

Addressing Privacy Issues During Disaster Recovery

Rebecca Herold, CISSP, CISM, CISA, FLMI

IS PRIVACY IMPORTANT DURING A DISASTER?

Businesses possess a staggering amount of private and personally identifiable information (which I will collectively reference for the rest of this article as “PII”), not only about their customers, but also about their employees. Under which circumstances and representations was the information collected? How is that information being used? To whom is that information being transmitted? How is that information being stored? Who has access, authorized or not, to that information? Unfortunately, many, if not most, businesses do not know the answers to these questions even under normal business circumstances.

The first order of business following a disaster of any size or type is typically to get the most critical parts of business going again as soon as possible. The concept of “continuous availability” has become more of a norm now than a decade or more ago

when it was just wishful thinking. As a result, disaster plans often address speed to recovery but overlook information privacy issues, leaving real vulnerabilities to the protection of PII.

LESSONS LEARNED FROM REAL DISASTERS

Here are just a few real-life examples of disasters and some of the associated privacy issues involved with each.

September 11, 2001, Terrorist Attacks

After the horrific World Trade Center and Pentagon terrorist attacks on September 11, 2001, many people were surprised by the abundance of papers that survived and were scattered around the city by the wind, much of them containing PII. Many were surprised to learn that as a result of the attack, all ways to determine where PII was stored were lost with the destroyed businesses, along with the information about who else

REBECCA HEROLD, CISSP, CISM, CISA, FLMI, is an information privacy, security, and compliance consultant, author, and instructor. Rebecca has more than 15 years of information privacy, security, and regulatory compliance experience and assists organizations of all sizes with their information privacy, security, and regulatory compliance programs. Prior to owning her own business, Rebecca was VP — Privacy Services and CPO at DelCrea for two years. She was also Senior Systems Security Consultant at Principal Financial Group (PFG), where she was instrumental in building the information security and privacy program, which was awarded the 1998 CSI Information Security Program of the Year. Rebecca is the author of The Privacy Papers (Auerbach, 2001) and Managing an Information Security and Privacy Training and Awareness Program (Auerbach, 2005), and co-author of The Practical Guide to HIPAA Privacy and Security Compliance (Auerbach, 2003) and The Business Executive Practical Guides to Compliance and Security Risks book series in 2004. She can be reached at rebecca.herold@rebeccaerold.com.

possessed or had access to that information, creating the risk of misuse of that information because the oversight was no longer in place. Soon after the attacks, items collected from the World Trade Center and Pentagon buildings were being auctioned off on the Internet site eBay¹; could some of these so-called artifacts have contained PII, being sold to the highest bidder? (Note that eBay soon disallowed the sale of such items.)

Privacy Issues

- During such a catastrophic disaster, PII is uncontrollably lost in the public environment and cannot be accounted for.
- Systems that stored the information became unaccounted for, with no documentation and no persons surviving to identify where copies of PII were stored within other locations.
- With normal communication lines destroyed, much PII was sent during recovery via wireless and public connections (such as the Internet).

Midwest Floods of 1993

In 1993, the Midwest experienced great floods that not only resulted in businesses being submerged under water, but an even larger number of businesses on dry higher ground in Des Moines, Iowa having no water (because of contamination of the public water supply) and no electricity for several weeks. Because this occurred during a sweltering July, these businesses had to adhere to health and fire safety requirements such as not allowing people above the third floor of a building and not having more than a set number of people in these temporarily non-air-conditioned buildings with no running water and only outdoor portable toilets. Even under these adverse conditions, systems were restored quickly to get business going, but most often without the full set of access controls. In addition to this, only a fraction of workers were brought to facilities to work, leaving the bulk of the employees to work in makeshift areas such as

churches and schools and from their own homes.

Privacy Issues

- Ad hoc sites were established to continue business with no physical access security to personal information and computing hardware in place.
- Systems were restored quickly under emergency conditions that did not restore the restricted access controls to protect PII.

Hurricane Andrew

Hurricane Andrew hit Florida August 23, 1992, destroying 35,000 homes and damaging 30,000 others. In Homestead, Florida, alone, one in seven businesses closed and never reopened. The hurricane cost insurance companies \$16 billion in claims, putting ten small insurance companies out of business. Neighborhoods had to be evacuated quickly, leaving business facilities vulnerable to looters, who soon arrived to take what they could from the buildings. Under such adverse conditions, even some usually law-abiding citizens quickly decided to loot whatever they could take from businesses.²

Privacy Issues

- Items stolen and looted after the hurricane likely included PII from the businesses, which subsequently could have resulted in fraud, identity theft, and other crimes.
- The PII from the businesses that had to close could subsequently have been misused, sold to other businesses to recoup some of the losses, or abandoned and left for others to find and misuse.

