

The Trust Catalyst Data Breach Prep Kit

Preparing your organization's response before navigating a data breach



Executive Summary



The number of records exposed in data breach incidents over the last decade has reached epic proportions putting customers in a vulnerable, anxious position. According to the Data Loss database created by the Open Security Foundation, over half a billion records have been exposed in over 1,990 incidents since 2000 and this number is quickly growing as unreported cases are added daily. And, while accidental disclosures have put companies in the headlines, a new enemy in the war on data breach is emerging – cybercriminals willing and able to profit from identity fraud. The U.S. Department of Justice recently testified to Congress that identity theft convictions have increased 138% over the last four years. The Federal Trade Commission estimated that over nine million Americans are victims of identity theft each year costing the U.S. business \$50 billion in damages annually.

Increasingly, identity theft crimes are targeted and organized by criminals who have a cyber connection. Perhaps no piece of research has put the profits of cybercriminals more on the map than the recent *Verizon Data Breach Investigation Report*, which documented the findings of 258 compromised records stolen from over 600 corporate networks investigated by Verizon. Unlike the Open Security Foundation’s database, this report focused only on the subset of compromised records that were investigated in connection with identity fraud crimes. Ninety-eight percent of these cases involved an outside intruder hacking into the corporate network through vulnerability, installing malware and collecting data. Ninety-nine percent of the time, the target of the breach was a server (as opposed to data loss incidents which often involve the loss of sensitive information via unencrypted backup tapes, laptops or “dumpster diving”). In over 90 percent of the cases reported by Verizon, the attacker was connected to a global cybercriminal ring already known to law enforcement. Probably the most disturbing finding was that for the majority of compromised organizations, they were unaware of the breach. Most often, these organizations were notified by either their customers, law enforcement, a credit card company or a business partner that verified an identity fraud crime had been committed before it was discovered by the victim organization.

In this environment, if you store customer sensitive data, you need to be thinking about how your organization will be prepared to handle a data breach. Most organizations collecting personal data about their customers will not be immune. In fact, we believe organizations should prepare themselves now for breaches that may happen in the future. Depending on the severity and size of the breach, you will face a different set of management challenges. When outside pressure from customers, media and regulators mount, you will not want this to be the first time where your data breach management skills are tested. In addition, as more of our customers are actually victims in identity fraud crimes, we must step up our response so as not totally destroy customer trust. We believe the way successful organizations handle breach events will raise the stakes of they typical response we are seeing today. Organizations interested in maintaining a relationship with their customers post-breach will be more open and transparent and exchange more critical information with customers and law enforcement agencies.

The Data Breach Prep Kit was designed to help you start thinking about how you want to handle breaches. It can help you prepare an incident response plan in advance of a breach, help you think through how to educate key stakeholders in your company and even estimate potential costs of breaches so you can build the right plan to protect your customers today. Unfortunately, this prep kit alone cannot accurately predict how a data breach crisis will impact your specific organization, but it can help you get prepared, gather the facts and make important trade-offs required to develop long-term strategies to protect the value of your company. If you find you need more help planning your response and weighing the costs, contact us and we will be happy to develop a customized plan for your organization.

The Data Breach Prep Kit includes a number of helpful resources and is a great first step for:

- Defining the three types of data breaches
- Creating a data breach incident response plan
- Managing the crisis – how to define strategy for threat level
- Data breach estimated costs worksheet
- Data breach incidents response report worksheets
- Data breach checklist
- References and helpful resources for future reading

We hope this reference helps you uncover some of the questions your business needs to address now and helps you calculate the risks and costs to sell strategies that will help you protect your customers.

Best regards,



Founder and Principal, Trust Catalyst


email: kim@trustcatalyst.com

direct: +1.415.887.9330

www.trustcatalyst.com

Data Breaches Defined

There are three different types of data breach incidents as illustrated in the illustration and table below. Each type of breach can elicit a different type of response from the organization, which is critical in the education of your organization, creation of your response plan and determining your costs.



