21st Century Incident Response
Incident Response Process Automation

JUNE 2011
Introduction

The business continuity and disaster recovery (BCDR) focus of the 1980’s gave way to widespread understanding and creation of written business continuity plans (BCP). A natural evolution of BCP was the realization that different events or incidents require different responses. In particular, the explosion of cyber-crime and data breaches over the past decade demonstrates the need for unique incident response.

Most organizations today are proud of the incident response plans that they have created. Some actually test the plans with tabletop exercises, and the unfortunate have executed the IRP due to actual incidents. From the execution of IRP’s and lessons learned, it is clear that information security incidents require process-driven tools to ensure a consistent, defensible, and thorough response. **Serious** consequences from incidents are rare (despite the fear propagated by sensational news headlines), and security professionals deal with hundreds or thousands of minor events and false positives each day. For these reasons, it seems like having just a conventional, written, incident response plan is enough.

This whitepaper will briefly look at key current events, heightened enforcement of regulations, and increased litigation which clearly indicate the need to do more and to do better. In addition, this whitepaper will give precise guidance on the requirements of automated, process-driven incident response applications. Finally, a Chief Security Officer (CSO) will give valuable insight on the real value derived from incident response process automation and how she applied this type of application in the trenches of actual incident response.
Current Events

Sony Online Entertainment America Data Breach

Between April 17\textsuperscript{th} and 19\textsuperscript{th} of 2011, over 100 million registered users of Sony Online Entertainment and PlayStation Network had their accounts breached in two separate incidents. The results have been the temporary shutdown of both services for Sony customers and a public relations nightmare. On top of the incalculable dollars this will cost, Sony has had to respond to the scrutiny of the U.S. Department of Justice, various state attorneys general, and Connecticut senator Richard Blumenthal questioning the timeliness of the notification of the public by Sony\textsuperscript{1}. Sony notified customers on April 26\textsuperscript{th}, only seven days after the first suspicious activity.

Given the magnitude of the breach, the laws of physics, and the complex nature of the investigation, seven days seems positively miraculous to information security professionals. The forensic imaging alone of mammoth servers certainly consumed a large percentage of that time. This breach demonstrates that Security Incident Response Teams (SIRT) must work flawlessly under near impossible time constraints and be able to document down to the very minute every action and decision made every step of the way from discovery to containment to remediation to notification.

HIPAA/State Data Breach Laws/Future National Laws

From the alphabet soup of healthcare industry legislation, it is clear that regulation of this industry is seen as critical to lowering costs and maintaining quality patient care through the adoption of

\textsuperscript{1}

http://www.sony.com/upload/assets/homepage_assets/Letter_to_Bono_Mack_and_Butterfield_5_3_11.pdf
Electronic Medical Records (EMR). From its inception, the Health Industry Portability and Accountability Act (HIPAA) was not viewed as having significant teeth. However when President Obama signed into law the American Reinvestment and Recovery Act (ARRA), a specific area of the law changed that. The Health Information Technology for Economic and Clinical Health Act (HITECH) in part strives to ensure security throughout the industry, increase enforcement, and requires breach notification according to certain thresholds and risk of harm. Possibly the most significant change is regarding enforcement authority. Under HITECH, the Privacy and Security Provisions of HIPAA are now extended to the business associates of covered entities. Covered entities must report certain breaches of patient health information (PHI) to the Department of Health and Human Services (HHS) Office of Civil Rights (OCR), individuals, and in some cases, the media. Such broad notification requirements have led to wider scrutiny of incident response practices by state attorneys general who, under HITECH, now have the authority to bring actions for damages on behalf of their state residents and enjoin further violations of HIPAA. In April, 2011, training began by the OCR for state attorneys general in HIPAA enforcement. Specific areas of training include investigation techniques, identifying and prosecuting alleged violations, and resources for enforcing HIPAA and HITECH. Attorneys general in Vermont and Connecticut were among the first to begin enforcement actions under HIPAA.

With the OCR requesting nearly $10 million in the 2012 federal budget for HIPAA enforcement, including the hiring and training of regional privacy officers as well as increased investigation of

breach reports, it's clear that the paper tiger of HIPAA now has some very big teeth. The HHS's own website\(^4\) lists numerous recent examples of various resolution agreements resulting in fines and penalties of millions of dollars levied against hospitals, insurers, student health centers, medical and dental practices, and other covered entities.

We've now reached the point in data breach laws where almost every state has one. All require notification to affected individuals, a few provide safe harbor for encrypted data, and one regulates the data of their state's residents even when the data is held in another state. This patchwork of laws has created a drum beat for a national data breach law. It is reasonable to assume that sometime in the next 18-36 months we will see a federal law to supersede the patchwork of state laws. Due to the fact that every state law, security guideline, certification, and framework invoke incident response, one can safely surmise that incident response program scrutiny will only continue to intensify for the foreseeable future.

