The Path to Recovery:

10 Actions to Take When A Data Breach Strikes
When a suspected data privacy or security incident is reported, an organization must quickly initiate and manage their response. The process tends to be complex, stressful and “high stakes” for the organization given that their customers are affected and their reputation is at risk.

In our extensive experiences helping organizations safely navigate such situations, ID Experts® has found that there are three key principles that improve your organization’s ability to manage a data breach incident to create a positive outcome.

**BE PREPARED**
A well thought out, cross-functional, detailed data breach incident response plan takes the uncertainty out of responding to a privacy incident. Have one and make sure it is current.

**RESPOND QUICKLY**
Your customers will not understand nor appreciate any delays in being notified about your data breach. Increasingly, regulatory and enforcement authorities are also taking a hardline position of rapid notification. Lax response times can and will lead to investigations, fines and penalties.

**ADDRESS CUSTOMER CONCERNS**
Amazingly, many organizations treat a data breach response as primarily a legal exercise. Yet the manner in which you choose to care for your customers will determine whether they decide to “fire” you as their provider of products or services. The most important thing you can do is to provide them with a real, live, knowledgeable person to talk with about the situation and their issues.

*With these three principles in mind, here are 10 immediate steps to take when a data breach strikes:*
1. Assemble your core incident response team.

Ensure that the team has a senior executive sponsor and is given the authority and the budgetary flexibility to take immediate action.

» Document everything because you are establishing a burden of proof.
» Establish a communication protocol with the extended team, including executives and operational staff, as well as outsiders in case the news is leaked prematurely before all the facts are known.

2. Confirm your priorities.

Make sure everyone knows the priorities that guide the team’s actions. Make a prioritized list to remind everyone of these end goals:

» Preventing harm to customers
» Protecting organization’s reputation
» Regaining customers’ trust
» Preventing revenue loss
» Avoiding regulatory fines
» Minimizing cost of customer notification and protection services

3. Contain, Fix, and Restore.

If the incident is system related, you must immediately contain the problem and restore the affected system while preserving digital evidence.

» It is critical to identify the scope and root cause of an incident and take immediate steps to prevent it from causing further damage by conducting digital forensics analysis and preserving evidence. Refer to step #4 if you need external expertise in this specialized area.
» Regulators will ask for evidence of any action you’ve taken to determine the root cause of the data breach.
» You will be asked to provide evidence of steps taken to prevent the situation from happening again.

“As appalling as the data loss, equally alarming and potentially illegal is the delay in disclosing it…Failing to promptly notify providers of the breach is inexcusable — and a possible violation of state law. Waiting two months left providers severely at risk — needlessly and irresponsibly exposing them to financial mayhem.”

— Richard Blumenthal
Connecticut Attorney General, speaking about Anthem Blue Cross Blue Shield of Connecticut
4. Engage pre-selected external resources.

Ideally you have already identified what breach response functions (legal, forensic, notification, victim protection) you will outsource based on your organization’s resource needs and priorities per #2.

» Sign business associate agreement(s) with your vendor(s) if you haven’t done so already.

» If you operate in the healthcare sector, secure your external resources’ support to assist you with the Department of Health and Human Services’ Office for Civil Rights (OCR) investigation.

5. Conduct an incident risk assessment.

Document your investigation and risk assessment process to meet regulatory requirements.

» You will be required to produce a risk assessment that is objective and consistent, when investigated by regulators, such as the OCR.

» Is your suspected incident a data breach? Does it qualify for any exception provisions allowed under the new breach notification rules? For example, if a laptop or server containing unprotected personally identifiable information (PII) or protected health information (PHI) is lost or stolen, the incident is a reportable breach.

» ID Experts offers a Web-based tool called RADAR™ to assist with this assessment and documentation.


Keep in mind that you have to address the immediate concerns of your customers while ensuring that your actions are in compliance with the expectations of regulatory agencies.

» Do not delay your notification just because the law gives you a certain amount of time. To a customer, even 24 hours can seem too long to wait. Also, remember that some state laws require much faster notification.

» Your notification letters must address all the elements required by both the state(s) and the federal regulations; and must be delivered within the required timelines.

» In healthcare, some laws also require you to notify the media if more than 500 individuals are affected in a single jurisdiction.

“Companies’ investments in finding and remediating data breaches may be paying off…In particular, increases in legal defense costs remain a main reason for increased spending in ex-post response, as companies fear successful class action lawsuits by breach victims.”

— Ponemon Institute

“2010 Annual Study: US Cost of Data Breach”, March 2011
» Consider state specific requirements and notification timelines since they may be different given that 46 states and one territory have their own privacy laws.

» Should you offer the affected individuals any protection services, such as medical or credit monitoring? This is often a consideration based on your priorities in step #2. Some states, such as Connecticut, give state agencies the discretion to require protection services under certain circumstances.

7. Set up a call center.

Plan for call center support and customer relationship management (CRM) system to handle concerned and often angry customer calls.

» Consider seeking outside assistance in handling this process. Most organizations do not have trained resources or the infrastructure necessary for handling calls from the affected customer.

» How will you handle calls from multi-lingual or unique populations, such as the deaf, mentally disabled or families representing deceased victims?

» Proper handling of these calls can significantly reduce any damage to your reputation and lower overall costs.

8. Know federal and state requirements.

Ensure compliance to both federal and state obligations to avoid risking additional penalties.

» Regulations, such as the Gramm-Leach-Bliley Act and the HITECH Act, have very specific requirements and thresholds for when and how to notify individuals and the media.

» Many states have introduced their own unique requirements, which can often be more stringent than federal regulatory obligations.

9. Report the breach to federal and state agencies.

Knowing what regulatory and investigative bodies expect is key to compliance.