Data Loss	<ul style="list-style-type: none">• Half a billion records disclosed• Over 1,990 incidents reported since 2000• Mostly accidental disclosure
Data Theft	<ul style="list-style-type: none">• Over 300 million compromised records• Over 600 reported cases• Crime committed against victim organization
Identity Theft	<ul style="list-style-type: none">• Costs US Businesses \$50B a year• Crime committed against your customer or employee• Estimated 9 million Americans impacted each year

Data Breaches Defined – A Short Summary

	Data Loss	Data Theft	Identity Theft / Fraud
Definition	Accidental loss or disclosure of unencrypted customer PII or other sensitive information – particularly that used in identity theft/fraud crimes.	Theft of PII or sensitive data used in identity theft/fraud crimes. Often the result of a computer intrusion (hacker) or malicious insider (employee or business partner) with permissions to the data who steals and uses in a crime.	Lost or stolen data is actually used in for identity theft or fraud. Now, the customer/consumer is damaged and a victim.
Common examples	<ul style="list-style-type: none"> • Lost laptop • Lost tape or media • Email accidents 	<ul style="list-style-type: none"> • Computer / network intrusion • Exploit mistake to gain access to network / hack into network, install malware and collect data • SQL injections • Malware in your customer’s computer • Business partners; supply chain, vendors • Insider malicious threat 	<ul style="list-style-type: none"> • New account creation • Account takeover • ATM or PIN compromise • Fraudulent charges (i.e. card not present fraud) • Open new loans and applications
How can I reduce the risk?	<p>Use encryption and Data Leakage Prevention (DLP):</p> <ol style="list-style-type: none"> 1. Encrypt PII that leaves the organization especially on laptops, backup tapes and in email. 2. Discover where sensitive data is located within the organization 3. Monitor PII in motion over the network for data leaks of PII going to partners or third parties. 4. Monitor PII leaving the organization or mistakes in web applications. 	<p>Regular security assessments and vulnerability scans conducted by an outside forensics or security professional service firm. Due to PCI requirements, your organization may be required to conduct these by qualified QSA a certain number of times a year. Even if you are not regulated by PCI, you can dramatically decrease your risks by conducting these types of audits regularly.</p>	<p>If you accept payment for services online or offer online banking/payment products you will be in a position to accept or reject transactions you think are fraud with:</p> <ul style="list-style-type: none"> • Risk profiling / risk scoring algorithms • Backend automated and manual fraud detection processes • Cross-industry information sharing databases
Impacts	<ul style="list-style-type: none"> • Estimated there are over half a billion records currently exposed and over 1,990 reported data loss incidents since 2000. • Costs organizations millions in data breach notification process. • The average cost per record in US is \$202 • Lost trust from customers can cause lost business – depending on how the organization responds to their customers, lost business can account for 69% of the costs of a breach 	<ul style="list-style-type: none"> • One forensic firm has estimated their caseload to account for over 258 million compromised accounts – there are over 600 individual cases. • Costs organizations millions in data breach notification process • The average cost per record in US is \$202 in 2008 • Lost business – depending on how the organization responds, lost business can account for 69% of the costs of a breach. • Regulatory fines • Costs to make customers “whole” • Lawsuits from damaged customers 	<ul style="list-style-type: none"> • Estimated there are 9M US ID theft victims a year • US ID theft convictions have risen 138% last four years • ID theft costs the US business \$50 million in 2008 • Average cost to the consumer who is a victim of ID theft is \$5,720 • Online fraud costs eCommerce merchants an estimated \$10 billion annually

Creating a Data Breach Incident Response Plan

If your organization experiences a data breach, there are a lot of moving parts and people that must be managed effectively to reduce damages from diminished customer trust. You will need to get the right information out to the right people very quickly. Business leaders in your organization who may have never worked together in a crisis may form your incident response team and, as it often turns out, different stakeholders have conflicting agendas. This is hard enough to manage under normal conditions but amplified when managing a crisis like data breach.

