Contents

INTRODUCTION

BANKRUPT NETWORKING GIANT Nortel reveals that its key executives' email passwords were stolen and the company's network hacked for a decade. Boeing, hiring away Lockheed employees who bring documents to their new employer, pays $615 million to avoid criminal prosecution, while two of its former managers are indicted. Apple scrambles to recover a sample of its unreleased new model iPhone that was left by an employee in a bar – a year after the same thing happened in a different bar. Starwood employees leave to join Hilton, taking with them ideas for a new kind of hotel. And the owner of Thomas' English Muffins goes to court to protect its "nooks and crannies" recipe from being used by a competitor. What do these corporate crises all have in common? Trade secrets. They reflect the enormous value of – and threats to – the most important assets of modern business.

The titans of the 19th Century made fortunes because they controlled access to the raw materials and infrastructure of commerce: steel, oil, lumber, railroads, canals, shipping. They oversaw the first Industrial Revolution and facilitated the second, which culminated in mass production, vastly increasing human productivity and prosperity. But there were only a few of them, and the resources they took often decreased what was available to others.

In contrast, the Third Industrial Revolution creates value not just from ideas that improve our ability to transform materials, but from information itself. In the increasingly globalized, hyperconnected electronic age, businesses and even markets are formed almost overnight.

Compare Watt's steam engine, which took more than thirty years to work on a boat (Fulton's, in 1807) with the photo-sharing technology of Instagram, a two-year-old start-up purchased by five-year-old Facebook in 2012 for $1 billion. Undeniably, the modern economy relies almost entirely on a rapidly unfolding universe of "intangibles."

This shift to intangible assets has been profound, but so swift that few have paid sufficient attention to the magnitude of the change. The accounting profession values corporations on their balance sheets, reflecting mostly tangible assets. In contrast, Wall Street votes with money, which is why Facebook was worth $100 billion on its first trading day. Of course, much of a company's stock value is based on what investors think it will be able to earn in the future, and a lot of that is speculation. But peel away the first layer of investor exuberance or wishful thinking, and what do you have to account for the big numbers applied to companies like Google, Facebook and Apple? Some furniture and computers, but likely not much real estate, raw materials, or product inventory. That's the old economy. Today's modern company is built on a foundation of information.

In the Information Age, your secrets – a new technology, a business plan, insights extracted from data analytics – define your competitive advantage. And because business is global, competition can emerge anywhere, anytime. Not just success, but survival requires vigilance and careful management. Those who know how to protect and exploit the most important secrets can quickly leverage their business to profitability and dominance; while those who fail to recognize this new reality are doomed.

What about patents? Isn't that how the value of new technology is captured? Patents do get a lot of attention. Economists often count them as a proxy for innovation, comparing companies and countries in league tables. The popular press focuses on the "patent wars" between high-tech giants and laments what it sees as a wasteful food fight. Certainly patents are critically important, and can be credited for enabling much of the modern technology-based economy. But there is another

part of the legal world of intangible rights that matters at least as much but gets far less air time: trade secrets.

A large part of the reason for this is that trade secrets are, well, secret. Companies don't talk about things that they don't want the competition to know. But according to well-documented studies, secrecy is by far the preferred form of protecting competitive advantage. A 2009 survey of U.S. businesses by the National Science Foundation and the Census Bureau found that, among companies that engage in substantial research and development (R&D) activity, trade secrets are the leading method of protection. And for those companies officially classified as "R&D intensive" – who account for 67% of U.S. R&D expenditure – secrecy is considered the most important form of intellectual property, more than twice the level for invention patents.

This preference for secrecy over patenting may seem odd to some, especially lawyers and judges, who look at the two systems in the abstract. In a landmark 1974 decision finding that trade secret law was not "preempted" by federal patent law, the U.S. Supreme Court said that secrecy, as a method of protecting innovation, was relatively "weak." This is because unlike patents, secrets are not exclusive; that is, someone who independently discovers the same information is just as free to use it as the original discoverer. No rational actor, the court explained, would choose to protect an invention by secrecy when he could claim the power of patenting instead.

