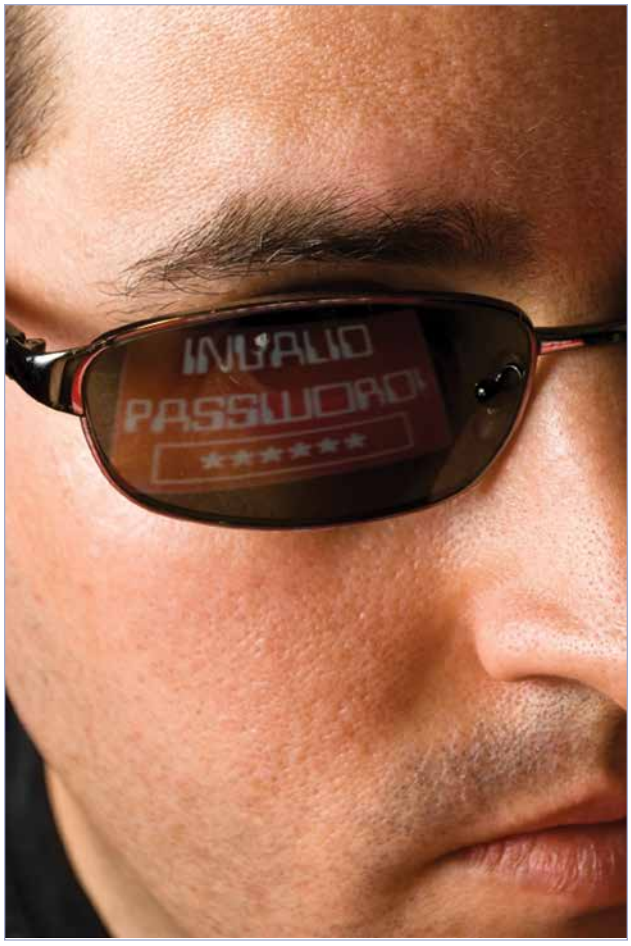
10 Things Organizations Should Do to Protect Against Hacking

John J. Isaza, Esq., FAI



A recent *New York Times* report about a Russian gang that collected the Internet security data of 1.2 billion people has stirred a maelstrom of pundits wondering if the situation is as dire as it sounds or just sensationalistic reporting. Regardless, one thing is clear: the mere specter of being hacked reinforces the importance of information governance (IG) and data protection processes, procedures, and technology.

But, some organizations are looking for a "silver bullet" to come along to make it easier for them to stay ahead of the criminals. Indeed, companies like Milwaukee-based Hold Security are now offering monthly fee-based services to help organizations detect if their sites have been affected by this breach. Frankly, though, organizations that need to rely on this type of service to protect themselves will remain a prime target; this incident should serve as a huge wake-up call for them to take more proactive steps to safeguard their information.

Accountability, Preparation Needed

Most importantly, someone with a high level of authority has to be in charge of information security to ensure that people, processes, and technology are in place and working effectively. This might be a chief data officer (CDO) or some similar officer who is tasked solely with responsibility for ensuring data is protected. The first of the Generally Accepted Recordkeeping Principles® (Principles), the Principle of Accountability, speaks directly to this point. (Read more at *www.arma.org/principles*.)

Stay on top of your information governance ecosystem.

After accountability is assigned, preparation is key. Following is a list of 10 things organizations should do to protect their data and stay ahead of the curve.

1. **Hire or appoint a CDO or a similar executive to be responsible for information security.** (See previous comments.)

2. **Learn from the past**. It has been said that those who do not know history are doomed to repeat it. Start by assessing your organization's previous hacking incidents and learning as much as possible from those experiences. If you have not had any breaches, consider yourself lucky and learn as much as you can from other organizations' breaches.

3. **Hire hacking professionals.** If data is stored locally, retain a consultant or task an employee with figuring out how to hack into the organization's systems. Depending on the size of the organization, this could be a full time job for one or more people.

4. **Vet vendor security.** If data is stored in the cloud or with other third parties, vet the vendors' processes and procedures around data protection. Check to see if they have staff dedicated to information security and whether they are technological game-changers in their space. Since data security should be of the highest priority for cloud vendors, for instance, being on the cutting edge of technology should be expected of them.

5. **Conduct a gap assessment.** A gap assessment is essential to identifying areas of vulnerability for critical assets that need to be protected. According to the Principle of Protection, "…every system that generates, stores, and uses information should be examined with the protection principle in mind to ensure that appropriate controls are applied to such systems."

   Use a maturity model and a scale of 1 to 5 to assess your status, with 1 being non-existent or in a dismal state and 5 being in a transformative state. (Check out the Information Governance Maturity Model at *www.arma.org/r2/generally-accepted-br-recordkeeping-principles/metrics*.) Be vigilant about assessing the more recent areas of vulnerability for many organizations, such as use of:
   - Work-from-home arrangements
   - Airplane, airport, and other public WIFI connections
   - Portable devices
   - Third-party contractors

6. **Update your data map.** Most organizations should have at least a semblance of a data map in connection with e-discovery preparedness, if nothing else. Leverage this data map to assess systems that need higher security and closer attention. Be sure to include data created and stored with third parties, including data in the cloud. (See "Six Steps for Creating a Super Data Map" by Mark Diamond on page 28.)

7. **Stay on top of your information governance (IG) ecosystem.** Most organizations focus on their servers and, maybe their "bring your own device" policies. However, the IG ecosystem is much bigger than that. Organizations need to align their data with all possible uses, compliance, data protection, and all other Principles' concerns.

8. **Update your data security policies and procedures.** Organizations should have a defined set of policies and procedures designed to protect data starting with expectations for every employee. If you do not have them, create them. If you do have them, review them annually to update and revise them as indicated by the results of steps 2 to 5.

9. **Train, train, train employees.** Be sure that all new employees are trained on data security policies and procedures as part of their orientation, and provide ongoing, periodic training for all employees.

10. **Audit, audit, audit systems and employee compliance.** Conduct random audits as part of your system checks and balances to ensure that not only are employees complying, but also that processes and technology are working as expected. Use these audit results to resolve gaps and vulnerabilities.

These recommendations are not exhaustive, and they are not intended to be followed as a one-time process. They need to be entrenched in the organization's culture for those who want to step ahead of today's savvy, information-seeking criminals. **END**

John Isaza, Esq., FAI, can be contacted at John.Isaza@InfoGovSolutions.com. *His bio is on page 47.*