Why Bother?

- Cost recovery and damages
- Effectively terminating a corrupt employee
- Revenge!
 - “Revenge is a dish best served cold.” Khan to Kirk in Star Trek II, The Wrath of Khan
- Good cyber-citizenship and domain leadership
- Avoid ending up on a cyber-mooch list
- California Civil Code section 1798.81.5





What Will This Cost?

- Hardware/Software
 - Image or retain hard drives from employees who leave under less than amicable circumstances or who had access to confidential data
 - Take offline or image and then restore from backup compromised servers
- Invest in strong backup technology to include offline storage of important computer and network logs.
- Invest in basic training in IT security for your IT staff or retain an IT consultant with security skills who can be available in an emergency.
- Create acceptable computer use policies and procedures and disseminate to all employees
- Optional: IT Security Audit; system upgrades; incident response planning.





What do I do now?

- Have IT staff enable computer and network logging
- Have logs stored offline
- Treat every cyber-incident as potentially malicious until it is determined that it is not
- Regularly confirm compliance with policies and procedures
- Consistently backup data and test that backup worked
- Train end-users
- Plan for incident response





Securing Our eCITY.
an ESET led initiative

Prevention

How to avoid a cyber incident



STOP | THINK | CONNECT™



5-Step Incident Prevention Plan

1. Education (situational awareness)
2. Implement network and end-point security
3. Restrict access to resources and information to those that actually need it
4. Schedule backups or imaging of systems (and test backups occasionally)
5. Identify where, and what, information resides on your network.





Securing Our eCITY.
an ESET led initiative

First Response

Your Organization is involved in a Cyber Incident

What Next?



STOP | THINK | CONNECT™



First Things First

- Don't panic
- Gain “situational awareness”
- Notification

Note: fast responses are warranted for active data exfiltration such as customer data or IP





What do I do now?

- Preserve the original compromised system's hard drives if possible, and provide documentation on anything that has been done to the system since the discovery of the incident.
- Provide copies of any network diagrams or system documentation showing the environment in which the system operated.
- Identify and provide copies of any externally generated log files, such as intrusion detection system or firewall logs.
- Consider monitoring the system's network connections prior to taking it offline. Other compromised systems or suspect Internet protocol addresses can frequently be identified.





What Else Can I Do Now?

- Your IT staff or a trusted consultant should document basic system information related to the compromised system:
 - IP Address of compromised system
 - Hostname or NetBios Name
 - Operating System
 - Use of DHCP or static IP address assignment
 - Date/time of incident response
 - Network Topology
 - Applications/Processes running
 - Impact - cost to restore/examine/investigate
 - Policies and procedures - i.e. permissions





Who do I call?

- We don't care! Take your pick:
 - Feds (FBI, USSS, DCIS (defense contractors))
 - Locals: CATCH (High Tech Crime Task Force)
 - Your trusted IT security consultant
 - Your lawyer
 - Your bartender
- Notify law enforcement as soon as practical so that available leads can be followed up in a timely manner





Securing Our eCITY.
an ESET led initiative

Questions?



STOP | THINK | CONNECT™