It's too bad no one at the Supreme Court surveyed companies about what they were actually doing at the time. One of them, DuPont – the inventor, among many other consumer wonders, of nylon, Teflon and Kevlar – has been the world's leading supplier of titanium dioxide (TiO2), a whitening agent used in products as diverse as paper, paint, toothpaste, and sunscreen. In 1948, DuPont had cracked the code for a new chloride process that made it possible to manufacture TiO2 better and cheaper than everyone else. But rather than patent its recipe, DuPont did what a lot of companies do with process technology: they kept it as a secret. So instead of teaching all its competitors through

publication of a patent that would have expired in the 1960s, DuPont continued for over sixty years to support its leading-supplier position in a multi-billion dollar market, enabling a spinoff of the business.

If like DuPont your company owns a process that can't be reverse-engineered by examining the end product, then the advantage of using secrecy is obvious. But even for other technologies, there are good reasons to keep secrets. They're cheap: you don't have to pay for government certification. They're broad, covering many things that patents can't (indeed, they cover just about any business information, like sales data and strategic plans). And unlike a published patent, you don't broadcast to the competition what you're doing.

Of course, as we all learn early in grade school, secrets are vulnerable. They depend on trusting somebody else not to tell. In business, increasingly valuable information is put in the hands of an increasingly mobile – and some might say decreasingly trustworthy – workforce. Paradoxically, the communications revolution that has brought us the Internet, Twitter and Facebook has also exposed corporate data to new and alarming risks of inadvertent loss as well as espionage. And not only is protecting your own information assets a newly compelling priority, but infection from unwanted secrets of competitors has generated expensive litigation and even criminal sanctions. Directors and executives who fail to confront this new reality are ignoring their responsibility to protect and commercialize the company's most valuable assets.

The law that applies to protecting trade secrets around the world is far from uniform. Although the 1995 TRIPS agreement requires all member countries of the World Trade Organization (that is, almost everyone) to enact laws that protect "undisclosed information," enforcement varies enormously from one country to another. And even though Europe is considering a process of harmonizing trade secret laws, the current reality for global business is a fractured system of secrecy regimes. Fortunately, U.S. law is relatively integrated and

advanced (and indeed was the inspiration for the TRIPS standard), and so will be the source for most of the practical "rules" described here. But a major part of any modern business strategy has to take account of the international legal environment, and you will find appropriate advice in later chapters.

I first wrote a book about trade secrets in 1982, when the most effective way to protect a company's confidential data was to watch who went in and out the front door. In the intervening years information security has been challenged by the Internet, an emerging culture of disclosure powered by social media, sophisticated hacking tools, global supply chains and a drive towards "open innovation", in which a company's search for new business solutions is outsourced to suppliers, customers and a variety of short-term "partners" including even competitors. (This new landscape is explored in more detail in Chapter 1.) The job of tending to information – no longer the exclusive province of IT or security but engaging every operational and strategic part of the enterprise – has never been more complex or rewarding, and it is my hope that this book will enable everyone responsible for creation and protection of ideas to make fewer mistakes and to deploy their intellectual property productively.

Reading this book will give you a deeper understanding of how your business differentiates itself from the competition, and how it must work to keep its edge. As an executive or manager or small-business owner you will come away armed to protect and exploit your company's advantages. As an individual you will have a greater appreciation for what intellectually belongs to you and how to use it to advance your career without being sued. And whatever your interest or line of work, you will have a much better understanding of how information has become the global currency of the 21st century.

Chapter 5

MANAGING YOUR INFORMATION ASSETS

NOW THAT WE have addressed what trade secrets are, who owns them, and how the law protects them, we can start to deal with the core message of this book: how to manage these valuable assets, keep them safe, stay out of trouble, and maximize their utility in your business. When you finish this chapter, you will have a good overview of best practices in information protection, ready to augment that understanding with a deeper examination, in the material that follows, of some of the most critical drivers of success: how to avoid contamination, how to deal with departing employees, and how to handle business secrets in a global environment.