Depending on the severity of the breach and number of victims impacted, you may also have to bring in outsiders to manage different aspects of the crisis including investigators and even law enforcement. And, as outside pressures from customers, media and auditors or regulators mount, your management skills will be tested. Put simply, the aftermath of data breach is not the first time where you will want to be tested. Putting together your response plan in advance can be invaluable learning experience. Inevitably, you will uncover questions in the planning that your organization may not have considered. Now is the time to uncover the unknowns, get answers from key stakeholders and building awareness and recommendations for how different types of breaches should be handled as well as estimate their cost to your business.

Getting everyone on the same page

Not all data breaches are the same. There are different levels, responses and costs based on the type of breach you encounter, number of customers impacted and type of fraud (if any) found. And, if you are in the fortunate position to act quickly, you can begin preventing a data loss situation from turning into a data theft / identity fraud crisis where costs and stakes are dramatically increased.

The worksheet below simplifies the types of breaches to four different scenarios that require different response plans. This worksheet will help you work through the type of response you will want to produce based on the stage of data breach encountered. It should help you start to identify the key resources you will need to successfully manage the breach. While this is not a complete response plan, where possible we have provided either recommendations or questions for you to consider to begin the process of building your own. We recommend using this worksheet as a starting point to create a chart in your organization that you can use as an educational tool to prepare different stakeholders about the action that will be required and questions that will come up in the process to manage a data breach. Train your organization on the difference between the different levels of breaches and how issues will be escalated and treated differently depending on the stage of the breach. Some organizations may even want to organize mock breach incidents like a fire drill to test their team in advance. Also, because each organization is regulated differently, you may want to add what compliance requirements you will specifically encounter at each stage.

Data Breach Incident Response Plan Worksheet

	Stage 0	Response / Action Required
Data Loss	<p>Lost laptop, PDA, backup tape or storage media with sensitive data was lost.</p> <p>This data was encrypted and there is an audit log that proves data is protected.</p>	<p>No notification process required because sensitive data has been adequately protected.</p> <p>Recommended Actions:</p> <ul style="list-style-type: none"> • Have an internal team investigate what was lost and produce a report that shows response proving the data was protected. Include the number of records/customers you protected in this incidence and estimate the cost having these protections in place save the organization. • Report on these types of breaches to the business as appropriate to build a case for the return on investment technologies you've put in place to protect the organization are producing. • <p>Questions for the business:</p> <ul style="list-style-type: none"> • Who is the internal team and key stakeholders? • Is there ever a case where encrypted lost data would need to be reported publicly? If so, document these examples and include them in the appropriate stage in this response plan. • If you are not encrypting high-risk data, what is preventing this from happening? Perhaps, going through a cost-based risk assessment of the costs of preventing a notification event is required to get investment for these types of solutions in your organization (for example, see the Cost Worksheet provided in this document).

	Stage 1	Response / Action Required
<p>Data Loss</p>	<p>Lost laptop, PDA, backup tape or storage media with sensitive data was lost.</p> <p>Data lost was not encrypted.</p>	<p>Notification process required. Customers at risk for identity theft.</p> <p>Recommended actions:</p> <ul style="list-style-type: none"> • Security team produces a report with critical information for example: customers affected, number affected, where they reside, date information was lost, type of information that was lost (e.g. SSN, CCN...). • In your opinion, what risk exists for these customers to become victims of identity theft/fraud? What steps would you take to prevent customers from being financially damaged if they become victims of identity theft (e.g. Can you work with law enforcement? Should you offer credit monitoring services or identity theft insurance? Who should receive these services?) • Create assessment of situation and offer the organization a recommended course of action depending on the type of information disclosed / potential risk. How much would this cost? Are the costs justified by the amount of business you will save from negative customer reaction and diminished trust? • Implement recommended course of action <p>Questions for the business:</p> <ul style="list-style-type: none"> • What would be the impact of losing revenue from 30% of your customers following the breach notification? • Who are the security team and key stakeholders? Will you require outside security, PR or legal services?