An Accident in the Midwest

Mundane incidents occur every day that require recovery and put information at risk. For example, in 1996, the paper shredding disposal company used by a large multinational financial and healthcare company did not securely lock the lid of its truck used to

As a result of the 9/11 attack, all ways to determine where PII was stored were lost, creating the risk of misuse of that information because the oversight was no longer in place.

Thousands of papers containing what looked like customer PII were blown through the streets of the city.

haul the papers to the shredding location. The lid opened while the truck was being driven through a major city during business hours, and as a result, thousands of papers containing what looked like customer PII were blown through the streets of the city.

In reality, the information was dummy data used for training purposes. However, to the people who saw the papers, they looked like the real statements they received in the mail from the financial company with real customer information. The financial company dispatched all their physical and information security personnel into the streets to collect the papers. They then confirmed with the area where the papers originated that the number of papers collected closely matched the number of papers thrown away. The rest of the day and all the next day the information security personnel reviewed each paper and verified the PII on each sheet did not match any real customer information.

The day of the incident the television stations ran it as their lead story. The second night, after it was verified that no real customer information was contained in the documents, the television stations reported this as a brief update to their original story. Subsequently, the financial organization contracted with a new shredding company that brought mobile shredders on site on the collection days, and it implemented new procedures requiring personnel to be present and observe when paper documents were shredded to ensure all papers were successfully destroyed while on site.

Privacy Issues

- If the information on the papers had been real, people on the street could have learned about others' financial records and healthcare activities and misused this information.
- The impact on the financial company from the adverse publicity could not be measured, but it certainly did not improve the company's image and likely resulted in loss of trust in the company to adequately handle customer information.

WHAT SHOULD YOU BE THINKING ABOUT?

While reading the prior examples you likely thought of more issues than were listed. That is good! You are now in a good frame of mind to consider aspects of disaster recovery and the privacy topics associated with each.

Controlling Access During a Network Recovery

One objective of disaster recovery is to minimize risk to the organization during recovery. This includes minimizing the risk to privacy. For example, if an automated call distribution system is implemented to permit continued operation of the business, it should not expose the company to undue increased risk. The systems must provide a baseline set of access controls to prevent intrusions during the recovery period and to ensure adequate identity verification of customers calling to request access to their information.

To protect privacy during network recovery, one must know the information repositories containing PII that are necessary for the recovery effort. It is vital that the company have in place an inventory identifying the PII used within the organization, where it is stored, and who should have access to each PII item.

The communication methods created during recovery should not put information and privacy at risk. If wireless, personal Internet, public kiosks, and other types of remote access methods are used as part of the disaster recovery process, or PII is processed from mobile computing devices such as PDAs, laptops, and Blackberry devices, then controls must also be implemented to ensure privacy and security are not compromised during their use.

Controlling Facilities and Physical Access

One of the most effective means for limiting the damage from a malicious act, which would potentially result in a privacy incident, is to limit access to the recovery data center and its periphery, including the floors

above and below the data center and the adjacent areas. This is often either ignored or overlooked during the recovery process. When different computer operations locations are used during recovery, be sure to restrict access as much as possible in these temporary locations to ensure unauthorized persons cannot enter the areas and access PII. Such precautions also help to secure and reduce risk to the makeshift data center environment. These recovery physical access controls should also be implemented to limit entry to communications facilities to authorized personnel only. Of course the first priority during recovery is to protect human life, so be sure the physical controls will allow the people in the temporary data center to exit in an emergency without being locked in.

Communications equipment is often stolen under normal business activity. The risk of theft in a disaster could increase dramatically depending on the type of disaster. Certain types of computing devices have high resale value, not to mention the value of customer information files stored on them. Servers out in the open are prime targets for a wide range of threats, from innocent tampering to outright theft. A thief, in stealing a server, gets away with not only an expensive piece of equipment but a potentially great amount of information, which may be several times more valuable and marketable than the equipment. For example, a 2002 study³ found that the average financial loss for a laptop is \$89,000, with only a small percentage of this amount actually relating to the hardware cost. The loss of information and the impact on the privacy of others could be as devastating as the disaster itself.

Many organizations have inordinate amounts of PII on printed documents. During recovery, address the storage and recovery of vital paper records. Who can obtain access to the sensitive papers in the recovery areas? What will you do if all the sensitive papers are spread throughout the countryside? How will you know if the papers were destroyed or if they got picked up by the

public? In disaster recovery planning, consider using scanning technologies for critical documents, and store the digitized documents in a secure off-site location. Such digital representations can then be used to help account for the location of the physical documents following a disaster, and thus help determine whether the privacy of the associated documents is at risk.