This is a business book, not a technical one, and so our coverage of the very hot topic of cybersecurity will be from the perspective of management. The technologies that are used to hack and spy, as well as those used to defend, are constantly changing. Our job here is to identify the general nature of those technologies and establish a rational way to lead your organization to information security in an unsecure world. By reading this chapter you should understand much better how to deal with security advisors and vendors, and how to optimize your cybersecurity efforts.

As you may already appreciate, almost all aspects of information security management boil down to risk management, which begins of

course 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.

Creating an Information Protection Plan

There are two major reasons for creating an information protection plan. The first, as we have already seen, is that the courts expect you to have one, and will help you with a problem only if they see that you have already exercised "reasonable" efforts to prevent it. Along the way, your efforts should also impress your employees and other relevant actors, who will come to learn that protecting your trade secrets is a priority. But beyond the demonstration effect, there is of course the objective of actually preventing loss and contamination, or mitigating the effects of a loss when it happens (as it likely will). So your goals here are two: prevent problems and show you care about them.

When I started in this field, 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 provided a compliance framework for avoiding inadvertent criminal misappropriation. (They remain relevant, as we will see in Chapter 12.)

The NIST Framework

Today, particularly in the wake of high-visibility cyberattacks on major companies and government agencies, emerging standards are

front and center. Perhaps the most significant of these was published in February 2014 by the National Institute of Standards and Technology (NIST), entitled "Framework for Improving Critical Infrastructure Cybersecurity." As the title suggests, the document – which will be revised over time – is directed at "critical infrastructure," which includes not only government networks but also the banking system, the energy grid and the like. So what relevance does that have for you if you run a different or smaller enterprise that perhaps isn't essential to keeping the lights on and money flowing? The answer is that the framework was reasonably well designed and is expressed in terms that are applicable to most businesses regardless of size or sector or nationality. Therefore, in the search for ways to advise boards and managers about this increasingly important issue, the NIST Framework is a good place to start.

For one thing, the Framework is expressed in terms of classical risk management, making it easier to integrate information security into other corporate functions. Despite the catchy "cybersecurity" in its title, the document provides guidance that applies broadly to the entire job of protecting data integrity. Its basic message is this: do what you can, to the extent it is both helpful and affordable. It describes separate levels of controls according to their complexity and cost (in terms of transactional overhead as well as expense), making it straightforward to begin the process of designing a system that can work for your business. As an Intel manager recently reported, their pilot project using the NIST Framework helped "harmonize our risk management technologies and language, improve our visibility into Intel's risk landscape, inform risk tolerance discussions across our company and enhance our ability to set security priorities, develop budgets and deploy security solutions." However, even though the Framework is presented as a voluntary reference at this point, it is likely that some version of it will become mandatory for government contractors, and this could easily lead to its being considered a de facto standard for industry in general.

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 consulting or accounting firms, and suppliers of custom systems.

In addressing information security, you should differentiate between trade secrets and "custodial data" or customer privacy data. 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 it. But a report issued in 2010 by Forrester Consulting found that companies spend much more time and money on protecting against its accidental loss than they do on preventing theft of trade secrets, even though they value 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 special 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 it to no one, 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 documents 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 well-meaning former security officials, 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; they will 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 what matters most.

Number four may seem counterintuitive in the days of headline cyberattacks: the greatest risk is inside, not outside. The biggest problem is not with foreign hackers, but with your own 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, as we will see later in this chapter, that the single most cost-effective aspect of any information protection program is employee education.