	Stage 2	Response / Action Required
Data Theft	Data theft occurred – know the origin / how theft was committed	<p>Notification process required. Customers at elevated risk for identity theft.</p> <p><u>Recommended actions:</u></p> <ul style="list-style-type: none"> • Appoint team that produces a report with critical information for example: customers affected, number affected, where they reside, date information was lost, type of information that was lost (e.g. SSN, CCN...), how the data was compromised and what steps are being taken to prevent this from happening in the future. • In your opinion, what risk exists for these customers to become victims of identity theft/fraud? What steps would you take to prevent customers from being financially damaged if they become victims of identity theft (e.g. Can you work with law enforcement? Should you offer credit monitoring services or identity theft insurance? Who should receive these services?) • Create assessment of situation and offer the organization a recommended course of action depending on the type of information disclosed / potential risk. How much would this cost? Are the costs justified by the amount of business you will save from negative customer reaction and diminished trust? • Implement recommended course of action <p><u>Questions for the business:</u></p> <ul style="list-style-type: none"> • What would be the impact of losing revenue from 30% of your customers following the breach notification? What can you do to make diminish the impacts of lost customer trust and lost competitive advantage? • Who is the team investigating the breach? Is it the same as in a level one breach or does it change? • Will you require outside security, PR or legal services? • What type of case can you pull together for law enforcement so that they can act quickly, before there are financial damages? Would this be the same course of action if there were an insider who stole data versus a hacker?

Identity Theft or Fraud	Stage 3	Response Action Required
	<p>Identity theft occurred because notified by outside source (e.g. consumer, customer) they are seeing fraudulent activities and you are the source of origin.</p> <p>You do not know how data was stolen.</p>	<p>Notification process required. Customers have become victims of identity theft.</p> <p><u>Recommended actions:</u></p> <ul style="list-style-type: none"> • Bring in outside forensics investigation team to find source of origin and determine: customers affected, number affected, where they reside, date information was lost, type of information that was lost (e.g. SSN, CCN...), how the data was compromised and what steps are being taken to fix the problem and prevent this from happening in the future. • Contact law enforcement to determine what steps can be taken to find criminals and when to notify customers. • Begin notification process. What steps can you take to prevent more customers from being financially damaged as victims of identity theft (e.g. Offer credit monitoring services and/or identity theft insurance). • Create assessment of situation and recommended course of action through a cost justification by the amount of business you will save from more customers becoming victims, public reaction and diminished trust? • Implement recommended course of action. <p><u>Questions for the business:</u></p> <ul style="list-style-type: none"> • What would be the impact of losing revenue from 30% of your customers following the breach notification? What can you do to make diminish the impacts of lost customer trust and lost competitive advantage? • Who is the outside forensics team you will call in to investigate? How often are they assessing your network? • Will you require outside security, PR or legal services? • What is your relationship with law enforcement? • What type of case can you pull together for law enforcement so that they can act quickly to catch criminals? Would this be the same course of action if there were an insider who stole data versus a hacker? • How much cash should be put in reserve for damages resulting from lawsuits, settlement and fines?

Data Breach Estimated Costs Worksheet

The spreadsheet below gives a breakdown of the various costs involved with cleaning up a data breach. Costs will vary depending on type of breach, number of customers involved and severity of breach. You can customize this to your organization or estimates for different types of breaches.

Type of breach (data loss, data theft):	
Number of customer records exposed:	
What was disclosed (e.g. Credit card, debit card, social security, address...):	
Number of customers exposed:	
How many customers have become victims of identity theft:	
Customer Management	Costs
Notification (letters, website, press releases, cost of creation, printing and mailing)	
Credit monitoring service	
Identity theft insurance	
Customer retention program	
Customer support help desk	
Costs to create new accounts or replacement cards	
Costs to make customers "whole"	
Employee Management	
Employee training programs	
Lost employee productivity	
Outside Services	
Legal	
PR / Crisis Management / Communication	
Marketing	
Forensic Investigators	
Security Experts	
Regulatory Fines / Lawsuits	
Fines	
Lawsuits	
Network Upgrades	
Security upgrades (encryption, data leakage monitoring, services, etc.)	
Total Estimated Costs	

Definitions of Costs

Notifications: If the breach requires notification, the organization will need to create the notification and decide how they intend to notify those impacted. The organization will need to decide if they will be handling the notification or outsourcing this activity to an outside firm.