» The Federal Trade Commission (FTC) is the enforcing agency for privacy data breaches.

“As more companies choose to use a third-party cloud provider in 2011, they need to outline specific requirements… to meet regulatory obligations…. Policies should include how soon the cloud provider needs to alert the organization of a suspected breach.”

— Ernst & Young

“Privacy Trends of 2011”, January 2011
For breaches affecting the healthcare sector, HHS requires concurrent reporting if 500 or more patients are affected as a result of the breach.

Based on many variables of the breach, you may need to report the breach to multiple agencies in each state where the affected victims reside.

10. Be prepared for an investigation.

As data breaches become more common, lawmakers are cracking down.

Anticipate and prepare for regulators’ requests. Ask your vendor for a checklist of required documents.

Make sure your vendors can support you during the investigation.

Managing a data breach lifecycle can be a daunting ordeal to any organization — but it doesn’t have to be.

With some thoughtful and prioritized objectives and the right outsourced partners, organizations can successfully contain the damage and even derive positive outcomes from a data breach incident.

To assist organizations with managing the risks of privacy incidents and maintaining compliance, including prevention, mitigation, and breach notification, ID Experts provides a complete range of services and technologies under its Complete Data Breach Care framework. Please visit http://www2.idexpertscorp.com/ for more information.

Talk to an expert today:

866.726.4271
info@idexpertscorp.com

ABOUT ID EXPERTS
ID Experts is the leader in comprehensive data breach prevention and response, with a focus on full recovery. Founded in 2003, ID Experts has managed hundreds of data breach incidents for leading healthcare organizations, corporations, financial institutions, universities, and government agencies across the United States. We are passionate about protecting the organizations and individuals we serve from the threat of identity crime.

Learn more >
**10 ACTIONS TO TAKE**

<table>
<thead>
<tr>
<th><strong>WHAT SETS ID EXPERTS APART....</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Immediately assemble your core incident response team</td>
</tr>
<tr>
<td>2) Confirm your priorities</td>
</tr>
<tr>
<td>3) Contain, Fix, and Restore</td>
</tr>
<tr>
<td>4) Engage pre-selected external resources</td>
</tr>
<tr>
<td>5) Conduct an incident risk assessment</td>
</tr>
<tr>
<td>6) Notify customers quickly</td>
</tr>
</tbody>
</table>

---

“…lawyers in Canada have announced they’re seeking a $1 billion class action lawsuit against the company [Sony] which has recently revealed not one, but two massive hacking breaches that left personal information from 102 million gaming accounts available to hackers.”

— MSNBC.com

“Sony Declines to Testify Before Congress”, May 2011
<table>
<thead>
<tr>
<th>10 ACTIONS TO TAKE</th>
<th>WHAT SETS ID EXPERTS APART....</th>
</tr>
</thead>
<tbody>
<tr>
<td>7) Set-up a call center</td>
<td>ID Experts establishes a tailored incident-specific call-center service to fit your needs, including support for more than 80 languages and unique populations. Our dedicated toll-free number provides easy access to experienced &quot;live&quot; agents, who can process up to 28,000 calls per day.</td>
</tr>
<tr>
<td>8) Know federal and state requirements</td>
<td>Notification laws for breaches vary by state. And in some cases, federal laws may preempt state laws, so achieving compliance is no easy task. ID Experts has extensive knowledge in state and federal requirements from managing hundreds of data breach incidents, protecting millions of affected individuals, for leading healthcare organizations, corporations, financial institutions, universities and government agencies.</td>
</tr>
<tr>
<td>9) Report the breach to federal and state agencies</td>
<td>ID Experts will notify all necessary federal agencies, as well as appropriate state agencies on your behalf. Additionally, our RADAR tool facilitates compliant communications with HHS.</td>
</tr>
<tr>
<td>10) Be prepared for an investigation</td>
<td>ID Experts helps organizations gather the required information, document the breach notification response and provide recommendations on necessary remediation efforts.</td>
</tr>
</tbody>
</table>

**ABOUT THIS DOCUMENT**

Please realize that every data breach situation is unique and requires individual attention to provide the best outcome for all affected parties. This document is intended to provide you with guidance as to general high impact best practices that will assist in responding to a data breach detection — it is not intended to be exhaustive as far as all of your privacy and security obligations. This information is not intended to be or replace legal advice. Please seek out your legal counsel for such advice.

**DATA BREACHES DON’T DISCRIMINATE**

Neither do federal regulators. Organizations of all types and sizes must comply with state and federal privacy and data breach notification regulations.

Learn more >
Helpful Resources and Information

ID EXPERTS’ DATA BREACH BLOG
News and insight on data breach privacy, security and notification.
http://www2.idexpertscorp.com/blog

NEWSLETTER SIGNUP — DATA BREACH EXAMINER
Stay informed with quarterly updates on the latest solutions and regulations.
http://www2.idexpertscorp.com/resources/general-resources/data-breach-examiner-archive/

DATA BREACH LIFELINE
Confidential, experienced help is only a phone call away.
1-866-726-4271

ALL THINGS HITECH — LINKEDIN GROUP
Join the conversation about privacy, healthcare and compliance in the All Things HITECH Group.
http://www.linkedin.com/groups/All-Things-HITECH-3873240

RESEARCH & RESOURCES
Find information tailored to the unique incident response requirements that apply to your business.
http://www2.idexpertscorp.com/resources


Ponemon 2010 Annual Study: U.S. Cost of a Data Breach — 51 U.S. companies weigh in on the effects of data breach: costs, customer turnover and preventive solutions. Download »

Benchmark Study on Patient Privacy and Data Security — A look at patient privacy, data loss, and the impact of the HITECH Act. Download »