## **Sample Incident Response Manual**

**INCIDENT AND BREACH RESPONSE PLAN**

**Overview**

1. **Definitions**
2. **The Team**
3. **Reporting an Incident**
4. **The First 24 Hours**
5. **Notifying Law Enforcement**
6. **Next Steps**
7. **Notifying Data Breach Victims**
8. **Managing Communications**
9. **Review Response and Update Policies**
10. **Auditing Your Plan**
11. **Template Breach Notification Letter**
12. **NIST Checklist**

**I. DEFINITIONS**

**“Breach”** or **“Data Breach”** means an incident resulting in the unlawful and unauthorized access or acquisition of personal information that compromises the security, confidentiality, and integrity of that personal information.

**“Event”** means any observable occurrence in a system or network, such as a server receiving a request for a web page, a user sending an email message, or a firewall blocking an attempt to make a connection.

**“Incident”** means an event that violates an organization’s security policies and procedures.

**“Personal Information,”** is not universally defined in the U.S. In California, it means an individual’s first name or first initial and last name, plus one or more of the following: SSN, driver’s license, state ID, account number, credit card or debit card number combined with the security code, PIN, or password needed to access an account. State breach notification laws vary on the definition of personal information and legal counsel should be consulted regarding the precise definitions that may apply. Multiple state laws may apply to one data breach because jurisdiction depends on where the affected individuals reside.

**II. THE TEAM**

Assembling a complete team (Incident Response Team) comprised of strong, capable representatives will go a long way toward ensuring an efficiently executed response. Your Incident Response Team should include the following constituents, as applicable:

* **Incident Lead**
  + Determines when the full Incident Response Team needs to be activated in response to an incident;
  + Manages and coordinates DEALERSHIP’s overall response efforts and team, including establishing clear ownership of priority tasks;
  + Acts as an intermediary between execs and other team members to report on progress and problems;
  + Ensures proper documentation of incident response process and procedures.
* **Information Technology and Security**
  + Identifies top security risks that should be incorporated into written incident response plans;
  + Trains personnel in data breach response, including securing the premises, safely taking infected machines offline, and preserving evidence;
  + Works with forensics to identify the compromised data and deletes hacker tools without compromising evidence and progress.
* **Legal and Privacy**
  + Determines how to notify affected individuals, the media, law enforcement, government agencies and other third parties;
  + Establishes relationships with any necessary external legal counsel before a breach occurs;
  + Final sign-off on all written materials related to the incident.
* **Law Enforcement (depending on the severity of the breach)**
  + Looks for evidence that a crime has been committed.
* **Forensics**
  + Advise DEALERSHIP on how to stop data loss, secure evidence, and prevent further harm;
  + Preserve evidence and manage the chain of custody, minimizing the chance that evidence will be altered, destroyed, or rendered inadmissible in court.

**III. REPORTING AN INCIDENT**

Regardless of origin, all information security events, incidents and breaches must be funneled through IT, which can be contacted at [*INSERT CONTACT INFORMATION*]. It is the central point of contact before the Incident Response Team is engaged.

**IV. THE FIRST 24 HOURS**

Acting swiftly and strategically following a security incident can help you regain your security, preserve evidence, and protect your brand. Always collect, document and record as much information about the incident and your response efforts as possible, including conversations with law enforcement and legal counsel.

1. **Record the moment of discovery** – Also mark the date and time your response efforts begin, i.e. when someone on the Incident Response Team is alerted to the incident.
2. **Alert and activate everyone** – Include everyone on the Incident Response Team, including external resources, to begin executing your preparedness plan.
3. **Analyze** – The Incident Response Team will review the nature of the incident, including whether the incident is a breach, and the severity of the incident.
4. **Secure the premises** – Ensure the area where the incident occurred and surrounding areas are secure to help preserve evidence.
5. **Stop additional data loss** – Take affected machines offline, but do not turn them off or start probing into the computer until the forensics team arrives.
6. **Document everything** – Record who discovered the incident, who reported it, to whom it was reported, who else knows about it, what type of incident it was (i.e. phishing attack, malware attack), etc.
7. **Interview involved parties** – Speak with those involved with discovering the incident and anyone else who may know about it—then document the results.
8. **Review notification protocols** – Review those that touch on disseminating information about the incident for everyone involved in this early stage.
9. **Assess priorities and risks** – Include those based on what you know about the incident. If required, bring in a forensics firm to begin an in-depth investigation.
10. **Bring in a forensics firm** – Begin an in-depth investigation.
11. **Notify law enforcement** – Do this if needed, after consulting with legal counsel and upper management.