Credit Monitoring Services: To improve customer satisfaction and depending on the severity and type of information disclosed, organizations may choose to enroll the victims in a credit monitoring service as an additional layer of protection.

Identity Theft Insurance: To improve customer satisfaction and depending on the severity and type of information disclosed, organizations may choose to give victims identity theft insurance as an additional layer of protection and customer service.

Customer Retention Program: Some organizations (especially organizations who are service providers) create customer retention programs in the aftermath of data breach to explain outcomes to their customers in face-to-face meetings. For example, this type of interaction was encouraged after the Heartland breach and the costs were reported in their quarterly earnings call after the breach.

Customer Support Help Desk: Depending on the notification strategy, it may become necessary to train, assign or outsource customer support personnel to answer questions customers.

Costs to create new accounts or replacement cards: Depending on what was breached, some organizations may need to create replacement cards or provide new account credentials to customers involved in the breach.

Costs to make customers “whole”: For customers who become victims of identity theft or fraud as a result of the breach, organizations will find that they incur costs making customers “whole” for fraudulent charges or damages.

Employee Training Programs: Some organizations rollout training programs for employees in the aftermath of significant data breaches to arm employees with the right types of information that can improve customer trust.

Lost Employee Productivity: Organizations face lost employee productivity as they are taken off revenue-generating activities to deal with the aftermath of data breach. What would be the cost to your organization if you lost five, ten or even 20 percent of employee productivity?

Legal Services: To effectively manage the data breach crisis, some organizations find they need to pay outside law firms who have specialized expertise in data breach. These services often require retainers or money paid up front for legal fees.

PR/Crisis Management/Communication Services: To effectively communicate and manage the media and their brand, some organizations turn to outside PR firms that specialize in crisis management and data breach. An outside, objective point of view is often an invaluable resource to effectively manage a data breach crisis and improve the handling of the breach in the eyes of customers and victims.

Marketing Services: To help plan the strategy to manage the customers and brand in the aftermath of data breach, some organizations turn to outside marketing and research firms to plan strategy or help increase customer satisfaction ratings to decrease the costs in lost business that follow data breach.

Forensic Investigation Services: For organizations victim of data theft, it is imperative that a forensic investigation firm find the source of the breach and help the organization capture evidence that could be used to catch the criminals.

Information Security Professional Services: Depending on the source of the breach and internal expertise of the IT organization, some organizations may need to retain additional information security professionals to help deploy or execute modifications required in the technology infrastructure in the aftermath of breach.

Regulatory Fines: If the organization has compliance or regulatory requirements, they could have fines assessed against the organization for not meeting these requirements.

Lawsuits: The organization may find they face a number of different lawsuits from class action on behalf of customers to lawsuits from other business partners who need to reclaim damages as a result of the breach.

Security Upgrades: Many organizations find they need to make upgrades to their technology infrastructure to protect against future attacks or breaches. Technology investments often include encryption projects and data leakage monitoring technology.

Incident Response Report Information

Part I: Information about the type of customer sensitive data you store and regulations with which you comply

This information can be completed in advance so you have a picture of the sensitive data residing internally and regulations that have requirements for protecting this type of information. You may find that you want to take steps to protect additional types of information even if not required by law.

