



Security Incident Response Process

**Category:
Information Security and Privacy**

The Commonwealth of Pennsylvania

**Pennsylvania Security Incident Response Process
Nomination for 2008 NASCIO Award**

Executive Summary

The Commonwealth of Pennsylvania is a trusted steward of citizen information. Trust in government is directly related to the quality of service and the sense of security that citizens feel when working with the government. Vital to maintaining that trust is the assurance that security incidents are reported and investigated in a thorough and uniform manner in order to mitigate potential problems and prevent future developments when incidents do occur. In the past year, the Office for Information Technology (OA/OIT), an executive agency responsible for leading and coordinating information technology services and policies in the Commonwealth, implemented enterprise-wide technologies, policies, processes, and procedures regarding incident reporting and response regarding cyber security.

The implementation of a robust incident reporting policy, including a centralized reporting mechanism, helped drive the incident reporting process. The implementation of an automated incident response solution and the formulation of the Pennsylvania Computer Security Incident Response Team (PA-CSIRT) further enhanced the Commonwealth's incident response and remediation process. The combination of these elements has since changed the employee culture throughout the Commonwealth regarding incident reporting and response, has enhanced the rapid dissemination and sharing of vital information, and has further strengthened the security awareness landscape. Pennsylvania's Computer Security Incident Response Process consists of the following components:

- **Security Incident Reporting Policy** – Developed to provide enforcement to all agencies regarding reporting of all incidents cyber in nature.
- **Incident Reporting Mechanism** – Utilizing current enterprise architecture, a Web-based incident reporting form and database for use by all agencies was implemented at no cost, using already implemented technologies.
- **PA-CSIRT** – A team of inter-agency personnel skilled in incident response was formed. Training and cyber exercises were routinely conducted to enhance response skills.
- **EnCase Enterprise** - An automated incident response and mitigation solution was established to enhance the Commonwealth's security incident response and alleviation capabilities to provide for a more standardized, rapid, and coordinated response to incidents.

The development and implementation of Pennsylvania's Computer Security Incident Response Process has provided real and measurable value to the citizens of the Commonwealth. Without a solution in place, it is estimated that a major incident causing a one-day outage would affect 80 percent of the workers of the Commonwealth and would cost approximately \$12 million in lost productivity. The implementation of the automated incident response and mitigation solution has provided for the rapid and proper gathering of digital evidence, better aligning with the direction of the federal government, and has ultimately helped the Commonwealth achieve its business goals and compliance regulations as well as reduce the overall costs associated with incidents.

**Pennsylvania Security Incident Response Process
Nomination for 2008 NASCIO Award**

Description of Business Problems

The Commonwealth of Pennsylvania is responsible for a vast amount of sensitive data and computing resources that are vital to the continuity of government services and operations. The protection of the information and resources from compromise or misuse from either errors or cyber security threats originating from both internal and external sources is vital to maintaining the Commonwealth citizens' trust. While the Commonwealth had taken a proactive approach to identify and mitigate threats through the use of advanced tools, policies, procedures, and training, it was recognized that cyber security or data security incidents may occur on occasion. Instances of involving the destruction, disclosure, loss, damage, misuse, or access to information technology (IT) resources such as systems, files, and data bases, as well as violations of security policies and practices, were all possible. It became clear that consistent and effective incident reporting and response capabilities were vital to carrying out the Commonwealth's main responsibilities.

As a result of externally conducted security assessments, areas involving computer incident reporting and response were identified as deficient regarding the overall security posture of the enterprise. While the Commonwealth had already improved security through the strategic implementation of enterprise security solutions at multiple layers through an over-arching enterprise initiative called Operation Secure Enterprise (OSE), the identification, reporting, mitigation, response, and prevention of all security incidents, cyber in nature, remained an area of challenge. Not only would policies, procedures, and technologies have to be put in place, but a change in culture for how incidents were reported were paramount. The need to implement a consistent array of initiatives while providing guidance and support on an enterprise scale, were vital to ensure timely and accurate incident reporting and a rapid and effective response process once an incident occurred.

Prior to the current efforts, the incident reporting process across Commonwealth agencies was fragmented and inconsistent. Incidents at times went unreported because of the fear of the ramifications of discovery from an incident occurring. This culture of non-reporting ultimately led to significant security concerns and added risk. Because there was no centralized enterprise-wide reporting and response mechanisms in place, agencies took it upon themselves to either not report security incidents when they occurred or kept the information to themselves. Thus, the dissemination of vital security-related information was inconsistent, incomplete, or missing altogether.

Incident response efforts throughout prior years varied tremendously. Because there were no standards and little guidance and training for how to properly identify, contain and mitigate incidents, some went un-noticed. When incidents did occur, resources were frequently limited and response times were not rapid enough to properly contain exposures to a rapidly evolving or imminent threat.

