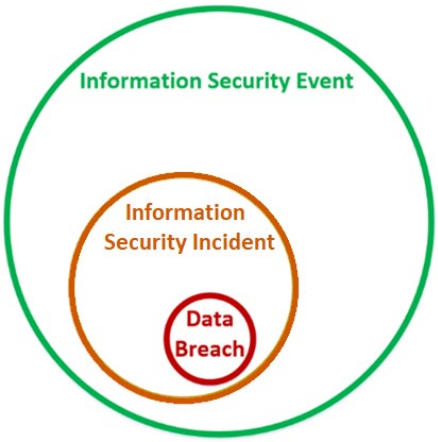
Example Information Security Events which May or May Not be a Data Breach

Information Security Event Definition:
Any observable occurrence in the operations of a network or information technology service, system or data indicating that a security policy may have been violated or a security safeguard may have failed.



Information Security Incident Definition:
An information security **event** where it is alleged or suspected that unauthorized access, use, modification, or disclosure of printed, electronic, audio or visual non-public institutional data to an unauthorized individual or entity may have occurred.

Information Data Breach Definition:
An information security **incident** validated by the Data Incident Response Team where unauthorized access, use, modification, or disclosure of information has occurred.

Examples

1) **Virus**
   Security Event: User states their computer is not working properly and they cannot access some files
   Security Incident: Help Desk finds a virus on that system.
   Non-Breach examples: Destructive virus that only serves to cause chaos
   Potential Data Breach examples: Trojan Horse Virus which is giving control to a hacker and institutional data has possibly been accessed. This would lead to further investigation which could identify a breach of institutional data.
2) **Ransomware**
   Security Event: A staff person reports their files cannot be opened and they have a notice on their screen.
   Security Incident: A Ransomware virus is on the user's computer and has a notification that files are encrypted and bitcoin payment is required to decrypt
   Non-Breach example: The computer had no institutional data and no university servers were affected.
   Potential Breach examples: Institutional data on file servers were encrypted by the Ransomware. This would lead to further investigation which could identify a breach of institutional data.
3) **Compromised web site**
   Security Event: Donor reports that the giveto.osu.edu web site's content has been changed to something obscene.
   Security Incident: The network team notices files have been changed on the web server.
   Non-Breach example: Only files changed are those which show on the web site. No other files show access.
   Potential Data Breach examples: The network team notices the server has been compromised and is hosting an illegitimate web site and institutional data has possibly been accessed. This would lead to further investigation which could identify a breach of institutional data.
4) **Slow Server**
   Security Event: User reports the file server is running very slow.
   Security Incident: The network team notices a rogue active network port scan
   Non-Breach example: A user's computer has been compromised and is being used to scan servers for vulnerabilities for future attacks.
   Potential Breach examples: That user's compromised computer has institutional data on their computer. This would lead to further investigation which could identify a breach of institutional data.