Recession Calls for Better Change Management

Separation of duties, logging paramount in times of great, rapid change

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI
Final Draft for March 2009 CSI Alert

I've been struck by the noticeable increase in news stories about the "new criminals" that are emerging since the beginning of 2009. People who would never before have considered stealing are now, in these desperate times, taking advantage of situations where they have access to things of value and taking them when they learn that they are losing their jobs, have lost their job, or just have a feeling that job loss is somewhere likely on the horizon.

Many people are feeling desperate and justifying their malicious acts by pointing to the economy, resulting in increasing crime by insiders. Two recent studies support this trend. A December 2008 Cyber-Ark Software study reported that around 60 percent of U.S. workers had downloaded sensitive information from their employer in anticipation of being fired. A January 2009 Ponemon Institute research study found similar results, reporting that close to 60 percent of already terminated employees did, indeed, take their employers' information with them when they left their jobs. And what types of information are most valuable to take? Usually customer and employee personally identifiable information (PII), along with the company's sensitive intellectual property and secrets.

As the economy gets worse the risks to information theft increases. The deepening recession makes it more important than ever before to ensure sound security controls are in place. Change management is one of the areas where controls need to be ramped up, which will also support multiple compliance requirements.

Desperate Times Increase The Crimes

When the economy was good there were plenty of instances of criminals and insiders taking PII to do bad things. The bad economy now provides even greater motivation for people to do even more bad things.

Poor information security practices provide great opportunity for crime to occur. A significant portion of personnel, business partners and others with authorized access to PII will succumb to temptation to do bad things for financial gain if they think they won't get caught, if they feel their job is threatened, or if they believe their employer is mistreating them. Criminals with no authorized access will exploit security weaknesses to obtain PII and use it for their financial gain.

Businesses possess a huge amount of valuable PII, such as credit card numbers, insurance policy numbers, Social Security numbers, banking information, along with names, addresses, phone numbers and other information that can easily be used for identity theft. Criminals can take this information and sell it to other criminals who can then use it in their illegal activities.

Personnel may also purposely sabotage computer systems if they feel their employment is threatened. For example, on August 27, 2007 a federal jury found Jon P. Oson, a former computer network engineer and technical services manager for the Council of Community Health Clinics, guilty of two counts of violating the Computer Fraud and Abuse Act. After he got a bad performance review, in retaliation Oson made a couple of significant systems changes; he disabled the systems backups of patient information and also deleted patient data on many of the servers. Not only did Oson do damage to the clinics' business systems, but Oson's actions could very well have negatively impacted the medical care of the people whose PHI he deleted.

Reduce risks while meeting compliance with change management

An effective change management program, with all necessary supporting policies and procedures, can prevent most unauthorized changes and more quickly catch those that were not prevented. Effective change management processes will also be able to detect download, installation, and release of malicious code. Malicious actions by technical insiders with authorized access can also be prevented or detected earlier using effective change management processes.

Establishing an effective change management program will also support a wide range of laws, regulations, industry standards and regulatory oversight guidance documents. Just a few of these include:

- Sarbanes Oxley Act (SOX): SOX requires responsibility and accountability for system changes within the organization's security policy, system availability policy, system processing integrity policy, and system confidentiality policy.
- The Health Insurance Portability and Accountability Act (HIPAA): The HIPAA security management requirements necessitate change management activities. If you want a specific quote from HIPAA specifying change management control requirements, then you can use § 164.308(5)(d) from the Security Rule, "Procedures for creating, changing and safeguarding passwords." Yes, don't forget to include password changes within your overall change management program.
- NIST 800-66, “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule” at § 4.8 addresses § 164.308(a)(8) of HIPAA. This section discusses an important aspect of change management; performing a periodic technical and non-technical evaluation in response to environmental and operational changes affecting the security of electronic protected health information (ePHI). The chart provided includes a lot of information about what should be included in the change management processes.
- The FFIEC “IT Examination Handbook – Development and Acquisition” indicates organizations need to have a change management system implemented to ensure all changes are approved, documented, and disseminated.
- The North American Electric Reliability Corporation's, CIP-003-1 R6, advises that that a Responsible Entity must establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.
- The Payment Card Industry Data Security Standard (PCI DSS) includes multiple change control requirements. For example PCI DSS, § 6.4 calls for the organization to establish change control procedures for all system and software configuration

changes, and directs the auditor to obtain and examine company change-control procedures related to implementing security patches and software modifications.
- The Federal Information Systems Controls Audit Manual (FISCAM) provides details on controls government auditors check for, including change requests and controls for routine and emergency software modifications. Additionally, FISCAM calls for organizations to implement formal procedures for controlling software changes.
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) requires safeguards to protect the integrity of and changes to PII.
- The European Union Data Protection Directive 95/46/EC requires PII to be accurate, and controls to be established to prevent unauthorized changes to PII that would impact the accuracy.
- The Australian Government ICT Security Manual (ACSI 33) § 2.7.38, 2.8.7, 3.5.20, 3.7.31, 3.7.32, 3.10.5 requires the organization to ensure the change management process is followed, changes are approved by the appropriate personnel, and documentation is updated to reflect the changes.