Additionally, because methods previously employed by agencies in responding to computer security incidents varied so greatly, these inconsistencies could end up ruining cases involving personnel or legal issues. For example, if a computer administrator found evidence of unauthorized access to a particular server and logged onto that server in an attempt to identify the intruder, any findings discovered thereafter could be deemed inadmissible because proper

**Pennsylvania Security Incident Response Process
Nomination for 2008 NASCIO Award**

response procedures were not standardized. If an employee was fired or arrested as a result of the findings and a lawsuit followed, the Commonwealth could have a very difficult time pleading its case and a favorable outcome would be unlikely.

Description of Solutions

In 2007 OA/OIT, an executive agency directed by Executive Order 2004-8, *Enterprise Information Technology Governance Board*, addressed the issues surrounding Incident Reporting and Response through a variety of policies and initiatives. These would have a significant impact on the Commonwealth's response and remediation capabilities that changed the employee culture pertaining to incident reporting and mitigation. These solutions include the following:

Security Incident Reporting Policy

When a cyber security incident occurs, it is critical that the incident is properly reported and managed in order to secure and protect the Commonwealth's critical IT resources from cyber-crime or breaches of information. The OA/OIT has established an IT Security Incident Reporting Policy (Information Technology Bulletin (ITB)-SEC024) to set standard policies, reporting, and processes for reporting and managing of cyber security incidents.

Along with the reporting requirement, the policy enabled users to report on incidents encompassing three levels of severity and offered guidance to agencies concerning response requirements. Additionally, upon receipt of the incident information the Commonwealth's CISO could prescribe necessary incident management and investigative steps to aid in containment and remediation, and also after action analysis.

Critical points of emphasis of the policy were centered around notification. Upon the discovery of an incident, the policy stressed that the affected agency's Information Security Officer (ISO) must evaluate the incident in relation to current and potential technical effect, business impact, and criticality of the affected resources, and provide e-mail, Web-based, or telephone notification of the incident to the Chief Information Security Officer by completing and submitting an incident form within four (4) hours of incident detection.

In instances where incidents involved compromised, lost, or stolen data, or any instance of the disclosure of personal information, the policy provided guidance for agencies to ensure compliance with the Breach of Personal Information Notification Act.

To ensure security awareness and education, the policy contained guidelines for agencies to put in place processes for ensuring that all users of agency systems are aware of the procedures and the importance of reporting security incidents, threats, or malfunctions that may have an impact on the security of agency information. To encourage enforcement of the policy, a series of enterprise memorandums was published reminding users of the incident reporting and response process. To provide agencies with the knowledge and tools they needed to carry out their tasks, classroom-based incident response and remediation training was provided to all agency ISOs and designates. Additionally, a PA-CSIRT "hotline" telephone number was established to all agencies with responders readily available to field all questions relating to mitigation, containment, and other agency action.

**Pennsylvania Security Incident Response Process
Nomination for 2008 NASCIO Award**

Incident Reporting Mechanism

The Commonwealth leveraged existing enterprise portal technologies to provide a Web-based vehicle for agencies to report security incidents to comply with the requirements established in the ITB-SEC024 policy, and enabled the agencies to report in a quick, easy, and secure fashion. Utilizing current standards to implement these services, the reporting mechanism was developed and put in place with no associated additional costs. Included notification services within the technology enabled designated individuals to receive instant e-mail alerts when security incidents were being reported, which helped to facilitate a rapid and immediate response for the affected agency.

The implementation of the incident reporting feature has provided a consistent method for reporting and value through the ability for immediate response, including the ability to correlate events from various agencies. Advanced metrics from the data received from security incident reporting forms have uncovered a wealth of information detailing areas of risk or trends.

Pennsylvania Computer Security Incident Response Team

The CISO implemented and formed a team of inter-agency personnel skilled in incident response. The PA-CSIRT was established to formalize reporting of incidents and disseminating incident information with internal staff and agency security personnel. This team of individuals received instant notifications of all submitted incidents. Training and cyber exercises were routinely conducted to enhance response skills. The team was formulated to establish an approved and consistent process, and coordinated efforts for response to address computer security incidents. These incidents include malicious code attacks, unauthorized access to an organization's systems, unauthorized utilization of an organization's services, denial of service attacks, general misuse of systems, hoaxes, or other computer security intrusions or events as defined explicitly in the Security Incident Reporting Policy.

Additionally, a Web site was developed utilizing current enterprise portal technologies to provide the response team with an enterprise view for all security incident reports entered into the system. The PA-CSIRT Commonwealth Web site was established at no cost utilizing the same portal technology as used in the incident reporting form while providing a tremendous benefit to the team with an enterprise searchable view enhancing the response process through the correlation and remediation of cyber incidents and the rapid dissemination of vital information.