**V. NOTIFYING LAW ENFORCEMENT**

If there is reasonable evidence of a crime, rather than simply an event or occurrence that resulted in a security incident, you should notify law enforcement. A preliminary inquiry should include:

* Ruling out normal hardware or software failure.
* Developing a chronology of what happened.
* Auditing for any unusual activity during that time frame.
* Identifying any users or processes involved.
* Evaluating the motives of any actors.

**VI. NEXT STEPS**

After the first day, assess your progress to ensure your plan is on track. Then, continue with these steps:

1. **Identify the root cause** – Ensure your forensics team removes hacker tools, and address any other security gaps. Document when and how the incident was contained.
2. **Alert your external partners** – If there was a breach, notify your partners, including your insurance carrier, and include them in the incident response moving forward. If required, engage a data breach resolution vendor to handle notifications and set up a call center.
3. **Continue working with forensics** – Determine if any countermeasures, such as encryption, were enabled during the incident. Analyze all data sources to ascertain what information was compromised.
4. **Identify legal obligations** – Revisit state and federal regulations that apply and then determine all entities that need to be notified. Ensure all notifications occur within any mandated timeframes.
5. **Report to upper management** – Generate reports that include all the facts about the incident, as well as the steps and resources needed to resolve it. Create a high-level overview of priorities and progress, as well as problems and risks.
6. **Identify conflicting initiatives** – Determine if any upcoming business initiatives may interfere or clash with response efforts. Decide whether to postpone these efforts and for how long.
7. **Evaluate response and educate employees** – Once an incident is resolved, evaluate how effectively your company managed its response in order to make the necessary improvements to your preparedness plan. Taking time to reflect and make these adjustments will ensure a smoother response in the future. Use the incident as an opportunity to retrain employees not only in their specific response role when a security incident occurs, but also in their own security and privacy practices.

**VII. NOTIFYING DATA BREACH VICTIMS**

Not all breaches require a notification. When they do, it is your responsibility to determine the deadlines for notification according to state law. **Multiple state laws may apply to one data breach because jurisdiction depends on where the affected individuals reside, not where the business is located or where the breach occurred.** Typically, businesses have 60 days to notify affected individuals of a data breach when notification is required by law. Certain state laws and federal regulations shrink the timeline to 30 or 45 days. The countdown starts the moment a breach is discovered. Notification may be delayed if law enforcement believes it would interfere with an ongoing investigation.

California law requires a business or state agency to notify any California resident whose unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person. California’s data breach notification statute[[1]](#footnote-1) defines personal information as first name or first initial and last name, **plus**: Social Security number; driver's license or state identification card number; financial account, credit or debit card number, in combination with any required security or access code or password permitting access to a resident's financial account; medical or health insurance info; or info collected by automated license plate recognition systems. It also includes a username or email address, in combination with a password or security question and answer that would permit access to an online account. The statute does not apply to encrypted information so long as the encryption key was not or is not reasonably believed to have been acquired. Notification must be made in the most expedient time possible and without unreasonable delay consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

Some states mandate specific content for you to include in your notification letters. This can include toll-free numbers and addresses for the three major credit bureaus, the Federal Trade Commission and a state’s attorney general. As dictated by state law, a notification letter should include:

* Clear language, not industry jargon, that the average person could understand.
* A toll-free phone number for individuals wanting additional information.
* Details about the type of data lost and how it was lost, unless prohibited by law.
* Next steps to help affected individuals regain their security, such as signing up for a complimentary identity protection product.

Under California law, notice must be in “plain language,” use at least 10-point font, and organized by clearly and conspicuously displayed titles and headings. Notice must include the name and contact info of the covered entity; the types of covered info that were the subject of the breach; the date, estimated date, or date range of the breach; the date of the notice; whether notice was delayed due to law enforcement; general description of the breach; and toll-free numbers and addresses of the major credit reporting agencies, if Social Security numbers, drivers' license or state identification card numbers were exposed. If Social Security, drivers’ license or state identification card numbers are affected, and if the entity providing notice was the source of the breach, the entity must offer appropriate identity theft prevention and mitigation services, such as credit monitoring, at no cost to the resident for not less than 12 months. A template notification letter for California is provided in Section XIII.

Mishandling notifications can lead to severe consequences, including fines and other unbudgeted expenses. It could also tarnish your brand reputation and customer loyalty, leading to potential revenue loss.

