Security Event:

is an observable change in normal behaviour to I.T. systems, environments, processes, workflow or a person

Western UNIVERSITY · CANADA

Security Incident:

is an event that negatively effects the confidentiality, integrity and/or availability of any Western system

If at any point in this continuum your are not certain, then treat it as a security incident

EXAMPLES	EXAMPLES	EXAMPLES	EXAMPLES
• An employee receives a phishing or suspicious email	• An employee opens a phishing or suspicious email	• The employee replies to the phishing email with confidential information	• Employee's account(s) has been breached
• A computer system crashes	• A computer system, after a crash is behaving oddly	• A computer's event logs indicate unauthorized privilege use	• Evidence is found to indicate that access has been used in a manner that violates a Western policy.
• An employee reports that their desktop may have a virus	• Multiple viruses are found on the desktop	• Virus is a worm and is propagating itself to other desktops	• A virus outbreak has been confirmed on multiple systems
• A user reports they can not access a certain service	• Multiple users have reported they can not access a certain service	• Incident responder can not login to the service in question	• An active DoS attack has been confirmed
• A system administrator believes that a system was breached	• A system administrator has a log entry showing suspicious activity	• Correlated data shows many active attempts to compromise the system	• Unauthorized access to a system has been confirmed
• An employee receives a phishing or suspicious email	• An employee opens a phishing or suspicious email and clicks on a link	• An employee's desktop receives a pop-up claiming to be Ransomware	• Ransomware has been identified on more than one system

Actions to be taken

Take remediation and investigative steps	Contact the appropriate escalation point and take steps to eliminate any further risk	Incident responder should notify the Western Incident Response Team and take steps to contain or eliminate any further risk	Activate the Western Incident Response Plan