Identifying and responding to data breaches

Independent agencies should work with IT staff and/or consultants to develop a pre-defined action plan to deploy in the event a security breach occurs. Do not wait until a breach occurs to think through how to react to the situation.

If you experience a security breach, here are some steps for you to consider to mitigate against further damage and to prevent a recurrence:

- **Identify senior staff to whom reports of known or suspected security breaches should be made. It is important that someone be designated as the point person so reports are properly directed and acted on in a timely way.**
- **Determine if any personal, nonpublic information about your policyholders or employees has been stolen or accessed by unauthorized employees or third parties. If so, consult with your attorney or others knowledgeable about privacy laws to determine your obligations and next steps. For Maryland business, these steps include notifying the affected individuals of the breach or possible theft of their information, and suggesting some steps they might consider to safeguard against the misuse of their information. You also need to notify law enforcement and possibly your agency's professional liability carrier.**
- **Investigate the cause of the breach. If it has resulted from the compromising of your hardware or software, isolate the hardware and software involved by disconnecting it from the network and the rest of the agency's systems, as well as the external world.**
- **Work with your IT professionals to plug any holes in your systems to prevent further incidents or a spread of the problem. Remove or fully quarantine the infected files and/or other identifiable cause(s) of the problem. Notify security software vendors if you believe the breach is something they should be aware of or is potentially a new problem to them.**
- **If the security breach has resulted from actions taken by unauthorized employees or third parties, take appropriate and/or corrective measures, such as disciplining the employees in accordance with your personnel manual and policies (which may include suspension, termination or other measures), notifying the third parties' organizations and/or notifying the appropriate law enforcement authorities.**
- **Notify your business partners (carriers, vendors, etc.) of the security breach in situations where the breach occurred through the use of their facilities or services, or in cases in which they may have been or may, in the future, be impacted by the breach. This notification will enable your business partners to safeguard their systems, limit access or take other necessary protective and corrective actions.**
- **Determine the appropriate monitoring processes and procedures in an effort to prevent a recurrence of the security breach and implement them. This should include a review of the existing processes to see where they failed. Train your staff in any new processes and procedures and in the nature of the security risks they are designed to prevent, and update or revise your written policies and procedures to reflect these changes.**
- **Once the cause of the security breach has been removed or addressed, and corrective or preventive measures have been put in place, bring the isolated software and equipment back into operation after testing it to be sure it is no longer a problem.**

Consider whether the nature of the breach calls for an independent security audit of your agency by an outside security professional.