THE PRINCIPLES OF INFORMATION PROTECTION PLANS

By James Pooley
www.pooley.com

Most information security management boils down to risk analysis, which naturally begins with knowing what's at risk, and particularly what the threats are. Because assets are located throughout all your systems and accessed by most of your employees and quite a few vendors, customers and business partners, securing these assets touches every aspect of the business, and therefore requires a thoughtful plan, informed by inputs from managers throughout the enterprise.

Creating an Information Protection Plan

There are two major reasons for creating an information protection plan. The first is that courts expect you to have one in case you suffer a loss and need their help with a misappropriation. In fact, if you had not exercised "reasonable" efforts to prevent the loss, they will probably conclude that you have no rights in the information. In addition to the courts, your efforts should also impress your employees and business partners, who will come to learn that you consider your trade secrets a priority. But beyond the demonstration effect, you also want to actually prevent loss and contamination, or mitigate the effects of a loss when it happens (as it likely will). So your goals here are twofold: prevent problems and show you care about them.

When I started in this field forty years ago, there were no real standards for information security; or rather, there were only very simple ones: control the perimeter, escort visitors, and get confidentiality agreements. Information as an asset was an evolving concept, but the Internet and all of the "threat vectors" that it enables had not yet arrived. Even fifteen years ago, in searching for published standards to inform the process, the best I could come up with was the Federal Sentencing Guidelines, which laid out a simple compliance framework for avoiding inadvertent criminal misappropriation. (In fact, the Sentencing Guidelines remain relevant today on questions of corporate governance.)

Protecting the data of others

As you consider how to formulate your own protection strategy, it's important to keep in mind that you are responsible not only for your own data, but also for all the information that is entrusted to you, for example, by customers and collaboration partners. In one case you are avoiding loss, in the other avoiding liability. This concern should be especially acute in organizations that regularly guard the confidential information of others, such as banks, law and accounting firms, and suppliers of custom systems.

In addressing information security, you should differentiate between trade secrets and Personally Identifiable Information ("PII") that implicates a customer’s privacy. The latter category has become a significant worry for a growing number of companies that gather and hold information from customer transactions, and privacy protection laws require careful attention to protecting PII. But a report issued in 2010 by Forrester Consulting found that companies spend a disproportionate amount of time and money on protecting against its accidental loss than they do on preventing theft of trade secrets, even though they valued commercial secrets much more highly in dollar terms. Of course, this doesn’t mean that companies should abandon efforts to protect privacy data, both as a matter of respecting customer relationships as well as avoiding liability. But business secrets also deserve your focus.

The principles of a protection plan

Several basic principles should drive the design of your trade secret protection plan. First, information should only be available to those with a need to know it. This derives from the basic truth that the best way to keep a secret is to tell no one about it, and the corollary that with each additional person you tell the security decreases and the risk increases. So information should be allocated and rationed, by marking records according to a known and accepted distribution policy, and by establishing your electronic file system with various layers of access according to authority and need.

The second principle is simplicity. This is where I have seen many company policies fall down. Often they are prepared by former military or law enforcement professionals, who seem to like categorizing information into seemingly endless strata with confusing labels. Here’s an actual example of categories used in one business, scrambled for effect: Private, Sensitive, Confidential, Highly Confidential, Restricted, Secret, Company Proprietary. Could you line up ten people and expect them to order those categories the same way, much less describe how one was different than the other? Here’s what happens when people confront a system that is too complex or that they don’t understand: they ignore it. And if there is anything worse than having no information control system, it’s having one that is regularly disregarded. Therefore, I tell my clients to keep the categories to two or three; you’ll get much better compliance.

Principle number three: you can’t keep everything secret all the time. A senior Navy intelligence officer once shared this nugget with me: every secret will eventually get out; the trick is to guess when that will happen with the secrets that matter most. So build some flexibility into your system, and don’t try to keep every single factoid locked up; it won’t work and you’ll be so distracted you may lose the best stuff.

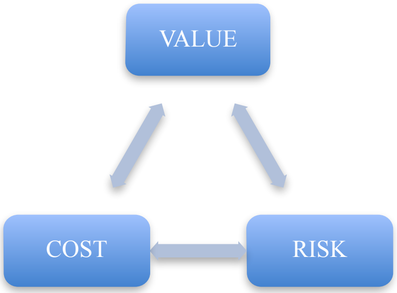
Number four may seem counterintuitive in the days of headline cyberattacks: the greatest risk is inside, not outside. The biggest problem is not in software, it’s in the “wetware” between the ears of employees. The vast majority of them are honest and well-intentioned. But they can be careless, chatty, boastful, and all too often are just poorly informed. This is why the single most cost-effective aspect of any information protection program is employee education.

This point bears some emphasis. A 2013 study by the Ponemon Institute, based on a survey of 3,317 trusted employees in six countries, employed in companies of varying sizes and in various industries, found that two-thirds believed it was acceptable to transfer confidential company information to personal computers and other devices, or to online data storage sites like Dropbox. For many, this was about convenience; but consider this: just over half of the respondents also thought that using confidential data at a later job (in this case software developed by the employee) was not wrong. Justifications included "It doesn't harm the company" and "The company doesn't strictly enforce its policies.”

