As an enterprise security professional managing information and cyber security, your duty is to protect your company’s data and confidential communications from theft or loss. The challenges are daunting. Despite defenses and precautions, hackers have stolen over a trillion dollars’ worth of intellectual property from the U.S. government and American companies, according to Ponemon. Yet while you fortify firewalls, encrypt data, and install the latest technologies, important confidential data may be regularly leaving your control in the legal process.

Hackers have discovered that law firms can be easier targets than the companies they serve. The FBI recently met with more than 200 New York law firms to warn them that they were being targeted for cybercrime. Mandiant estimates that at least 80 major law firms have been hacked, some by nation-states, Bloomberg reports. The discovery process requires that data potentially relevant to litigation be preserved and collected. Often this data is sent to law firms for review before it is shared with opposing counsel. Law firms often subcontract to e-discovery service providers for assistance in this review.

Why is data at high risk in litigation? The main reason is that some lawyers may not be as security-conscious as their clients. Data security experts, therefore, should consider educating legal teams, develop security protocols, and be involved in assessing and improving the security of firms and vendors.

Educate Your People
Many data loss events are not malicious, but result from lack of training and accidental misplacement of unencrypted data. Lawyers, like many other professionals, are not often highly technical. Indeed, Kia Motors requires would-be attorneys to take a basic technology skills exam – which over 90 percent fail, according to Law Technology News.

Technology cannot be separated from the people that support it. Your legal team should understand the requirements for handling data and the risks at issue. For example, most public Wi-Fi locations lack security. Yet the practice of attorneys working off of such Wi-Fi in public locations (such as coffee shops or restaurants) has become so commonplace that the State Bar of California felt it necessary to remind attorneys that they risk violating their duties of confidentiality when using public Wi-Fi to work on client materials (Read PDF here).

Those with responsibility and possession of your data should consider standards similar to your own. Law firms trail some corporations in data security. Some firms and vendors have a CIO/CISO and established protocols, many others do not. In the e-discovery industry – a relatively new industry with few barriers to entry and no uniform security standards or oversight – the focus has been more on speed and cost reduction rather than security. Lawyers may use e-discovery providers without understanding the provider’s data security measures and whether those measures are appropriate for a particular client, case or set of data. For example, a lawyer or client may rely on a “budget” vendor that licenses a “brand name” review platform, unaware that data may be hosted in an unsecured garage or further subcontracted. The cloud is no more or less risky than other hosting, but is only as safe as the cloud vendor itself. And although law firms may bring hosting and e-discovery in-house, they may not focus as closely as some clients would prefer on data security.

Raising the Bar
Data security experts should consider companywide standards, and may require assurances and certifications of vendors and law firms. Some companies have formed cyber-risk or e-discovery committees that may include the GC, CIO/CISO, HR, compliance and others to share information and responsibility. Data security personnel may also either participate in the vetting process, or train your attorneys to ask the tough questions of firms and the prospective vendors.
Highly litigious companies have brought some processes in house; however the costs of hardware, software and experts to run the rapidly changing e-discovery technologies must be balanced against the overall litigation profile. Top tier e-discovery partners may have standards that surpass your own, as well as expertise in the e-discovery process, reducing risk. The bottom line is that no one is 100-percent safe from hacking and data security is not a one-size-fits-all problem. Law firms and service providers, just like corporations and other businesses, vary wildly in their ability to provide data security. That said, if you educate, choose wisely, and proceed with caution, hackers will most likely move on to easier quarry.