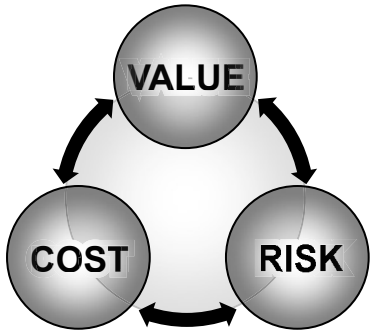
This point bears some emphasis. A 2013 study by the Ponemon Institute, based on a survey of over three thousand trusted employees in six countries, employed in companies of varying sizes and in various

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." This report has relevance not just to how you educate your current employees, but also how you screen new hires, who may be inclined to do you a "favor" by bringing over some of their work. (More on that issue in Chapter 8.)

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 number one 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 them. 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

As I pointed out in the last chapter, a useful rule of thumb here is reflected in the value-risk-cost triangle:



Keep in mind that risks, or threats, change with time and circumstance, and so risk assessment must be a continuing process, reconsidering the program at reasonable intervals. It is also important to revisit your plan in connection with mergers and acquisitions, where the challenge is to integrate legacy entities with their 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 in 2011, surveying over 600 experienced IT security professionals, found that in 88% of companies the security budget was smaller 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 pushing 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 (I have suggested a barebones approach below), 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 phones. 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.

As I pointed out in the introduction to this book, 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.

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 "fail[ed] 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. And even though this case was about data privacy, it's not much of a leap to imagine similar claims being filed about neglect of technology security issues. Finally, as we will see in Chapter 12, avoiding criminal liability for receiving trade secrets may require establishing compliance plans that include intense 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 all companies will have to confront external expectations about their management of data security.

Insurance coverage

Can you insure against these risks? Yes, to an extent. However, look carefully at coverage and exclusions in cyber insurance. The lack of reliable data about losses makes it hard for insurers to handicap the risk, and so they can be expected to protect themselves with high premiums and deductibles. And keep in mind that there is a certain moral hazard in believing that insurance will take care of the problem, leading you to drop your guard a bit. You can't afford that in an area where losses may be unknowable or in the worst cases catastrophic.

All that said, there is no such thing as perfect security in the business context. The most you can hope for is to reduce risks to a level that works for you. As security expert Vincent Berk has said, "The only instance where you can be truly secure is when you have nothing to protect and there is nothing at stake."

Models For Protection Plans

In fact, almost all businesses have a lot at stake in protecting their data. Now we turn to the specifics of trade secret protection plans.

It shouldn't surprise you to learn that there is no one-size-fits-all approach, since this like any kind of risk management is driven by the special circumstances of your business and the sector in which you operate. Regulatory and other special compliance environments can affect the design of your system. And the contracts that you enter into may include very specific provisions on handling information belonging to others. But there are common issues: inventory, physical security, electronic systems and devices, document control, external relationships, and employee hiring, education and firing. The best way to understand options and variations is to consider what a basic program might look like according to the size of your business, which we will take as a rough proxy for the kind of threats you face and what you can afford to do to address them. Following that review, we will dive deeper into several areas that need special attention.

The basics, with options to grow your plan

Let's start as most businesses do, relatively small. Small and Medium Enterprises (SMEs), measured by a variety of yardsticks (anywhere from 10 to 500 employees), have certain advantages but also face particular challenges when it comes to information security. Being innovative and nimble, they are naturally flexible and can adapt quickly to changing environments and demands of larger companies whose needs they often fulfill. But with smaller size comes fewer structures and resources to attend to security, even though SMEs often face the same kind of risks as much larger companies. But this is just a challenge, not a barrier or an excuse. There is a lot that SMEs can do to identify and reduce their risks, and along the way develop perspectives and tools that will continue to serve them well as they grow.

The core of any security management program is the manager's attitude. As stated elsewhere in this book, losses happen mostly because someone is not paying attention, not because of deliberate espionage. So the most effective risk mitigator and loss deterrent is

an informed and engaged workforce. That tone has to be set at the top, and a large portion of your success will be determined by management's commitment to the project.

