nilan johnson lewis PA

Detailed Breach / Security Incident Checklist

In the event of a security incident or potential compromise of data, assess as follows:

- **Has a security incident been identified?**
  - Document who discovered and how was it was discovered.
  - Is it immediately apparent that a breach (i.e., unauthorized access or disclosure) has been confirmed?
    - If yes, the server/system affected should be immediately secured (to ensure not changed) and not accessed pending review by a forensic examiner.
    - If no, has the server/system on which the security incident was identified been removed from Internet access and/or any other user access?
  - Have the system files related to the affected software, email systems, or other been preserved?

- **Has the organization's data privacy officer and/or security officer been informed?**
  - If the organization does not have a data privacy officer, an executive needs to assume this responsibility.
  - Have affected employees, customers, etc. been instructed to not access accounts which may modify the affected servers/systems? Have such accounts been globally locked from such access?

- **Assuming that a forensic expert is retained, ensure that the forensic review:**
  - Audits the systems to determine date of first access related to the security incident;
  - Assess the extent of access? Is there any indication of use of data?
  - Is it clear that data on individuals has been accessed or used by unauthorized persons (i.e. a breach)? If yes, then:
    - Have the affected individuals, if any, been identified?
    - Has the nature of the data affected been identified?
    - Does it include personally sensitive information (i.e., SSN, driver's license, credit card information)?
    - Does it include regulated data (i.e. protected health information, credit card or banking information)?
    - Is the affected individual from a strictly regulated regime (i.e., EU)?

- **Once the forensic review and/or root cause analysis has been completed, assess:**
  - Are existing security protocols sufficient to have precluded the incident?
  - Is the training of such policies sufficient?
  - Did an employee trigger the incident? If yes, had that employee been trained? Followed protocol? If the employee had violated security policies, was such violation negligent? Intentional? Does the organization believe that the employee's access to systems needs to be stopped pending an investigation?
  - Did a third party (i.e., subcontractor or vendor) trigger the incident? If yes, did the contractual obligations between the organization and the third party preclude such action (or inaction)? If yes, was the violation of that obligation negligent? Intentional? If yes, does access need to be immediately terminated?

- **Once a breach has been confirmed, coordinate with legal as to the breach notification and timing obligations.**

Based on the answers to the above inquiries, legal considerations include:

- Does an employment lawyer need to be involved?
- Have any affected customer, vendor or other contracts been reviewed by legal for additional breach response and/or notice obligations?
- Does a regulator need to be informed?
- Does the affected individual have to be informed? Timing of such notice?
- Does the external computer forensic examiner need to draft a formal report?

Kate Andresen
612.305.7730
kandresen@nilanjohnson.com