And the list could continue for many more pages. Suffice it to say that implementing change management practices supports a very wide range of compliance requirements in addition to mitigating information security risks.

Consider some case studies

Effective change management will be able to detect changes to the organization's software, hardware, and information assets. Used appropriately, change management practices can provide early detection of many malicious and inappropriate insider actions.

Consider the example provided in the U.S. Secret Service and Carnegie Mellon CERT January 2008 "Insider Threat Study: Illicit Cyber Activity in the Government Sector":

> *"One insider modified the program used by employees for changing their passwords so that their new passwords were saved in a file unencrypted and accessible only to him. He also modified the source code for a critical function in a mission critical business application to turn off an automatic security notification that would have alerted them to his fraudulent activity. These modifications were not discovered until an external customer reported suspicion of criminal acts and an investigation was initiated. Interestingly, the organization in this case did use a configuration management system for tracking and controlling all program changes. After the insider's criminal acts were discovered, logs from that system were used to determine the changes the insider had made to the programs."*

Including frequent checks of the configuration management system logs for all changes to critical programs and utilities would have allowed the organization to detect the changes much more quickly. Enforcing separation of duties within change management processes would likely have prevented the same person from making the changes to also approve of the changes to be placed into files used for production.

Consider another example from the same study:

> *"A network administrator in a government agency arrived at work to find the network experiencing problems. He quickly diagnosed the problem and had the*

> *network up and running within half an hour. While working on the problem, he surreptitiously downloaded a logic bomb from the Internet and modified the network logs to make it appear as though his supervisor had sabotaged the network. After the insider produced the network log as evidence, the supervisor was placed on administrative leave, all the while protesting his innocence. The insider was only suspected after he started to exhibit odd behavior at work, and items stolen from the office were traced back to him. Investigation by an outside forensic specialist revealed that the logic bomb had been downloaded while the supervisor was away from the office, and that the logs were modified by the insider."*

Effective change management processes would not have allowed the same person making changes to computer code to also have access to the logs; at least not update access. Separation of duties is a key component of an effective change management program.

Of course, change management processes are not foolproof, and there will always be risks that insiders will do malicious activities, on purpose or through accidents and lack of awareness. However, change management processes can detect suspicious changes in systems or applications code that can allow business leaders to act more quickly to limit the amount of damage done by insiders. And, as previously discussed, these change management activities also support a wide range of laws, regulations and industry standards.

Change management for compliance

Include the following activities, based upon the Control Objectives for Information and related Technology (COBIT®) framework that most auditors use, within your change management program to support a wide range of compliance requirements as well as to mitigate the risks associated with making changes within business processes. Also consider using the ITIL v3 Change Management concepts to help ensure your change management activities are successfully adopted and implemented throughout your entire enterprise.

1. Establish Change Management Policies and Standards

Create and implement formally documented change management policies and standards to consistently and securely handle all types of changes, including patches, maintenance, applications, procedures, automated processes, system and service parameters, and all other types of business processing platforms. Make sure to include within the policies the requirement that one person cannot have all authority, control over, or access to critical and sensitive data. This is a situation that can be hard to address within small and medium sized businesses (SMBs), but it is something important to do if possible. Not only does this make changes more effective and secure, it also supports a wide range of compliance requirements.

2. Establish Change Procedures

Once the policies and standards are established, each business area should create and implement procedures for their respective areas to be in compliance with them. If formally documented procedures do not exist, policy and standards compliance will be spotty at best, and nonexistent at worst. Don’t forget to include the following types of procedures:

- Procedures to address emergency changes; this is often overlooked within organizations.
- Procedures for defining, testing, documenting, assessing and authorizing emergency changes that do not follow the established change procedures.
- Procedures for making multiple generations of backups for critical systems and data. Ensure copies are stored in a secure offsite location.
- Procedures for logging the access of personnel with authorized access to sensitive data and systems. No one individual should be controlling the entire network and data resources. If this is the situation, there should be another position, outside the individual's area, logging and monitoring the individual's activities.

3. Perform a Privacy Impact Assessment and Risk Assessment

Before actually making changes, make sure to assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Identify all components of the change that involve or impact PII and related compliance. Ensure changes are categorized, prioritized, authorized and fully documented. Documented procedures should exist for doing these assessments.

4. Establish Change Status Tracking and Reporting

Establish a tracking and reporting system to keep track of the progress and status of each change made. For example, you need to document any changes that are rejected along with the reason for rejection, the status of the changes throughout the change process, and completed changes.

5. Perform Change Closure and Documentation

Following the implementation of changes, update the associated system and user documentation and procedures as necessary to clearly describe the changes. This is very important not only to allow for the possibility of backing out the changes, but also supports compliance requirements for change documentation.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI, “The Privacy Professor” tm is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. She creates learning tools, such as “Protecting Information” and “The Privacy Professor’s Security Search #1,” and blogs daily at http://www.realtime-itompliance.com. She can be reached at rebeccaherold@rebeccaherold.com or http://www.privacyguidance.com.