Principle number five: information security is just ordinary risk management. Most businesses, even relatively small ones, recognize the importance of internal controls. And for most enterprises today, information loss is the greatest risk. As in other areas, this is not about eliminating risk – usually that’s impossible – but about understanding and analyzing risks so that informed decisions can be taken about the ones that can be mitigated in a cost-effective way. Here, you need to go to the grass roots, to the lower-level managers who know what is important, what the risks are, and what might be done to control or reduce the risk. It will be your job to take all that in and decide how the value and cost issues affect your company’s appetite for information security risk. In general, appetite for risk goes up as value decreases and the inevitability of loss increases. (See principle number three.) And whatever plan you implement needs to be led by someone with responsibility, and be reviewed frequently to take account of changes in the risk calculus.

Balance value, risk and cost

A useful rule of thumb is reflected in the value-risk-cost triangle:



Keep in mind that risks and threats change with time and circumstance, and so risk assessment must be a continuing process, reconsidering the program at reasonable intervals. It’s also important to revisit your plan in connection with mergers and acquisitions, where the challenge is to integrate legacy entities that have their own, sometimes conflicting, policies. Also, be realistic about what you might be required to spend in order to match today’s threats. Another Ponemon Institute study from 2011 surveyed over 600 experienced IT security professionals, and found that in 88% of companies the security budget was less than the coffee budget.

One final note of caution to start-up companies: please look carefully at your secrets. After decades in Silicon Valley, I appreciate the pressures that force new companies to triage their priorities, and getting a prototype ready may seem like the only objective worth focusing on. But if in the process of getting the innovation out the door you also destroy any chance of protecting the competitive advantage it represents, all of that work will serve only to power someone else’s market success. It’s not hard to put the basics in place, and the very modest distraction will almost always be worth it.

Information Security Is a Board-Level Concern

Up to this point, I have addressed these issues as a “management” concern. But exactly who within management should be concerned about information security? The short answer is everyone, although naturally at different levels of detail, according to the complexity of your program. Again, a historical perspective should illuminate the issue. In pre-Internet days, data integrity was the exclusive province of the IT staff, who were more or less focused on keeping the equipment running in the computer room. Employees did not carry around powerful computers in portable smartphones. Trade secret issues were isolated events, and using the resources of HR, legal, and security, it was often sufficient to react to them when they occurred.

Those days are gone. Along with increasing importance of information as an asset, businesses now must contend with an essentially insecure environment in which everything they do is globally connected and “controlled” by a workforce with the power to seriously compromise data integrity. In short, the threat level has moved from occasional to existential. With information security almost universally rated as a top category risk, governance of this function has to be a board-level concern, and directors must ensure that they are well informed about the company’s risk profile and its control systems.

Regulatory action

Here’s something to think about. The Federal Trade Commission in 2012 brought a case against Wyndham Hotels, which had been the victim of a hack that pulled customer information from its records, causing over $10 million in fraud losses.

The FTC alleged that Wyndham's management had "faile[d] to maintain reasonable security allow[ing] intruders to obtain unauthorized access" to its network, and that this violated federal laws against unfair and deceptive behavior. Although a related shareholder derivative suit was dismissed, that happened in part because the Wyndham board engaged experts to thoroughly review their vulnerabilities and instituted a program to address them. Ultimately, Wyndham settled with the FTC, agreeing to a special 20-year oversight program. And even though this case was about data privacy, it's not much of a leap to imagine similar claims being filed over neglect of security issues. Finally, avoiding criminal liability for receiving trade secrets may require establishing compliance plans that include serious board-level engagement.

In early 2014, the Securities and Exchange Commission issued a "Cybersecurity Initiative Risk Alert" that defines expected measures by companies operating in the securities industry. Again, although this was guidance directed to a particular industry, it may be prudent to see this a straw in the wind, and recognize that companies across the board will have to confront external expectations about their management of data security.

What to do next

Various resources are available to help you take this project to the next level and create a plan. My recent book *Secrets: Managing Information Assets in the Age of Cyberespionage*, includes a series of exemplary frameworks tied to the size and resources of the organization. This principle of flexibility is also reflected in an excellent document prepared by the National Institute of Standards and Technology (NIST). Although its title – "Framework for Improving Critical Infrastructure Security" – might indicate it is only for banks and energy companies, the NIST Framework was designed (with industry input) for application to almost any enterprise, regardless of size or sector.

Another great place to look is the website of CREATe.org, a not-for-profit organization that helps companies, particularly small to medium-sized ones, address their information security issues. Available tools include an online self-assessment, evaluation and improvement plan, as well as an extensive guidebook with model policies, procedures, checklists and training materials.

Organizations with existing plans should perform a gap analysis to identify weaknesses in risk assessment and controls. All companies should consult with an experienced professional on the design and implementation of larger projects that may involve complex relationships, international issues or coordination with other aspects of a company's intellectual property strategies.