What type of organization are we:	
<input type="checkbox"/> Data Owner	<input type="checkbox"/> Service Provider
We store the following PII about customers:	
<input type="checkbox"/> Email addresses	<input type="checkbox"/> Credit Card Numbers
<input type="checkbox"/> Date of Birth	<input type="checkbox"/> Account Information
<input type="checkbox"/> Mother's Maiden Name	<input type="checkbox"/> Debit Account Numbers
<input type="checkbox"/> Employee ID Number	<input type="checkbox"/> PINs
<input type="checkbox"/> Social Security Number	<input type="checkbox"/> CVVs or Card Security Codes
<input type="checkbox"/> Passport Number	<input type="checkbox"/> Credit Card Magnetic Strip Track 1 or 2 Data
<input type="checkbox"/> Driver's License Number	<input type="checkbox"/> Passwords, secret codes or access numbers for account info
<input type="checkbox"/> Passwords for online accounts	<input type="checkbox"/> Billing Address
<input type="checkbox"/> Health Data	<input type="checkbox"/> Shipping Address
<input type="checkbox"/> Payroll information	<input type="checkbox"/> Phone Number
<input type="checkbox"/> Credit scores	
<input type="checkbox"/> Other:	
We are required to comply with:	
<input type="checkbox"/> State Data Notification Laws (U.S.)	<input type="checkbox"/> PCI DSS
<input type="checkbox"/> GLBA	<input type="checkbox"/> HIPAA
<input type="checkbox"/> UK Data Protection Act	<input type="checkbox"/> Other:

Part II: Data Breach Incident Response Team – Internal Team

Complete the information for the key personnel that will make up your internal team, their contact information and who is the project lead.

Data Breach Incident Response Team	Contact Information; Indicate Project Lead
<input type="checkbox"/> Chief Executive Officer	
<input type="checkbox"/> Chief Risk Officer	
<input type="checkbox"/> Chief Financial Officer	
<input type="checkbox"/> Chief Privacy Officer	
<input type="checkbox"/> Chief Information Security Officer	
<input type="checkbox"/> Chief Information Officer	
<input type="checkbox"/> Chief Compliance Officer	
<input type="checkbox"/> General Counsel	
<input type="checkbox"/> Marketing	
<input type="checkbox"/> Sales	
<input type="checkbox"/> Customer Relations / Customer Support	
<input type="checkbox"/> Other	
<input type="checkbox"/> Other	

Part III: Law Enforcement Contacts

Insert information about the law enforcement contacts that you would need to contact in event of a crime has been committed. The more relationships you have with these people prior to the incident, the easier it will be to get an appropriate response. Attend industry meetings with law enforcement presence or establish relationships with the key personnel when possible.

Data Breach Incident Response Team	Contact Information
Local law enforcement:	
FBI	
U.S. Secret Service	
U.S. Postal Inspections	
International Law Enforcement Agencies	

Part IV: Data Breach Incident Response Checklist

The following is a checklist of the items that you may or may not need to complete depending on the severity and number of records breached. This will allow you to decide which items fit your business needs and assign ownership of the tasks with a completion date.

Project Lead:		
Incident Stage (0-3):		
Planning:		
<input type="checkbox"/> Will you provide customers with a credit monitoring service?		
<input type="checkbox"/> Will you provide customers with an identity theft protection insurance?		
<input type="checkbox"/> Will you creation new accounts or plastic for customers?		
<input type="checkbox"/> If customer is damaged with identity fraud, how can they report this to you?		
Tasks	Owner	Completion
<input type="checkbox"/> Assign who will manage PR about the breach (current firm, crisis management firm or internal resource)		
<input type="checkbox"/> Determine corporate spokesperson for breach questions from media		
<input type="checkbox"/> Write website copy about breach and steps taken to protect customers from identity theft		
<input type="checkbox"/> Approve website copy about breach		
<input type="checkbox"/> Post to website		
<input type="checkbox"/> Draft copy for press release		
<input type="checkbox"/> Approve press release		
<input type="checkbox"/> Post press release		
<input type="checkbox"/> Draft FAQ for customers		
<input type="checkbox"/> Approve FAQ for customers		
<input type="checkbox"/> Post FAQ for customers on website		
<input type="checkbox"/> Create data breach notification letters to breached customers (or edit sample letter)		
<input type="checkbox"/> Approve data breach notification letters		
<input type="checkbox"/> Create de-duped customer mailing list		
<input type="checkbox"/> Print and mail letters		
<input type="checkbox"/> Create FAQ for employees (to educate all employees about the situation)		
<input type="checkbox"/> Approve FAQ for all employees		
<input type="checkbox"/> Post to internal corporate website		
<input type="checkbox"/> Write email to notify employees about breach		
<input type="checkbox"/> Approve email to notify employees about breach		

