The Sony hack signals the need for information governance

One of the most important reasons to adopt information governance is the need to address the increasing security risks associated with unchecked data growth

BY PHILIP FAVROJANUARY 22, 2015

31

Where do you stand on information governance?

Many view information governance as a laudable yet dispensable component of a company's information management plan. Information governance is sometimes conflated with e-discovery preparedness, which may lead in-house counsel to dismiss governance programs as the province of repeat litigants. And big data advocates are also questioning whether governance — with its stated objectives of classifying and deleting information — is necessary given recent advances in search technology and decreasing storage costs.

Though there is some merit to these positions, there are still many reasons why companies *should* adopt governance initiatives. Perhaps one of the most important is the need to address the increasing security risks associated with unchecked data growth. While some big data adherents espouse the benefits of mining value from stockpiled emails and other materials, that data could be exposed in data breaches. This notion – that data stockpiles could become vulnerable if not eliminated through information governance – gained support from the now notorious breach of Sony's computer network. Commonly referred to as the "Sony hack," this data breach could end up being the bellwether that pushes more organizations to adopt governance programs.

The hacking details

The basic details surrounding the Sony hack are as follows. A hacking group — apparently sponsored by the North Korean government — infiltrated the "corporate network" of Sony Pictures on Nov. 24, 2014, removing "terabytes of private data, delet[ing] the original copies from Sony computers, and [leaving] messages threatening to release the information if Sony didn't comply with the attackers' demands." Slowly and painfully, the group has leaked that confidential information, which includes executive compensation, employee social security numbers, unreleased movies and a massive trove of corporate emails.

Rather predictably, the leaked emails have divulged salacious details about Hollywood gossip. They have also revealed some weaknesses in Sony's overall

approach to information governance. A few of the more noteworthy points include the following:

Information governance lessons

So what information governance lessons can be learned from the Sony hack? The first is probably not to follow the reflexive reaction of certain fearful Hollywood executives who are shunning email to conduct business. While prudence should be used in drafting emails, the better lesson is to eliminate unnecessary email stockpiles. As Sony's general counsel apparently explained in one of the now disclosed emails:

"[T]he issue behind our moving in this direction is not one of whether the company should continue to retain its records etc. It is about the fact that email is not the correct repository for this . . . . While undoubtedly there will be emails that need to be retained and or stored electronically in a system other than email, many can be deleted and I am informed by our IT colleagues that our current use of the email system for virtually everything is not the best way to do this.

Thus, one way to protect the company's "ESI blindside" (using a football analogy) and create an effective information governance defense is to implement an "offensive" email reduction program.

Another such measure is to implement effective security strategies and complement them with intelligent processes and technologies. For example, organizations should begin taking simple steps such as identifying, segregating, and securing IP, PII and other sensitive propriety material. As suggested in a recent Bloomberg Businessweek article, this could involve adding "layers of encryption to protect internal traffic from prying eyes" and isolating confidential materials "from central data-storage systems connected to the Internet, making it harder to find." It could also include the use of artificial intelligence, machine learning and automated technologies, all of which facilitate the identification and isolation process.

While even the most effective information governance programs may not be sufficient to defeat sophisticated attacks on an organization's network, they can mitigate the extent of the damage and limit risks and potential liability. What is more, they have the potential to address lesser attacks and remedy other related and collateral issues with data hoarding. As the Sony hack demonstrates, the alternative — doing nothing or taking nominal remediation measures — are not viable options. Information governance may be the most effective method.