EnCase Enterprise

An automated incident response and mitigation solution was established to enhance the Commonwealth's security incident response and mitigation capabilities to provide for a more standardized, rapid, and coordinated response to incidents.

To facilitate this endeavor, the Commonwealth rolled out a one-year production-based pilot program to evaluate EnCase Enterprise in order to test the effectiveness of the automated incident response capabilities by using it to conduct real-world investigations.

During the pilot EnCase Enterprise was used to provide successful incident response for nine major security incidents including twenty-seven forensic examinations and twenty-one

**Pennsylvania Security Incident Response Process
Nomination for 2008 NASCIO Award**

compromise assessments. All investigations were carried out without system downtime and were completely transparent to end-users. The estimated cost savings for one case alone exceeded \$130,000. Systems suspected to be compromised could be analyzed and a determination could be made within hours in the same day.

Forensic capabilities provide a much more robust platform for retracing intruder footprints to determine the origin and magnitude of an incident. Security analysts are no longer only limited to relying on log file analysis. Additionally, security incidents were quickly contained and mitigated as a result of the advanced forensic capabilities such as: volatile data analysis, parallel searching across many systems simultaneously, filtering according to date/time stamps, file type/signature, and by hash analysis.

EnCase Enterprise has helped reduce risk as much as possible and provides a bulletproof enforcement mechanism for holding individuals accountable. The pilot was deemed a success for the Commonwealth because it was able to carry out incident response without disruption to business and in a manner that was timely and effective.

Significance: How did the project improve the operation of government?

Pennsylvania's Computer Security Incident Response Process has had a tremendous impact on all agencies under the governor's jurisdiction. All agencies participate in a consistent process by reporting all incidents cyber in nature to a centralized location. Additionally, inter-agency support and communication has increased dramatically and has facilitated better information sharing between affected parties. Because there are consistent and well defined containment and remediation efforts, agencies are well informed and able to take rapid response and mitigation actions. The speed of the response has had an impact on risk in the Commonwealth and incidents are mitigated and handled more efficiently and effectively. Additionally, the culture has changed dramatically concerning incidents. Agencies are no longer hesitant to report security incidents because they know that they have a strong team-based support mechanism in place to help aid response and mitigation efforts. All this combined has had a positive effect on the security posture of the Commonwealth and has provided a significant value to citizens, businesses, and customers by ensuring that incidents are handled efficiently and properly in the Commonwealth.

Benefit of the Project:

The Commonwealth of Pennsylvania's implementation of a successful Computer Incident Response Process has provided a robust process and methodology pertaining to the Commonwealth's response and remediation capabilities. These additions have not only changed the employee culture in a positive light pertaining to incident reporting, but have added a real value to the citizens of the Commonwealth and are best brought to light by a few case examples of real incidents.

For example, on one occasion, Commonwealth Web sites were infected with malicious code and ultimately brought down for a period of time due to a major attack. Efforts including assisting with and trying to identify the source of the attack, cause of the attack, mitigation of the attack, restoring the sites to normalcy, and implementing proactive/reactive monitoring and preventive measures all contributed to bringing the situation under control very rapidly in ways previously

**Pennsylvania Security Incident Response Process
Nomination for 2008 NASCIO Award**

not possible. Ultimately, the sites were quickly brought back online in a matter of hours, providing assurance to the citizens of the Commonwealth and maintaining their trust in government.

On multiple occasions, proactive measures by the PA-CSIRT have aided in providing real measurable cost avoidance benefits to the Commonwealth taxpayers. For example, in April 2008 PA-CSIRT members found a significant vulnerability in a Commonwealth Internet facing Web application that could have had exposed sensitive records online to the public. The security analyst who discovered the vulnerability was able to point it out to the owners of the application and show that the records had not been breached. If the exposed records had not been caught in time and had been breached, the costs associated with notification to the affected individuals would have been significant. This successful example illustrated how the well-established processes in place helped save the Commonwealth taxpayers \$19 million.

The establishment of and automated incident response solution for the enterprise enhanced the Commonwealth's multi-tiered security approach and incident response and mitigation capabilities. Without a solution in place, it is estimated that a major incident causing a one-day outage would affect 80 percent of the workers of the Commonwealth and would cost close to \$12 million in lost productivity. The implementation of the automated incident response solution has provided for the rapid and proper gathering of digital evidence, better aligning with the direction of the federal government.

The implementation of a successful uniform Computer Incident Response Process has ultimately helped the Commonwealth achieve its business goals and compliance regulations, reduce the overall costs associated with incidents, and provide an inordinate value to citizens. The development and execution of an enterprise Computer Security Incident Response Process has been a critical success factor in allowing Pennsylvania to successfully maintain the highest trust with its citizens and protect the data that it manages.