Tasks	Owner	Completion
<input type="checkbox"/> Send email to employees		
<input type="checkbox"/> Determine if additional employee / sales training required (concall, webcast or meeting??)		
<input type="checkbox"/> Schedule training		
<input type="checkbox"/> Send invitations to employees required for training		
<input type="checkbox"/> Write customer support / help desk training FAQ		
<input type="checkbox"/> Approve help desk training FAQ		
<input type="checkbox"/> Train help desk personnel on how to handle customer calls about breach		

Notes:

Part V: Incident Response Form – Frequently Asked Questions

The questions below are frequently asked in the process to create notification letters, write FAQs for customers and manage the breach. Marketing, PR and customer-facing employees will need to know how to answer these questions.

What stage is the breach (0-3)	
When was it reported?	
When did it occur?	
How was it discovered?	
Who was impacted?	
Has it been remediated?	
How was it remediated?	
How many customers impacted?	
Where are customers located?	
Are you working with law enforcement?	
Have arrests been made?	

Conclusion

While the prevention of data breach is mostly an IT function, managing the aftermath of a breach turns out to be a less of an IT function and more of a marketing / customer relations program. Organizations find these events challenging because they are a crisis that tests the leadership of different business units within the organization. We hope this Data Breach Prep Kit can help you plan the appropriate action plan for dealing with a breach before one affects your organization. We also hope you are able to start to assemble the right inter-departmental team in advance to help protect customers, their trust in your organization to manage their sensitive information and your brand.

We will be updating this Data Breach Prep Kit over the course of the next year, as we receive more feedback from the organizations that put it to use. Email the author Kim Getgen, Principle, Trust Catalyst at kim@trustcatalyst.com to provide feedback or check back at www.trustcatalyst.com for updated versions and new resources to manage data breaches. We very much would like to hear from you. You can also join us at the LinkedIn Group “Prevent Data Breaches” to exchange updates and questions with colleagues and peers about the subject of data breach and data protection.

Resources Mentioned in This Document:

- Open Security Project Data Loss Database at: www.datalossdb.org
- 2009 Verizon Data Breach Investigation Report: www.verizonbusiness.com/products/security/risk/databreach/
- 2009 Online Fraud Benchmark Survey Report:
<https://365.rsaconference.com/community/efraudnetwork;jsessionid=F522AF189405DBF831ED292FADFA9FD0>
- 2008 Encryption and Key Management Benchmark Survey: www.trustcatalyst.com/Research.html
- Consumer Survey on Data Breach Notification, Javelin Strategy and Research 2008

About Trust Catalyst

Trust Catalyst helps companies make critical decisions about how to protect their most valuable resource – their customer’s trust. We understand that the adoption of a successful data protection or security program is about selling a strategy to a larger audience. We speak the language business executives understand and quantify the need for security by helping establish the costs of lost customer trust and the disruption to business when that trust is broken. As more insidious attacks from cybercriminals specifically targeting organizations with customer’s sensitive data grows, we help businesses understand the threats, the costs of the threats and how to maintain trusted relationships with their customers. Learn more and download helpful tools that can help you prepare for these types of attacks at www.trustcatalyst.com

Notice About This Document

This document is not intended as legal advice. This document is intended to assist companies get a jump-start on preparing their response to data breach incidents. Each organization is different and we encourage you to customize these worksheets to your particular situation. If you have feedback or advice to make this a better guide, please contact us so we can update this guide. If you would like to share any feedback, please contact us at kim@trustcatalyst.com or call +1.415.877.9330.