FRCP and E-Discovery

Traditional incident response thinking has focused solely on security incidents related to preventing, detecting, and remediation of data breaches. While this conventional wisdom is correct, it is far from complete. An incident should be viewed in today's organizations as *any event which presents risk to the organization*. When that risk involves data, it should be included in the incident response plan, with clearly documented processes, work flows, and accountability. For this reason, litigation and the associated

\(^4\) [http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html](http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html)
holds, preservation, collection, searching, and production need to be part of today's incident response programs.

In the past two decades, electronically stored information (ESI) has presented ever increasing challenges to civil litigation. Nearly every organization, business, and individual in the country possesses ESI in one form or another. When disputes arise, be they personal or business in nature, evidence has increasingly come in digital form from electronic media and devices. This monumental change in the way information is processed, stored, transmitted, and used presents unique and evolving challenges for our legal system. The Federal Rules of Civil Procedure have governed the procedures for civil litigation in the United States since 1938. Various changes and amendments have taken place over the years, but in 2006, substantive changes were made to specifically address the unique challenges that ESI presents in the pursuit of “just, speedy, and inexpensive determination of every action”.

Landmark cases such as Zubulake v. UBS Warburg (five opinions between 2003 and 2005), and the more recent The Pension Committee of Montreal, et al. v. Banc of America Securities, et al span nearly a decade and are excellent examples of why e-discovery must be treated as a defined process. While great legal minds debate and study these cases, incident response practitioners would do well to give them attention as well. The clear, redundant theme throughout regarding ESI is that ad-hoc methods will not be tolerated by the courts and may result in negative outcomes to either party in legal matters. While it can be argued that the Zubulake decisions were very early in the evolution of e-discovery and therefore mistakes were understandable, by the time we get to the Pension Committee decision of 2010, it is clear
that policy, procedures, training, and documentation are the minimum requirements for competent preservation, collection, searching, and production of ESI.

Fortunately, the E-Discovery Reference Model (EDRM) and the Sedona Conference are two organizations which have led the charge in e-discovery processes and best practices. An excellent example of the process-driven nature of e-discovery is the following illustration from the EDRM:

By taking the lessons learned from case law, the FRCP, and the EDRM, process-driven work flows for particular types of e-discovery matters can be created in any organization.

The Sedona Conference is a great resource for further information on e-discovery best practices. Their publications, conferences, and seminars offer a wealth of information and provide the methodologies behind each step of the process depicted above from the EDRM.

5. [http://www.edrm.net](http://www.edrm.net)
A 21st Century Incident Response Management Program

A Plan to Withstand Scrutiny – Defensible, Repeatable, Holistic

The ever increasing corporate responsibility to protect institutional data has created the requirement for a codified, process-driven incident response program. Incident response should not be viewed as a corollary responsibility of the IT department; it must be its own entity with its own charter. The incident response program should be designed to achieve the following organizational objectives:

- Guarantee rapid cohesive and consistent responses to incidents
- Minimize disruption to normal business operations
- Protect the organization's reputation, brand, and information assets
- Establish controls for accessing and distributing incident information
- Ensure proper documentation of incident response efforts
- Promote the accumulation of and accurate reporting of, incident information
- Empower senior management with knowledge

No longer is it sufficient to handle incidents in a casual, ad hoc manner. Today's incident response program must be laser focused; designed to react and minimize damage quickly and effectively. It is important to determine what actions will be taken,
who will approve these actions, who will perform these actions, and who will be informed of the results of these actions prior to an incident actually occurring. This way, when a crisis strikes, the team is prepared to respond quickly and decisively. The elements of a well crafted incident response program include the following:

- **Creation of an Extended Incident Response Team** - many departmental groups support incident response; departments such as computer operations, human resources, and legal. It is important to have liaisons in these departments who understand the function of incident response and can facilitate the cooperation between their departments and the core responder team.

- **Consistent Prioritization and Escalation of Incidents** - often the priority given to an incident is based on how difficult it will be to return to a normal operating state. It is vital to use true business drivers as the parameters for prioritizing (or reprioritizing) an incident. For example, which is more serious; a virus outbreak impacting 200 machines or the loss of the CFO's laptop computer?

- **Defined Communications Channels** - it is critical to keep appropriate individuals and groups appraised on the progress of a response effort. The decisions regarding which individuals and groups will be informed should be made in advance.

- **Recognition of Internal Response Capabilities** - it is important to make an honest assessment of your organization's overall response capabilities. Generally, not all the capabilities will be in-house; it may be cost effective to
have portions of this, such as computer forensics or breach notification, out-sourced.