The second basic element is awareness of the risks, by understanding what your trade secrets are, as well as the threats that they face. Here is where we sometimes lose executives who resist the distraction and costs of an "audit." But for a smaller business, it doesn't have to be complicated or time consuming. It can be done by calling together the main people in the company who (a) know what you have (or are caring for on behalf of others) that is sensitive and valuable; (b) know the areas of likely leakage or loss – including gabby salespeople and careless engineers; and (c) can readily assess the effectiveness of specific policies and control measures. Don't rely here on just security people, who in my experience are often inclined to impose maximalist restrictions and lock everything up. That is just not possible in the modern corporation, certainly not one that expects to find success through collaborations. So in your design process include managers with responsibility in research and development, sales and marketing, operations, human resources, communications and legal.

With the value-risk-cost triangle in mind, this group should brainstorm the issues to come up with a plan that is likely to match the vulnerabilities that you face, that is simple and that can be managed by a single responsible executive. This last point is very important. Security will be structurally compromised by distributing functions among managers perceived to have a special stake in it. One person has to be in charge. And that person needs to have ready access to the CEO and the ability to command respect at the board level.

At a minimum, the plan should specifically address these areas:

- Premises security. Visitors should sign in and be escorted, and leave their phone cameras behind. Access to especially sensitive areas should be controlled. Data-rich computer displays and sensitive documents should be located in private spaces and locked away when not in use.

- Classification. Information contained in documents, including electronic files, should be designated where appropriate as confidential. Remember that information should be available for access only to those who need it.

- Process security. Robust password (or better) controls for appropriate access into parts of the system. Firewalls. Encryption on mobile devices.

- Contracts. Employees should sign confidentiality and invention assignment agreements. Outsiders should be allowed sensitive access only under confidentiality agreements.

- Education. Employees, including executives, should be trained on basic information security.

When you can afford it, extend your program with these elements:

- Rules: publish clear, simple but comprehensive rules and policies covering information security.

- Responsibilities: delegate clear responsibilities and tasks below the primary manager; elevate overall management responsibility to a higher level.

- Preparedness: make information security part of a specific business continuity and emergency response plan.

- Review: establish and implement regular reviews of the program, to ensure its appropriate coverage and management.

For larger businesses, or those with higher information risks, do the above, plus:

- Full-blown security policies and procedures, including social media and email use policies.

- Comprehensive systems for managing security (planning, reviewing, improving) with accountability.

- Confidentiality agreement (NDA) and third party due diligence (for collaborations and outsourcing) management.
- More robust protection systems, such as stronger encryption and intrusion detection tools for networks.
- More extensive education of the workforce.

Throughout the process, no matter your size or resources, carefully consider:

- Related security issues that should be incorporated, such as protection for Personal Identifying Information (PII), which is subject to many laws and regulations designed to protect individual privacy and security.
- Relation to other corporate compliance programs, with opportunities for management efficiency.
- International issues: how do your risks and available mitigation strategies vary according to the markets in which you operate?
- Priorities: the value of information changes frequently; are you setting your priorities to focus on today's most important data?
- Attitude and cooperation: is your plan taken seriously by all areas of the business? Are there silos of resistance to cooperation?

If you are having trouble getting started with your own plan, there is help available. One excellent resource is CREATe.org, a not-for-profit organization that helps SMEs address their IP issues with an online self-assessment, evaluation and improvement plan. They also provide an extensive guidebook with model policies, procedures, checklists and training materials.

Special attention to electronic systems

Some issues deserve deeper treatment because of their importance and complexity. The first one is obvious: electronic systems, which are as essential to modern business as they are risky. In the past, many communications were prepared on typewriters and went off by mail. Meetings were in person. Calls were made over twisted copper lines that took some effort to physically tap. With the advent of modern communication systems, we have vastly increased our output, frequency and speed – and our vulnerability to loss. Each network, internal or external, has thousands or millions of "endpoints," represented by laptops, tablets, phones and other connected devices. (This is without accounting for the Internet of Things, or the Internet of Everything, as Cisco likes to call it, which it says by 2020 will have over 50 billion parts of cars, planes and refrigerators talking to each other.) Each of those endpoints is operated by a person who may be insufficiently trustworthy, or perhaps not fully appreciate how he is using his device in a way that may leak data or act as an open gate to receive unwanted information, including malicious software. This is the brave new world in which today's information security professionals have to operate.

