STINSON LEONARD STREET

Data Security

INCIDENT RESPONSE CHECKLIST

IDENTIFICATION

The identification process should be thorough enough to understand the event and complete the response plan but not so thorough as to delay more detailed action items.

☐ Determine the nature and characteristics of the incident

- Vulnerability or actual breach?
    - Breach = Access + Acquisition
- If a breach, did it involve personal information, health information, financial information, intellectual property or other proprietary information?
- When did the incident occur and were there any warning signs?

☐ Identify the parties involved

- If personal information can we be sure about the scope of individuals affected?
- Are there any other third parties affected?
- Do data subjects reside outside of the US

☐ Identify the response team

- Legal/Risk
- Technology
- Communications
- Leadership/Governance

☐ Identify the laws and regulations implicated

- Specific privacy laws (COPPA, GLB, FCRA)
- FTC and General Privacy Implications
- Data Breach Notification laws
- Securities law disclosures

☐ Engage external and internal resources to stop the threat

☐ Establish process to record findings

☐ Evaluate IP involved in the incident

RESPONSE PLANNING

Ideally, the company has a detailed response plan already in place and this becomes a process of moving through the steps in the plan.

☐ Establish timeline for updates, reports and team meetings

☐ Determine need for outside consultants

- Consider whether to contract with a data security vendor through outside counsel to try to preserve privilege
- Consider an outside communications firm.
- Obtain service agreements and NDA's from consultants.

☐ Establish Information Flow to Board and Shareholders

- Review threshold for Board level reporting
- Define schedule for Board reports

☐ Determine need to notify key internal stakeholders not on the immediate response team

- Billing and accounts (need to suspend billing)
- Human resources
- Procurement and vendor relations

DATA BREACH NOTIFICATION COMPLIANCE

☐ Confirm actual breach and SEC disclosure requirements

☐ Compile list of implicated states and state statutes

☐ Establish timeline for notice based on state statutes

☐ Investigate risk of harm under applicable state standards

☐ Evaluate delayed enforcement to meet law enforcement needs

☐ Determine whether notice to Attorney General is required

☐ Determine whether substitute notice is permitted

INVESTIGATION STEPS

☐ Identify compromised systems, connectivity of compromised systems, and scope of breach

☐ Identify information compromised and persons affected

- Catalogue specific data elements
- Catalogue applicable jurisdiction
- Evaluate risk of identity theft if PII is involved

☐ Identify source or suspects involved

- Identify internal individual involved
- Identify third party vendors involved
- Collect and review agreements with third party vendors involved
- Evaluate liability limitations with third parties
- Evaluate indemnity obligations of third parties

☐ Identify communications with legal as "Privileged and Confidential Attorney-Client Communication" and consider with vendors engaged by counsel.

- Specific privacy laws (COPPA, GLB, FCRA, EU Data Directive, FTC Act, CalOppa, GDPR)
- FTC and General Privacy Implications
- Data Breach Notification laws

DAMAGE CONTROL

☐ Evaluate insurance coverage and notify carrier

☐ Determine any securities law disclosures

☐ Engage technology vendor or internal staff to remedy the compromise

☐ Engage internal and external communications team

☐ Conduct vulnerability testing and assessment post remediation

☐ Review customer and other third party vendor contracts to determine disclosure requirements

☐ Determine whether remediation efforts require disclosures going forward

COLLECTION OF EVIDENCE

☐ Security incident response form

☐ IT forensic evidence (e.g. reports, logs, audits).

☐ Law enforcement agency and police reports

☐ Legal counsel guidance

CONSIDER CONTACTING LAW ENFORCEMENT OFFICIALS

☐ Verify that the event constitutes a crime that is reportable

☐ Determine appropriate government agency. FBI has agents dedicated to cyber security. Consider DHS.

☐ In cooperation with local enforcement officials, determine the need to involve other external law enforcement.

☐ Obtain the name of law enforcement contact to provide upon victim request

☐ IT forensic evidence (e.g. reports, logs, audits).

☐ Law enforcement agency and police reports

☐ Legal counsel guidance

ATTORNEY CONTACTS

Steve Cosentino, Partner
Data Security Incident Response Team
steve.cosentino@stinson.com
816.691.2450

STINSON LEONARD STREET