This just touches the tip of the privacy iceberg for physical security considerations. Other physical security issues and considerations that affect privacy include:

- Printed files and storage media access
- Electronic card access systems
- Closed-circuit television
- Security guards and hours of coverage
- Intrusion alarms
- Restricted access areas
- Locations of windows and doors
- Security systems connected to police, fire, and security service
- Limited number of access paths, such as doors, to the operations recovery area
- Sign-in logs
- Visitor badges and escort practices
- Data classification

Legal Privacy Requirements

Privacy-related laws worldwide require that organizations restrict access to PII to only those who have a need to know to perform legitimate business activities. When recovering from a disaster, systems and operational facilities are often restored without such granularity of access control with the intent that when activities get “back to normal” the controls will also be modified to appropriately limit who has access to PII. Unfortunately, historically, changes to the emergency mode of computer operations have not been restored to more restrictive controls for months, and sometimes even years, following recovery, if they get changed back at all. Once a business is back up and running, it is easy to put all efforts toward continuing business as usual and trying to make up the lost time, and not expend resources on more appropriately securing

Servers out in the open are prime targets for a wide range of threats, from innocent tampering to outright theft.

The global trend is to hold company leaders accountable for noncompliance.

the network. How much time following a disaster is it allowable to not be in compliance with the applicable privacy-related law requirements, if indeed any time at all is permissible?

The large and aggressive expansion of legal and regulatory initiatives that address privacy considerations in the United States include the Sarbanes–Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm–Leach–Bliley Act (GLBA), and internationally such regulations as the European Union Data Protection Directive and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), to name just a few. This expanding universe of standards and regulations requires a comprehensive business continuity management program to manage the risks of an organization, help ensure continuous availability of services and products, protect assets, and keep management aware of standards and regulations that may impact the organization in a negative manner if not addressed properly within disaster recovery plans. The global trend is to hold company leaders accountable for noncompliance. Professionals in business continuity, security, and other risk management positions, especially auditors, should be aware of the latest standards and regulations as they carry out their responsibilities.

Consider HIPAA as an example; the Privacy Rule and the Security Rule require covered entities to establish adequate safeguards, which include disaster recovery plans, that address and ensure the privacy of protected health information (PHI). Even before HIPAA, legal action was taken when medical records got into the wrong hands. Cases of PHI being misused, such as a patient’s HIV status being published in newspapers, have become more widespread. With such types of information at increased risk during recovery, the organization is at increased risk for fines, penalties, civil suits, and criminal charges if these legal issues were not appropriately addressed within the recovery plan.

The Amount of PII Detailed Within Disaster Recovery Plans

The personnel on the disaster recovery team often need access to information about most, if not all, of the employees in the company. The information typically shows where to contact people and provides their alternate contact numbers, such as parents’ or in-laws’ houses. To preserve your employees’, and their alternate contacts’, privacy, controls must be in place and enforced that detail the conditions for using the call and recall lists.

To help address this privacy concern, some organizations keep the personnel contact lists in sealed envelopes. When the recovery leader activates the disaster plan, these envelopes are marked with the date, circumstance, and name of the person accessing the information. Other companies keep the call and recall contact lists on a CD, which is accessible to the recovery leader and used on the leader’s computer, from which recovery processes are activated or recorded. However, a printout is kept too, in case of dead batteries, corrupted disks, electromagnetic pulse, damage to the computer because of acidic fumes or volcanic ash, or other adverse circumstances.

If you can demonstrate and ensure the privacy of individuals, it will be easier to get the information you need from all of the employees. The recovery team is also more likely to obtain updates from personnel who move or change telephone numbers. Some personnel might not want to provide such PII because of abusive spouses, lingering privacy concerns, or other reasons. Phone numbers for essential recovery personnel should be confirmed by periodic communications tests that validate the information provided.

Access to Backup Media

Backup media can contain massive amounts of PII. An organization must establish a process to identify the media that contain PII and clearly detail how privacy and integrity will be managed during recovery. Workstation-based information is one of the greatest

vulnerabilities for most companies, because so much vital information is stored locally on these workstations with little or no backup. If individuals have taken the precaution of creating backups, they are typically stored right next to the workstations, creating privacy risks and leaving the company exposed to any type of catastrophic disaster. The company must proactively address this issue through policies and procedures and by providing solutions for creating and storing effective workstation backups.

Disaster recovery planners must decide when and how often to take backups off site. Depending on the company's budget and any regulatory or contractual requirements, off site could be the building next door, a bank safety deposit box, the network administrator's house, the branch office across town, or a secure media vault at a storage facility maintained by a company that specializes in off-site media storage. After separating the backup copy of PII from the source within the company, organizations must address the accessibility of the off-site copies.

There are many factors in safeguarding PII. If it is kept at a branch office or at the network administrator's house, where is it stored in these locations? How is the information put at risk during data transfer? How are the backup media transported to the off-site location? Are secondary backup sites used? If so, how are security and privacy issues addressed?