As with the general trade secret protection plan, electronic systems security begins with a cross-functional effort to identify and mitigate risks. Here, because of the speed and ubiquity of communications, a core principle is "data ownership," in which a single individual is supposed to take responsibility and be accountable for the classification of a particular document or file that goes into the system. As already noted, the classification system ideally will be simple and tailored to the practical needs of the business. Classification is tied to an acceptable use policy, which supports ready access to particular information by those who need it, while protecting it against misuse. The entire system becomes the subject of intense training of employees and contractors, to influence safe behaviors and serve as

a notice to those that might be tempted to let down their guard or deliberately redirect sensitive data. Finally, the most comprehensive systems include monitoring functionality: knowing where data are "at rest" and "in motion" at all times, requiring in turn that the system be capable of inventory and tagging so that it can track what matters and log everything as appropriate.

User behavior

A major component of most IT security systems focuses on user behavior by implementing systems designed to control access, the most famous – or notorious, depending on your perspective – of which is the password. Subject to mounting criticism – after all, the most popular password used by real people is "password;" and even strong passwords can be detected by key-loggers or wheedled out of busy executives by a sophisticated phishing attack – passwords are likely to be mostly replaced in the near future by two-factor authentication, in which identity is assured by a separate text or email message to the user containing a one-use code. In the long run, biometric systems such as fingerprints or iris scans will be widely used to assure a higher level of trust. This rapid evolution of technological solutions should remind you that your job as a manager of this function – your requirement to use "reasonable efforts" to protect your trade secrets – is a moving target that requires periodic reassessment.

Personal devices

After people and their behaviors, it is equipment that attracts the most attention from information security specialists. Realizing that a great deal of information loss, as well as infection from unwanted files, occurs through use of the ubiquitous USB drive, some government agencies and companies have disabled those ports on their computers. Laptops always require special focus because they (along with smart-

phones) travel with their users, requiring procedures for use in insecure countries. Some executives take stripped-down mobile devices containing only the bare minimum required for the trip, and then have them cleaned on return. Whatever the risk profile of your particular environment, you need to account for the fact that large amounts of your data, as well as authorized connections into your network, move around the globe and require sensible controls.

For security personnel, perhaps the most alarming and vexing development of recent years is the "BYOD" (Bring Your Own Device) phenomenon, in which employees bring their own smartphones, tablets or laptops to the office, connecting them to the network, and more or less scrambling their personal data with the company's. For a long time, this development was resisted, on the reasonable basis that it would be impossible to provide security, much less technical support, for such a varied and uncontrolled collection of devices. But social momentum having swamped those concerns, businesses now have to adapt to a new set of risks. Policies and procedures regulating use can help, as does registration that requires installing remote wiping functionality in order to protect corporate data when a device is lost. This is just one aspect of technical solutions offered by products collectively known as MDM, or Mobile Device Management, software.

Connecting all these devices is the company's network, and of course this part of the system deserves close attention because it is at once the way that open and robust communication takes place with the outside world, as well as the way that the outside world frequently uses to break in and cause damage or steal data. A large variety of tools can be used to defend your network, and the offering is constantly changing. In any event, this book is about how to manage the process, not about how to pick a solution.

Focus on network breach detection

That said, you should assume that antivirus software is not enough

anymore. And one message I hear frequently from security professionals is that you can't hope to keep everyone out all the time. Some will even say that a focus on guarding the network perimeter is both delusional and dangerous, because it saps resources from the two other jobs that have to be done: breach detection and response planning.

So with networks as with other aspects of data integrity, security is relative, and a multi-layered approach is necessary, beginning with understanding that your network is vulnerable, has been breached, and will be breached again. You're not aware of any breaches, you say? There is the root of the problem. Data loss is not like theft of other property, which leaves a gap when it's gone. Data are read and copied, but otherwise left alone. Indeed, some things are added: malware and spyware. The theft itself is silent and – if the thieves are very sophisticated – leaves very few if any clues that someone has broken in.

