20 Ways To Mitigate The 3 Types Of Insider Threats: Part 2 of 2

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

Final Draft for April 2008 CSI Alert

In the March Alert I described the three common insider threats that face all types of organizations. They include:

- People make mistakes
- People are unaware
- People purposefully do vengeful and malicious actions

Of course you'll never be able to completely eliminate the insider threat; to err is human, no one can know everything, and someone is always going to be ticked off about something. However, with increased awareness and training, along with strong, consistently enforced, policies and procedures the insider threat can be mitigated.

Here are 20 quick tips, enumerated but in no particular order, that will help to address and mitigate the insider threat:

1. **Have comprehensive policies and procedures in place**. Organizations need to document and communicate their information security and privacy policies and procedures to create the framework for safeguarding information, in addition to ensuring their personnel know and understand what responsibilities they have to protect information. Policies and procedures should also help personnel know how to spot red flags in the behavior of co-workers and report such suspicious behavior to the appropriate position.

2. **Provide periodic training and ongoing awareness communications**. Perform periodic training and provide ongoing awareness communications to personnel, business partners and vendors to ensure all who handle or otherwise have access to PII know and understand how to properly safeguard the PII. It is not only a good idea, but absolutely necessary, to let personnel know what your information security and privacy policies are, along with your organization's sanctions, and then consistently enforce your policies.

   If personnel know that policies are not enforced, and that there is no negative consequence for not properly safeguarding information and systems, it becomes easy for personnel disregard policies when it is inconvenient or time-consuming to do so. It is also easier for personnel to do bad things as vendettas when they get upset.

   Organizations must provide ongoing awareness communications about information security and privacy policies and requirements. This will help to keep some from intentionally doing bad things, and will help others to spot the red flags that indicate their co-workers might be doing bad things. Personnel should be told how to spot red flags of coworkers who may be doing bad things, and they should know how to report them.

Communicate real events, such as when employees have been fired, or even gone to jail for doing bad things at work. This sends a message to personnel that they WILL be held accountable for doing bad things, and could end up on jail and have significant fines applied to them. Provide targeted training and awareness communications to personnel in positions of trust.

3. **Consistently enforce sanctions**. Enforcing your organization's sanctions motivates most personnel to follow policies. Another strong motivation that will work for most personnel, and likely some that do not fall under the previous motivation, is knowing that they could face jail time and monetary penalties for doing bad things to/with the information and systems to which they've been entrusted. This motivation also transcends job termination for a large portion of the population. Most people don't want to go to jail and/or pay huge fines even if they are really ticked off at a former employer and want to do bad things for revenge.

4. **Mitigate messaging risks**. Implement a policy directing personnel to not send clear-text personally identifiable information (PII) in, or attached to, email, instant or text messages. Organizations should provide solutions for personnel to use to strongly encrypt data passing through public networks, as well as on mobile storage devices.

5. **Make backups**. Make backups of business files regularly! Store the backups in a secure offsite location; and no, this is not an employee's basement or car trunk. Employees may mistakenly or maliciously delete files and you must have backups to be able to recover quickly and with the least damage possible. Make sure multiple generations of backups are made of critical systems and data. You don't want malicious former employees able to get to the backups and erase them.

6. **Do personnel background checks**. Organizations need to do background checks on individuals they are hiring, contracting or otherwise giving systems and PII access to before they actually start work. Organizations then need to do regular checks for personnel in positions of authority and authorized access to sensitive information following hire, as allowed by law.

7. **Work with other area in the organization**. Information security and privacy areas need to work closely with the Human Resources, Safety, Physical Security and Legal areas to create procedures to address the insider threat and to ensure all the links between the areas are thoroughly considered.

8. **Provide minimal information access**. Effective controls must be established to ensure personnel have access to only the information they need to perform their job responsibilities, and no more. Access control should be designed, implemented, and enforced at the enterprise level for all business practices.

9. **Implement exit procedures**. Effective exit procedures must be established to ensure personnel who leave the company, under any conditions, do not take sensitive information such as PII with them. Have thorough exit plans in place and follow them consistently for when employees in critical positions are terminated or resign. There should also be heightened monitoring following the unharmonious

resignation of an employee from a position of excessive systems and data access control and responsibility. Be sure that all computer and information access is deactivated following termination.