- **Proscribed Response Playbook** - this playbook details the actions to be taken, based upon the incident type and severity. Not all permutations of incidents can be anticipated, and provision must be made for professional judgment to be used, but the playbook should be able to provide detailed instructions on the vast majority of all incidents.

- **Built in Feed-Back Loop** - the program should include both self assessment and input from other groups to help improve and evolve the overall response efforts.

There are two methods which can be employed to implement the program. The most common is to define it through a series of documents and then administer it through a group of spreadsheets, email, or stand-alone databases. The other is to manifest the written program utilizing an enterprise software tool specifically tailored to facilitating an incident response program. The tool should be web-based, allowing easy access to authorized users while protecting the sensitive information that it will contain. While both approaches can be effective, there are advantages to utilizing an electronic tool; advantages that allow the response team to focus its efforts on the incident rather than the administrative tasks accompanying the response. These advantages include the following:

- **Facilitating Communications** - a tool can automatically notify appropriate individuals and groups about the status of incident response efforts. It can also simplify collaboration between the various departments participating in the incident response.
21st Century Incident Response

Incident Response Process Automation
JUNE 2011

- **Enforcing Corporate Policy** - a tool can be configured to require appropriate approval before allowing the release of incident information or commencing specific response actions.

- **Centralized Repository** - a tool can serve as a central repository for all incident response information. This facilitates tracking incident trends, allowing the organization to be more proactive in its preventive actions. As the central repository, all members of the response team can request and deposit information directly in the tool, greatly reducing or eliminating the amount of sensitive information being transferred in open emails.

- **Automated Documentation** - a tool can provide real time documentation regarding the progress of an incident investigation. This allows interested parties to obtain the information and updates they require without interrupting the responders. It also frees the responders from the tedious task of post-resolution documenting of the incident.

- **Dashboard Views** - a tool can be configured to provide a variety of useful dashboard views. For the individual responder, this view would include incidents and tasks for which he/she is responsible. And for the executives, the dashboard would graphically highlight those incidents which are of a serious nature, requiring additional attention.

Whichever approach an organization chooses, it is vital to spend time thinking about the incidents that could occur and having a plan of action prior to having an incident.
Incident Response Process Automation

A strategic, process-driven incident response application can make the difference in how much exposure an organization suffers during a crisis. The effective handling of an incident or crisis can make all the difference to a CSO’s career as well. Here is a summary of a typical scenario:

Friday afternoon at the end of June, 4PM, many employees and senior managers are starting vacations or heading out of town early. Your CSO is hoping to join their ranks when the phone rings. The authorities have tracked fraudulent activity impacting thousands of consumer credit cards, which appears to have started from a breach within your company.

The prepared CSO gathers the necessary information, scopes the issue to assess risk level and determines who needs to be notified and who needs to be assembled, simplified through use of an incident response process application. All primary members of the incident response team are alerted and on a conference call within 30 minutes. Lawyers make the necessary determinations as to whether there needs to be public notice, the CTO works with the incident response investigators to ensure they can gather data. The heads of the business assess what instructions need to be delivered to employees, call centers, public relations, etc. The incident response process has kicked in and all involved will work around the clock through the weekend.

The CSO can confidently call the CIO on his cell. This is part of the process automatically determined by the risk level warranting that level of notification. Regular status calls take place over the weekend so that by start of business Monday, all incident response members have their marching orders. An ongoing review of the automated dashboard helps to prepare the key members of the
incident response team for briefing the management in their chain of command. All updates and data collected are reflected in the system, which ties incident responders to a central point for consistent updates and reporting.

During an incident, the need for process, speed and ease of execution is critical. Delay or indecision at any point can have disastrous consequences for the company and inevitably the CSO. There is a famous breach which did not follow the scenario above. Delays and lack of process hindered the company and resulted in a public relations nightmare. The company lost revenue, incurred material expenses related to the breach, the stock price dropped and the CSO was out of a job. Questions around their lack of process, lack of timely notification and improper handling of evidence hurt their credibility and damaged their brand.