**VIII. MANAGING COMMUNICATIONS**

You should develop a communications incident response process and plan that clearly outlines who will be responsible for developing and approving the key messages that will be communicated to media, as well as internal audiences. Communicating the right messages at the proper points in the lifecycle of a breach will have a significant impact on how a breach is reported.

* Focus initial messages on the steps being taken to investigate the issue and frame it as a criminal issue.
* Think through what you push out and how to respond via social channels. There’s no need to have a public debate in front of millions of followers.
* Set up the appropriate media/social monitoring and listening posts to see how the breach is being covered.
* Customers must be your north star, so make sure that you communicate with them clearly and effectively through traditional and digital channels.
* Do not neglect the wide variety of stakeholders interested in breaches, including policymakers, regulators (state and federal), and industry stakeholders (e.g. payment brands).

**IX. REVIEW RESPONSE AND UPDATE POLICIES**

In the aftermath of a security incident, you must plan and take preventative steps so a similar incident cannot happen again. Consider whether:

* An additional policy could have prevented the incident.
* A procedure or policy was not followed which allowed for the incident, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
* Any security policies need to be updated.
* Any lessons can be learned from this experience. The longer you wait to document lessons learned, the less likely it is that the lessons learned will be documented accurately and completely.

**X. AUDITING THE PLAN**

Auditing your preparedness plan helps ensure it stays current and useful. The chart below will help you audit your plan.

|  |  |  |
| --- | --- | --- |
| **Status** | **Action** | **Timing** |
|  | Update data breach Incident Response Team contact list.   * Check that contact information for internal and external members of your breach Incident Response Team is current. * Remove anyone who is no longer with your company or with an external partner and add new department heads. * Redistribute the updated list to the appropriate parties. | Quarterly |
|  | Verify your data breach response plan is comprehensive.   * Update your plan, as needed, to take into account any major company changes, such as recently established lines of business, departments or data management policies. * Verify that each Incident Response Team member and department understands its role during a data breach. Create example scenarios for your Incident Response Team and departments to address. | Quarterly |
|  | Double check your vendor contracts.   * Ensure you have valid contracts on file with your forensics firm, data breach resolution provider and other vendors. * Verify that your vendors and contracts still match the scope of your business. | Quarterly |
|  | Review notification guidelines.   * Ensure the notification portion of your response plan takes into account the latest state legislation. * Update your notification letter templates, if any, as needed, to reflect any new laws. * Verify your contacts are up to date for the attorneys, government agencies or media you will need to notify following a breach. | Quarterly |
|  | Check up on third parties that have access to your data.   * Review how third parties are managing your data and if they are meeting your data protection standards. This is done during the due diligence process. * Ensure they are up to date on any new legislation that may affect you during a data breach. * Verify they understand the importance of notifying you immediately of a breach and working with you to resolve it. This should be addressed in your contract with the vendor. | Quarterly |
|  | Evaluate IT Security.   * Ensure proper data access controls are in place. * Verify that company-wide automation of operating system and software updates are installing properly. * Ensure automated monitoring of and reporting on systems for security gaps is up to date. * Verify that backup tapes are stored securely. | Quarterly |
|  | Review staff security awareness.   * Ensure everyone on staff is up to date on proper data protection procedures, including what data, documents and emails to keep and what to securely discard. * Review how to spot and report the sign of a data breach from within everyday working environments. * Verify that employees are actively keeping mobile devices and laptops secure onsite and offsite and changing passwords every three months. | Yearly |

**XI. TEMPLATE CALIFORNIA BREACH NOTIFICATION LETTER**

All breach notification letters should be reviewed by legal counsel before being sent out.