Public Conversations about PII

During disaster recovery not only do many businesses need to perform work in ad hoc work locations, but personnel also spend much of their waking days discussing with colleagues the details of the recovery. Oftentimes these discussions happen over lunch, dinner, or coffee at a nearby café or through cell phone discussions while traveling in airports or running personal errands, such as buying groceries, taking children to school events, and doing other activities in

public spaces. It is surprising to me the amount of confidential information people are willing to divulge over the phone.

Over the years, I have heard through such megaphone levels of voices way too much PII, without trying, just during a typical day. I first started noticing this phenomenon a few years ago. While I was sitting in an airport terminal waiting to board, an extremely professional-looking young man sat down next to me, whipped out his cell phone, and started detailing in his outdoor voice his just-completed visit to a CISO in that city. I happened to know the CISO, and, given the traveler was sitting within two feet of me, I heard every detail of his visit to my professional colleague. The irony is that he was from a large information security consulting company (he mentioned his company's name during the conversation), and he was detailing what he had discovered about this large potential client's network security system and plans during his meeting: the firewalls used, the number of nodes, the operating systems, and other technical points. He went on to discuss the company's security budget, along with his opinions of the information security management members — not all flattering. No, I did not say anything to this young man; I boarded the plane while he was still talking. However, I did call my CISO friend and let her know that I knew quite a bit about her company's information security based on this man's public discussion I could not help but overhear in the airport. I imagine that impressive young man wondered why his "sure thing" client never signed the contract.

Something similar could quite easily happen during disaster recovery. How many companies have unknowingly lost substantial revenue during the normal course of business from similar divulged information and careless conversations? Most customers will be somewhat sympathetic to your disaster situation, but if their PII is involved, they do not want you to create another personal disaster for them by not preserving their privacy.

Workstation-based information is one of the greatest vulnerabilities for most companies.

Organizations must be careful about sharing information with other businesses and government officials; in particular, they do not want to end up, as a result of the request, integrating private sector and government databases.

Making Others Custodians of PII

Oftentimes third parties are contracted to assist with the recovery process. Backup media are often stored at a vendor site specializing in such a service. Companies often contract with vendors to use their cold or hot sites for recovery. Some businesses arrange with other companies to use part of their computer facilities during recovery. Another aspect is the sharing of information with government and law enforcement after a disaster. For example, after a terrorist attack, a company may be asked to share e-mail messages or access logs with investigators. Organizations must be careful about sharing information with other businesses and government officials; in particular, they do not want to end up, as a result of the request, integrating private sector and government databases. There are ways to do it right and ways to do it wrong; the wrong ways can jeopardize the privacy of PII.

A company may have third parties already performing activities involving PII; for example, using a service bureau to process payroll. Payroll must usually be paid either every two weeks or semimonthly. Depending on when the payday falls in relation to the disaster, and whether or not the disaster also affected the service bureau, this might be a pressing concern, or there might be a week or so to prepare. If a service bureau does payroll, the company should test getting backup payroll and banking information to it. The following questions should be answered: What exposures to employee privacy (related to payroll processing) were created during the disaster? If the disaster happened the day before payday, the recovery time goal for this function would be much shorter. Could accounting personnel work in a rented hotel room or boardroom if hot or warm site facilities were not available right away? During a wide area disaster, could they work in a tent or trailer? If local banks were crippled by the same disaster, could the company pay

employees in cash brought from outside the local area? What security arrangements would be necessary? Payroll is an essential task. Ensure all privacy concerns are addressed.

KEEP PRIVACY CONSIDERATIONS IN MIND FOR DISASTER RECOVERY

This article has touched on just a few of the disaster recovery issues involving privacy concerns. Other issues with privacy implications include, but are not limited to, the following:

- The use of hot sites and cold sites
- How surveillance is used during disaster recovery
- The types of investigations that may occur during or following recovery
- The disaster recovery promises that exist within the Web site privacy policy
- Maintenance of privacy during recovery testing
- Testing of recovery scenarios where PII is most at risk
- Verification of work following recovery to ensure privacy issues were not overlooked during the stress of the recovery activities
- The response to privacy incident disasters, such as stolen customer files from laptops or PDAs

The bottom line is that the company needs to build information privacy and security activities within its documented disaster recovery plans and procedures that address these issues as they apply to the particular organization.

Notes

1. CNET News.com, September 12, 2001, <http://news.com.com/2100-1023-272901.html?legacy=cnet>
2. *Looting — Neighbors Cruising for Your Goods*, Rhema Publishing, <http://members.aol.com/ken-inga/looting.htm>
3. 2002 Computer Security Institute/FBI Computer Crime & Security Survey.