Wikipedia defines Information Governance (IG) as "the management of information at an organization" which "balances the use and security of information". AHIMA describes IG as "a strategic approach to maximizing the value while mitigating the risks associated with creating, using, and sharing enterprise information. "The Gartner IT Glossary defines IG as "the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information." While all these definitions vary, they all make mention to the balance between usability and security. This is the root of Information Governance, the tightrope upon which the entire practice exists. Much like it's existence in IT and RIM, it teeters one way and back, from buzzword to serious business practice, from security to freedom.

My search results for Information Governance were varied. The top two results (both ads) were for serious Information Governance services. The first was for IBM corporate Analytics and Information Governance solutions, the second for Datum Strategy corporate solutions. Most of the suggestions and selected results have to do with IGs interaction with healthcare information and legal stipulations surrounding the NHS. Most of the clickbait-esque articles I've read focus on the negatives of not implementing proper Information Governance like additional litigation during lawsuits or audits, fines and punitive actions for non-compliance with regulations, and the risks to cybersecurity if files are lost or stolen or digital security is ill maintained. Most articles place the onus of Information Governance upon IT instead of RIM. Even many definitions mention the importance of IT in the implementation of proper Information Governance, but not a single article or definition I encountered included any mention of RIM.

Some of my favorite articles place the onus of Information Governance on ***everyone*** involved in the creation or storage of information. An article on skillsplatform.org mentions the hacking of the infidelity dating site Ashley Madison and the findings of the investigation that the most popular passwords on the site were "123456" and all lower case "password". Around 11 million people's accounts were cracked in that fiasco, mostly because of poor security on the user's end. If users of an infidelity dating site were unwilling to use halfway-decent security to keep their extra-marital affairs secret from their partners, what kind of digital security measures do you think they would use on the job? I don't know about you,

but when my relatives find themselves 'locked out' of their computer or their email somehow, the first attempts at passwords I try are always the two listed above and then several more personal (like all-lower-case names of grandchildren or beloved pets) and more often than not, I get in in the first couple of guesses (and then chide them for their lack of security and try and convince them to pick a harder password).

Cybersecurity and Information Governance has been in the realm of IT for far too long. While I think some speculation of the future of IG is a bit pie-in-the-sky, I do believe the future rests in the hands of all employees that work with records and information. As RIM professionals seek to educate the employee about records management, we should expand this teaching into all aspects of Information Governance including security measures, risk reduction, and safe storage of digital and physical records.

Whether or not your IT and RIM staff are trained with the latest techniques and using the most cutting-edge technology, most security breaches occur because of employee error or lack of security. To remedy this, RIM should seek to include more individuals in the implementation and education of Record Management procedure and tools. People really are willing to learn, and the easiest way to keep future breaches from occurring is to make sure all staff involved with information creation or storage (most of them I'd imagine) are savvy to the regulations, stipulations, security measures, and other further expectations their work has. Most people like to see the big picture. If they know their work has an impact or can make life a little easier for everyone down the line, they're more apt to do that work. Ignorance of regulations, expectations, and procedure by the general employee only serves to harm and organization.

I think the future of Information Governance is going to be less glamorous than IBM makes it out to be. It's not going to be a hierarchy of smartly-dressed IT reps making everything work and keeping it safe, but all of us who work with information. Keeping employees in the know can only help with cybersecurity and analytics in the future. Creating properly categorized and maintained information will cut back on the backlog of unorganized and semi-organized data that already exists and bring IG into the future instead of worrying about the past.