At the moment it is clear there is a true incident, the CSO is concerned about:

- Minimizing and containing the damage to the company
- Bringing together the right people and assessing the right risks quickly
- Alerting outside agencies
- Wanting consensus quickly in defining holistic strategy with which to handle the incident
- Having a comprehensive status report ready to brief senior management as needed
- Ensuring customers, employees, and end users have appropriate information
- Staying on top of how the incident response is progressing
A CSO has responsibility for the Incident response process. That includes:

- Identifying the risks, quantifying the impacts, creating the plan and process
- Educating incident response team members and senior management about the process and ensuring they understand key features
- Obtaining support from key functional leaders in Legal, the Business, Finance, Communications, the CIO and Physical Security
- Getting senior management to nominate critical team members and back-ups to participate as part of the incident response team
- Analyzing past incidents and creating appropriate strategies to assist the business in minimizing the exposure of a repeat issue in the future
- Ensuring incident response plans are updated and successfully tested
- Sharing the incident response process with other parts of the organization to help those areas benefit when wrestling with disaster recovery and business continuity planning efforts
- Working with other functions to update risk, SLA’s and severity matrices annually
- Providing necessary updated information to awareness, training and education programs as appropriate
21st Century Incident Response

Incident Response Process Automation

JUNE 2011

- Analyzing and briefing senior management and the Audit Committee as required and on an annual basis

An incident response application was invaluable in saving essential time at every step in the life cycle of the successfully executed incident response described above. From automated notification, to real time documentation and dashboard reporting, everyone on the incident response team can be kept up to date on the status of an incident, as well as ensure critical evidence and data gathered is properly secured and maintained in one place. Having all this housed in a central repository alleviates the need to be emailing sensitive information. Through access control, all access is predetermined and can be confirmed periodically. The right incident response solution, if adhered to, will create an immediate return on investment and shareholder value on its first use.

While e-discovery doesn't necessarily present the same time sensitivity as a security incident, many jurisdictions have strict deadlines for legal matters. Couple this with the lack of understanding by non-technical people of the difficulties in preserving, collecting and searching terabytes or petabytes of data, it's not hard to image how chaotic and pressure-filled an e-discovery event can become at any point. While the technical steps are different for an e-discovery event, there are steps nonetheless. Multiple stakeholders such as legal, executive, HR, and IT all benefit tremendously from automated notifications, real time documentation, and efficient dashboard reporting.
Conclusion

For those few organizations that still exist without an incident response plan, it's simply a matter of time before lack of a plan will result in a "resume-generating event".

For those organizations with a plan that is sitting on a shelf collecting dust, it's time to take another look. A thorough review of the plan will lead to the realization that e-discovery events need to be included, work flows need to be updated or created, and tabletop drills need to be performed for the possible scenarios of risk to the organization.

For those organizations with a well-documented, up-to-date incident response plan: Congratulations – but now's not the time to rest on your laurels! From a plan like this, it is very easy to take the next step and implement an incident response process application custom tailored to your program.

It goes without saying that such diligence in security incident response and e-discovery matters will go a very long way in demonstrating to the courts, regulators, boards of directors and shareholders a serious, competent, defensible program.
21st Century Incident Response

Incident Response Process Automation

JUNE 2011

Angie Singer Keating,
CISA, CIPP, CISM, CRISC

Angie is co-founder and Vice-President of Compliance and Security for Reclamere, Inc. Reclamere is a leader in data security, computer forensics, IT risk management, data recovery, and secure data destruction for a wide variety of highly regulated industries. With over 20 years of experience, Ms. Keating is a popular speaker and author for organizations such as the National Association for Information Destruction (NAID), the Pennsylvania Bar Institute, the International Association of IT Asset Managers (IAITAM), the Pennsylvania Chamber of Commerce, and many others.
Jim Bothe

Jim possesses over thirty five years of experience in the information technology field, with the last fifteen focused in information security. His experiences range from the development of information security strategies and programs to architecting and managing the deployment of information security technology. Mr. Bothe's clients have included organizations in the communications, banking, insurance, technology, retail and manufacturing sectors.

Working with an international Fortune 500 company, Mr. Bothe created, implemented, and operated its computer security incident response program, strongly contributing to the organization's successful PCI QSA audit review. This also became the foundation for Process One™, an industry leading system designed to facilitate the creation and operation of incident response programs and teams.

Mr. Bothe was co-founder of Network Security Consulting, building information security programs for a number of major health care organizations. He co-authored the Common Compliance Framework™, one of the industry's earliest Governance, Risk and Compliance (GRC) systems.
21\textsuperscript{st} Century
Incident Response
Incident Response Process Automation
JUNE 2011

Roseann Larson,
CPA, CISA, CISM, CRISC

Roseann is founder and Managing Director of CSO On Call. \textbf{CSO on Call} provides Fortune 500 IT Risk Management, Compliance and Professional Consulting Services to organizations of all sizes. Ms. Larson speaks on IT Risk Management regularly for Tech Executive Network, Women's Executive Network, CSO Executive Network and contributed a chapter to the Executive Alliance Leadership Series, SECURE.

Ms. Larson has over 20 years of senior executive Fortune 500 experience and the CISO for a Fortune 100. She currently chairs the Audit committee and serves as a Director, on the Board for a San Jose technology firm.