When you hear the term Data Loss Prevention (DLP) tools or software, remember that point: the best technical solutions will monitor the entire network, addressing not only breach and loss, but also – and sometimes primarily – detection of attacks. Happening by the dozens or even hundreds per day, these attempts, whether or not successful, can generate useful information about where hackers are coming from, what they are using to try to get in, and what they want to get.

These systems can monitor not only what is happening outside the walls, but inside as well, such as the employee now sitting at a desk and inserting a USB stick into the computer. Using learned intelligence about what sort of data is most sensitive, the tool determines whether that kind of usage might violate protocols and put secrets at risk of improper disclosure. It looks for unauthorized applications running on the network, and instances of information being copied to removable media, printed or especially transferred to vulnerable sites like Facebook, Google or Dropbox, attempts which it can block for specific kinds of documents or particular users. Some can even monitor the security behaviors of individual employees and provide scoring on awareness that will tell you how well your security training is working.

The Cloud

What about that wonderful extension of (if not replacement for) your network, the Cloud? First, let's de-mystify the thing: in many ways it's just a larger and more complex version of mainframe timesharing networks that existed decades ago. But they now are ubiquitous; if you use Twitter, Facebook, Amazon or Google, you are flying in the Cloud. The fundamental security challenge with the Cloud is that your data are under someone else's control, more or less. The more or less turns out to be both critical and controllable to an extent, because for many applications you can choose among Cloud vendors and you can negotiate levels of protection and separation of your data from others', or even a specialized form of "hybrid" that leaves your most sensitive data inside your walls, while using the Cloud for the rest. But generally it's like renting an apartment, where both you and the landlord have a key. And this landlord's facility may be a special target for data hackers, in the same way that banks are attractive to thieves because that's where the money is.

Beyond generic Cloud services that provide a place to park your data, some of the fastest growing businesses have been selling a specific species called Software As A Service (SAAS). They run the software tools, you provide your data for processing, and they deliver the results back to you. If we can employ another metaphor here, you are taking your laundry to a facility that may wash it with others'; naturally there is some possibility of contamination.

But the Cloud, properly managed, can be enormously effective and efficient not only in handling normal processing of your confidential data, but also in providing very sophisticated monitoring and detection tools at a fraction of the cost of running your own, and often with better reliability and disaster recovery capabilities. The primary management issue is the relationship with your provider, who will have control over the security of your sensitive information. Therefore, due diligence, contractual restrictions (e.g., encryption, confidentiality

and segregation of data), guarantees on support, availability, and compliance (and no limitation of liability, especially for security breaches) will be very important, as well as continued monitoring/auditing to make sure that the supplier performs as expected.

Incident response plan

As I've said before, there is no perfect security; and where electronic systems are concerned it's not an issue of whether, but when and how you will suffer a loss. This implies a critical management responsibility: you must be prepared with an incident response plan. There are vendors and government agencies that can lend a hand with the usual gap analysis and scenario planning that will allow you to assign responsibility and ensure that you know what to do when the alarms go off. As McKinsey points out in its publication "How good is your cyberincident-response plan?," "Even if you have emergency response plans, the chances are that they are not designed for cybersecurity issues, and the review cycles are not sufficiently frequent to cover rapidly evolving security threats. And it's not just timing, but spread of exposure, that changes rapidly as the modern company evolves its relationships and therefore its cyber connections."

Training the workforce

Reading about the cyberthreats facing today's global industries and contemplating the costs of meeting those threats may leave you dizzy and discouraged. But there is one area where I guarantee your efforts as a manager will pay off: training. Chisel this message into your memory: most trade secret losses happen from the inside, not the outside, and they happen because of negligence, not deliberate theft. Dwell on that thought for a while. If you can turn the tide of carelessness by raising awareness, you will do more for your company's information security, and at a much lower cost, than all the network protection

systems you might install. A quality training program will engage your employees as part of the security defense team, not only making fewer mistakes themselves but looking out for the mistakes of others.