|  |  |
| --- | --- |
| [*NAME OF DEALERSHIP/LOGO*]  Date: [*INSERT*] | |
| **NOTICE OF DATA BREACH** | |
| **What Happened?** | [*INSERT DESCRIPTION OF THE INCIDENT*] |
| **What Information Was Involved?** | [*INSERT DESCRIPTION OF INFORMATION INVOLVED*] |
| **What We Are Doing.** | [*INSERT DESCRIPTION OF WHAT DEALERSHIP IS DOING TO MITIGATE THE INCIDENT*] |
| **What You Can Do.** | We recommend the following steps that you can take to protect your information:   * **Credit Report Monitoring**   [*INSERT IF YOU ARE OFFERING CREDIT MONITORING*]   * **Monitor Your Credit Reports**   Even if you choose not to take advantage of this complimentary credit monitoring service, we remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:  **Experian**, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742  **TransUnion**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800  **Equifax**, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111  If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General’s office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft, as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:  Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).   * **Fraud Alert**   There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.   * **Fair Credit Reporting Act**   You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit [www.ftc.gov/credit](http://www.ftc.gov/credit). The FTC’s FCRA rights include:   * You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request. * Each of the nationwide credit reporting companies – Experian, TransUnion and Equifax – is required to provide you with a free copy of your credit report, at your request, once every 12 months. * You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You’re also entitled to one free report a year if you’re unemployed and plan to look for a job within 60 days; if you’re on welfare; or if your report is inaccurate because of fraud, including identity theft. * You have the right to ask for a credit score. * You have the right to dispute incomplete or inaccurate information. * Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. * Consumer reporting agencies may not report outdated negative information. * Access to your file is limited. And you must give your consent for reports to be provided to employers. * You may limit “prescreened” offers of credit and insurance you get based on information in your credit report. * You may seek damages from violators. * Identity theft victims and active duty military personnel have additional rights. |
| **Other Important Information.** | You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or call 1-877-438-4338. |
| **For More Information.** | Call [*TELEPHONE NUMBER*] or go to [*WEBSITE*]. |

**XII. NIST CHECKLIST OF ELEMENTS INCLUDED IN A RECOVERY PLAYBOOK**

In addition, the National Institute of Standards and Technology (NIST) provides the following checklist of elements to be included in a recovery playbook:

**A.1 Pre-Conditions Required for Effective Recovery**

The organization understood the need to be prepared and conducted planning to operate in a diminished condition. The playbook includes the following critical elements:

* A set of formal recovery processes.
* The criticality of organizational resources (e.g., people, facilities, technical components, external services) that are required to achieve the organization’s mission(s).
* Functional and security dependency maps to understand the order of restoration priority.
* A list of technology and personnel who will be responsible for defining and implementing recovery criteria and associated plans.
* A comprehensive recovery communications plan with fully integrated internal and external communications considerations, including information sharing criteria informed by recommendations in NIST SP 800-150 [11].

**A.2 Tactical Recovery Phase**

The following steps summarize the activities of the recovery team in the tactical recovery phase.

**A.2.1 Initiation**

* Receive a briefing from the incident response team to understand the extent of the cyber event.
* Determine the criticality and impact of the cyber event.
* Formulate an approach and set of specific actions.
* Heighten monitoring and alerting of the network and systems.
* Understand the adversary’s motivation.
* Identify the adversary’s footprint on the infrastructure, command and control channels, and tools and techniques.
* Inform all parties that the recovery activities have been initiated.
* Utilize all available information gathered to create the restoration plan.

**A.2.2 Execution**

* Begin to execute the restoration by validating and implementing remediation countermeasures in coordination with the incident response team and other information security personnel.
* Restore additional business services and communicate the restoration status with predefined parties.
* Track the actual time that critical services were unavailable or diminished, comparing the actual outage with agreed-upon service levels and recovery times.
* Document any issues that arise, any indicators of compromise, and newly identified dependencies.
* Coordinate with representatives from management, senior leadership, HR and legal to discuss appropriate notification activities.
* Additional recovery steps are initialized, including external interactions and services to restore confidence and to protect constituents.
* Validate that the restored assets are fully functional and meet the security posture required by the security team.

**A.2.3 Termination**

* Determine that termination criteria have been met and declare the end of the tactical recovery event.
* Stand down recovery team and have staff return to their normal job functions.
* Continue to monitor the infrastructure for potential persistency of malicious activities and inform the incident response and recovery team of any evidence.
* Finalize the metrics collected during the event.

**A.3 Strategic Recovery Phase**

The following steps summarize the activities performed during the strategic recovery phase.

**A.3.1 Planning and Execution**

* Support the various communication teams as they interact with internal users and public customers.
* Close the loop with external entities who have been involved during the tactical phase.
* Develop a plan to correct the root cause of the cyber event.
* Implement changes to strengthen the security posture of the organization.

**A.3.2 Metrics**

* After recovery is completed, review metrics that were collected.
* Review achievement of key milestones and assumptions that were made pre-recovery.

**A. 3.3 Recovery Plan Improvement**

* Use lessons learned from the recovery process to enhance the recovery plan.

1. Civil Code Section 1798.82. [↑](#footnote-ref-1)