10. **Log access**. Technology controls should be established to log access authorized personnel have to sensitive data, such as PII, and an independent area, such as internal audit or information security, should review the logs regularly. Log reviews will help to identify inappropriate access and stop it as soon as possible to lessen the potential for bad things to happen; to not only the company, but also to prevent bad things from happening to personnel and customers. Log the access of personnel with authorized access to sensitive data and systems.

    No one individual should control 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. System logs should be stored in a secure location and backed up to ensure that all actions can be traced back to a specific individual user.

11. **Implement extra controls for positions of authority**. Implement additional controls for personnel with excessive access authority to systems, databases and applications. Log their network activity and audit the logs regularly.

12. **Implement change management controls**. Make sure you have a strong change management system and procedure in place. Make sure there is separation of duties. Programmers should not be able to modify code and put it into production with out having it reviewed and the changes authorized by someone else outside the influence of the programmer.

13. **Document red flags**. Be aware of red flags that indicate those with positions of trusts may be doing something illicit. Have procedures for personnel to follow to report suspected violations. Organizations should train supervisors to recognize, document, and respond to inappropriate or concerning behavior in the workplace. Establishing a formal process for reporting and sharing information may encourage employees to alert employers of potential insider activity.

14. **Obtain executive support**. Obtain the obvious and strong commitment of executive management for information security policies. Business leaders must let personnel know that they expect everyone in the company to appropriately safeguard PII, and they must also let them unequivocally know that noncompliance with policies will result in consistently applied sanctions.

15. **Establish separation of duties**. Make sure one person does not 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 as the examples from last point out, it is something important to do. Organizations need to ensure procedures and oversight controls are in place to enforce separation of duties to address insider threats. Documented procedures should be used to validate the data collected has not been altered inappropriately through between multiple insiders. Technical controls, such as role-based access controls, can be

used to help ensure separation of duties. Use a combination of manual and technical controls help to prevent and detect when insiders are trying to do bad things.

16. **Implement effective password management**. Organizations need to have strict password and account management policies and practices in place and enforce them consistently. Password and account management can help prevent insiders from exploiting access control gaps. There have been many incidents that occurred as a result of personnel following poor practices, such as sharing user IDs and passwords, allowing poor quality passwords, and not locking out accounts after multiple incorrect password attempts.

17. **Implement security layers**. Use a layered defense to help prevent insiders from easily getting past only one security control to do bad things. Organizations should not only use security layers within the networks, systems and applications, but also make use of physical security and personnel security controls. Perform periodic risk assessments to find where more security layers need to be implemented.

18. **Implement configuration management procedures.** Implement configuration management and characterization procedures to detect download, installation, and release of malicious code. Malicious actions by technical insiders can have been prevented or detected earlier with effectively implemented characterization procedures and configuration management. The characterization procedures can be engineered specifically to detect changes to software, hardware, and information assets that can flag potential insider abuse. Configuration management systems can track and control changes to systems or applications to identify when authorized personnel are making changes that are unplanned, unscheduled and unnecessary for business purposes.

19. **Implement sound vendor and business partner practices**. Many incidents have occurred from insiders at outsourced vendors and business partners. Include detailed information security requirements within outsourced business partner and vendor agreements. Send outsourced vendors and business partners only the minimum amount of PII necessary for them to perform the activity for which they are contracted. Perform due diligence and ongoing follow-up to ensure business partners and vendors have a comprehensive information security program that they enforce.

20. **Document and maintain incident and privacy breach response plans**. Document and test a privacy breach incident response plan to most efficiently, effectively and consistently handle breaches when they occur. Be sure to include how to respond to privacy breaches that can occur as the result of insiders abusing their authorized access to lessen the negative business impacts of such attacks. Preserve evidence. Collect and save data for use in investigations.

The insider threat is very real, in businesses of all sizes. As the example of the architectural firm employee from part one in the March Alert showed, even a perceived, but not real, threat to a worker's job can trigger her to try and take down the business with her. Organizations must address the insider threat. Disgruntled and/or mentally

unstable personnel are a threat to the business, and if they have authorized access to the network infrastructure or business information, extensive damage can occur.

You cannot prevent people in positions of trust from abusing their capabilities to do bad things. However, you must implement appropriate due care controls to mitigate the risks of them doing bad things as much as possible. Trust is good, but it is not a control, and it is not a standard of due care.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. She just released the quarterly employee awareness tool, “Protecting Information” (Information Shield) and blogs daily at http://www.realtime-itompliance.com. She can be reached at rebeccaherold@rebeccaherold.com or http://www.privacyguidance.com.