# CONVERGING INFORMATION SECURITY AND PRIVACY ACTIVITIES DURING BUSINESS CONTINUITY

BY REBECCA HEROLD

What kinds of disasters are looming ahead for your business? What kinds of business interruptions will you need to deal with tomorrow? Of course we do not know the answers to these questions. But what we do know with certainty is that whenever business interruptions and disasters occur, information and associated access is impacted in one way or another. And when information and access are impacted, so are the safeguards around that information. When the information is personally identifiable information (PII), such as found in customer databases and employee files, privacy also becomes an issue you must address.

## Have You Prepared To Address Security And Privacy?

Businesses, of all sizes and in all industries, possess a staggeringly large amount of PII. It is more important than ever before for organizations to be able answer the following:

- Under which circumstances and representations was the PII collected?
- How is PII being used?
- With whom is PII being shared?
- How is PII being stored?
- Who has access, authorized or not, to PII?

Unfortunately, many, if not most, businesses do not know the answers to these questions even under normal business circumstances. The first priority for a business following a disaster of any size or type, after getting everyone safe, is usually to get the most critical parts of the business going again as soon as possible. Business resiliency (keeping business going during disruptions exactly as it would under normal circumstances) is a top priority for most organizations. Unfortunately, as a result, disaster plans often address speed to recovery, overlooking information security and privacy issues; this results in significant risks to PII.

When the unexpected happens, you can minimize business interruptions while also ensuring PII remains appropriately protected by ensuring information security and privacy leaders have collaborated on some very important business resiliency issues.

## What Should You Be Thinking About?

When establishing business resiliency plans, it is important to include input from the information security and privacy areas. Consider some of the common aspects of disaster recovery and business resiliency and the related data protection issues associated with each.

### Controlling Access During Network Recovery

An objective of disaster recovery is to minimize risk to the organization during recovery. This includes minimizing the risk to privacy. There should be a baseline set of documented access controls to use during recovery activities to prevent intrusions and privacy breaches during the recovery period.

To help protect privacy during network recovery it is important to know the locations of the information repositories containing PII necessary for the recovery effort. The privacy office must have clearly defined the types of information that qualify as PII. The information security area must know where all those information items are located and then provide appropriate access controls. There may be different types of access allowed during network recovery, but these exceptional access capabilities must be replaced when normal business functions resume.

#### Privacy and Information Security Convergence Areas:

- Identifying information that is considered to be PII
- Maintaining an inventory of PII storage locations
- Documenting appropriate access controls to PII during recovery and continuity activities

### Controlling Access to Mobile Computers

Mobile computers are increasingly used for regular business activities. During a disaster or business disruption of any type, they are used even more. Businesses often allow employee-owned computers to be used. The increased use of these mobile devices during such times should not put information and privacy at unnecessary risk. If wireless, personal Internet, public kiosk, 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 mobile computers and smart phone devices, then controls must also be implemented to ensure privacy and security are not compromised during their use.

#### Privacy and Information Security Convergence Areas:

- Document the PII items that can and cannot be stored on mobile computers and electronic storage devices
- Document PII access and security controls to use during business resiliency activities

### 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 edges, 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 alternate 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 will also help to secure and reduce risk to the make-shift data center environment. These physical access controls during recovery activities 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 these physical controls will allow those in the temporary data center ways to exit in an emergency without being locked in.

#### Privacy and Information Security Convergence Areas:

- Identify the locations of equipment containing PII
- Identify the locations of repositories of printed PII
- Establish physical access control requirements for the equipment and print repositories during business resiliency activities
- Determine if installing surveillance, such as closed circuit television, is appropriate for these areas to minimize security and privacy risks

### Controlling Access to Backup Media

Backup media can contain massive amounts of PII. For example, on February 27, 2008, the Bank of New York (BNY) Mellon lost six to 10 unencrypted tapes while it was transferring backup tapes that contained names, addresses, birth dates and Social Security numbers of over 12.5 million of their customers. They are still paying for that incident.

