# Six Tips for Managing the First 24-48 Hours of a Data Incident

When an organization experiences a compromise of computerized personal information, time is of the essence. Legal guidance from knowledgeable counsel on applicable state and federal data privacy and security laws, a privileged computer forensics examination, notification of law enforcement and government agencies, and preservation of evidence are among the key action items. During the initial stage of an incident response, legal counsel will advise you to take a number of response and remediation steps, depending on the type of incident, which may include the following:

1. ***Assemble your incident response team (IRT) members.*** The IRT members may vary depending on the type of incident but usually include legal counsel (internal and/or external), IT, information security, HR, operations, management, risk management, communications, and investor relations. An outside forensic expert may also be required depending on the incident. Advise the IRT to refer to the incident as a "data security incident," rather than a "breach," until a determination has been made that the incident constitutes a "breach" under applicable law.

    - Ensure your legal counsel is part of your IRT to establish a privileged communications channel and to advise on legal and contractual notification obligations and whether to notify law enforcement and/or regulators.

2. ***Notify insurance carriers to secure coverage.*** Call your insurance broker to request notification per the applicable insurance policy. Some insurance policies may cover response and remediation costs related to privacy and data security incidents, including legal counsel fees, forensics, breach notification, credit and ID monitoring, government investigations, fines and penalties.

3. ***Isolate the infected system.*** Remove the infected system from all networks, and disable the computer's wireless, Bluetooth, and any other potential networking capabilities. Ensure all shared and networked drives are disconnected, whether wired or wireless.



WYATT

4. ***Preserve forensics evidence.*** Segregate and preserve firewalls, system logs and intrusion detection logs of the affected computers, servers and VPNs that support email, internal networks, client networks and websites. Consult with an expert before powering-off the infected computer(s) as this could impact available forensic evidence.

5. ***Secure your network and all connected devices and equipment.*** Change security credentials and passwords of all authorized users to affected computers and systems.

6. ***Document the events leading up to and immediately following the discovery of the incident under the direction of legal counsel.*** Document a) the date and time the incident was discovered; b) how it was discovered; c) the date and time it was reported; d) name(s) of individuals involved in the chain of discovery and reporting; e) the type of encryption on the affected devices and data files; and f) description of personal information on affected computers. This information may be essential to investigating the event by forensic experts, government and law enforcement as well as helping you comply with legal and contractual obligations triggered by the event.

## Wyatt's Data Incident Response Team is available to help:


**Kathie McDonald-McClure, CHC**
*Partner & Chair,*
*Data Privacy & Security Team*
502.562.7526
kmcclure@wyattfirm.com

**Margaret Levi**
Counsel, Lexington
859.288.7469
mlevi@wyattfirm.com

**Carole Christian**
*Partner, Louisville*
502.562.7588
cchristian@wyattfirm.com

**Emily Lineweaver**
Associate, Louisville
502.562.7246
elineweaver@wyattfirm.com

**Martha Ziskind**
*Counsel, Louisville*
502.562.7310
mziskind@wyattfirm.com

**Jennifer Wintergerst**
*Partner, Louisville*
502.562.7330
jwintergerst@wyattfirm.com

**Dan Soldato**
*Partner, Lexington* 859.288.7631
dsoldato@wyattfirm.com

**Mark Vorder-Bruegge**
*Partner, Memphis*
901.537.1069
mvb@wyattfirm.com

**Vonda Motsinger**
*Paralegal, Louisville*
502.562.7169
vmotsinger@wyattfirm.com


For more information on our Data, Privacy and Security Team, please visit wyattfirm.com/services-detail/Privacy-&-Information-Security.

The Wyatt "HITECH Law" blog tracks legal developments in the privacy and security of confidential patient, consumer and business information across multiple industry sectors.

Visit wyatthitechlaw.com to learn more.

WYATT