An organization must establish a process to identify the backup media that contains PII and clearly detail how privacy and security will be managed during recovery. Endpoint-based information, such as on workstations and on mobile computers, is one of the greatest vulnerabilities for most companies. There is so much vital information stored locally on these endpoints with little or no backup. If individuals have taken the precaution of creating backups, they are typically stored right next to the endpoints, creating privacy risks and leaving the company exposed to any type of catastrophic disaster. The company must proactively address this issue through policies, procedures and through providing solutions for creating and storing effective endpoint backups.

#### Privacy and Information Security Convergence Areas:

- Establish policies and procedures to secure PII on backups, including encryption and access controls
- Document how to effectively make PII backups for not only central repositories, but also endpoints
- Document when and how often to take backups off-site
- Document how to effectively secure PII backups at off-site location

continued on page 76

CONTINUED FROM PAGE 75

### SOME PRIVACY AND INFORMATION SECURITY CONSIDERATIONS

Controlling access during network recovery

Controlling access to mobile computers

Controlling facilities and physical access

Controlling access to backup media

Limiting public conversations about PII

Making others custodians of PII

## Limiting Public Conversations About PII

During disaster recovery many businesses not only need to perform work in ad hoc work locations, but they also spend much of their waking days discussing with colleagues the details of the recovery. Often times these discussions happen over lunch, dinner or coffee at a nearby café, through cell phone discussions while traveling in airports, or while also trying to run personal errands such as buying groceries, taking children to school events and doing other activities in public spaces. I've been in coffee houses during flood recoveries and have seen and heard individuals on computers and discussing…loudly…very sensitive information. It continues to surprise me the amount of confidential information people are willing to divulge in public places and over the phone.

### Privacy and Information Security Convergence Areas:

- Include privacy and security issues, such as public meetings and computer access, within disaster recovery and business continuity training
- Provide regular and ongoing awareness communications about not discussing PII in public, along with any of the many examples of how such actions have resulted in privacy breaches

## Making Others Custodians of PII

Oftentimes third parties are contracted to assist with recovery and continuity processes. Backup media is often stored within a vendor site specializing in such services. Companies often contract with vendors to use their cold or hot sites for recovery. Some businesses have arranged with other companies to use part of their computer facilities during recovery. Information is often shared with government and law enforcement after a disaster. For example, after a terrorist attack, a company may be asked to share email messages or access logs with investigators. Organizations must be very careful about sharing information with other businesses and government officials, or with actually ending up, as a result of the request, putting the PII from the company into government databases. There are ways to do it right, and ways to do it wrong that jeopardize the privacy of PII.

### Privacy and Information Security Convergence Areas:

- Identify and document all third parties contracted to help with business resiliency activities
- Ensure appropriate security and privacy requirements are included within the contracts
- Implement policies and procedures to involve information security and privacy areas when law enforcement and other investigators want access to PII to ensure such information sharing is appropriate, and that necessary controls are established prior to sharing

## Keep Privacy and Information Security Considerations in Mind

These just touched upon a few of the business resiliency issues and situations that require the involvement of both the privacy and information security areas. Other issues that should incorporate the advice and direction of information security and privacy experts include, but are not limited to, the following:

- The use of hot sites and cold sites
- How surveillance is used
- The types of investigations that may occur during or following recovery
- The disaster recovery promises that exist within the website privacy policy
- Maintaining privacy during recovery testing
- Testing recovery scenarios where PII is most at risk
- Verifying work following recovery to ensure privacy issues were not overlooked during the stress of the recovery activities
- Responding to privacy incident disasters, such as stolen customer files from laptops or USB storage devices
- Using PII within electronic messaging for business resiliency communications
- Remote access controls during recovery and resumption
- Access to phone and voice mail systems
- The use of virtualization systems
- Using cloud computing for emergency and resumption activities

The bottom line is, you need to heed the advice and recommendations of the information security and privacy experts when creating disaster recovery, business continuity and other business resiliency plans and procedures. Your plans will then not only be effective in application, they will also protect PII and meet many legal requirements.

### ABOUT THE AUTHOR

Rebecca Herold, CIPP, CISSP, CISM, CISM, FLMI, "The Privacy Professor," has over two decades of information security, privacy and compliance experience. She's been named on Computerworld's "Best Privacy Advisors" list for the past two years. Contact her at rebeccaherold@rebeccaherold.com or www.theprivacyprofessor.com.