What kind of mistakes am I talking about? The kind that make you slap your forehead in disbelief. The sales manager at a trade show who, excited about closing the deal at hand, lets slip the existence of an unannounced product. The engineer who brags to his friends on Facebook about a patent application he's just filed. The R&D director who hires someone from her former employer in order to get an "update" on what they've been doing since she left. The business development executive who examines potential licenses of technology without walling off company employees who are working in the same area. These are the kind of mistakes that provoke litigation, and they are all preventable. It's about attitude and learning.

In her very engaging and useful book "Positively Confidential," Naomi Fine makes the important point that it's not confidentiality agreements that provide protection to trade secrets – it's the people who make up the corporate ecosystem who do that through their informed awareness. So how do you get your employees, who by regular use of social media are encouraged to disclose the minutiae of their lives, to protect company secrets? A lot rides on the answer to that question; remember, someone can reveal a lot in 140 characters.

First, make the process inclusive. Not just people who you think are most likely to be exposed to confidential information, but everyone in the company should understand the importance of the issue. Even contractors, temporary employees and interns should be part of the effort. In fact, they may be even more important because they have inherently less loyalty and are more likely soon to be working somewhere else.

Second, make the training interesting. To keep it fresh and positive, consider using specialized vendors or products that can present serious material in a lighthearted but memorable way, rather than relying on internal managers to conduct classes.

Third, be sure that training is not an event but a continuous process. Follow up with email tips, stories, refreshers. And if business conditions worsen and you start to lose employees, this is a time to increase your training effort, not cut back, because the people who remain represent the source of your intellectual capital.

Collaborations

As Marshall Phelps, Microsoft's former Vice President for Intellectual Property, has said, "few if any companies today can hold all the pieces of their own product technology . . . . [T]hey simply must collaborate with others if they want to survive and prosper . . . . IP has become much more of a bridge to collaboration." Or as the Federal Trade Commission put it in a 2011 report, "Technology has become so complex that it is impossible for a single business to be the source of every invention that comprises a single product." In the immediate post-war era, the best innovations came out of Bell Labs, and the most favored form of business was the fully integrated corporation, responsible for its own technological destiny. In that environment, trade secret protection was pretty much limited to making sure that what you did inside the walls didn't go outside. But Bell Labs is no more, and globalized markets require a much more nimble innovation strategy that takes advantage of the perspectives and expertise of other companies. Going it alone may be more secure, but there's too much risk that you won't get it right.

As a result, even a company's basic research and development increasingly is done through outsourcing and other forms of collaboration. In effect, this is about shared creation. In its ideal state, synergies enhance the capabilities and learning of each partner. Rewards and resources are shared, but so are risks and responsibilities. Therefore, trust is a key driver of success, and that is why the enforceable confidence of the trade secret framework is so important.

Open innovation

A currently popular term to describe this shift is "open innovation," coined by Professor Henry Chesbrough at the University of California. The basic idea is that you look outside the company for what may be the best approach to design, engineering, production, marketing or distribution. This can take various forms, from simple outsourcing, to collaborations with other companies, to the "virtual enterprise" which knits together independent parts to form an operating company. The common theme, however, is trust; in each one of these relationships there will be some sharing of sensitive information on a confidential basis. And that requires careful management.

Let's pause and distinguish "open innovation" from its confusing cousin "open source," which typically applies to people or entities coming together to create something, such as open source software like Linux, in the public interest, where access is more or less free. That is not what we're talking about here, where "open" does not mean free, but only that you are going outside your own organization to get help for a commercial project. And we should also distinguish the various forms of public prize systems. Charles Lindbergh won such a contest when he became the first solo flyer across the Atlantic in 1927. Today, the tradition is continued by various organizations and governments, perhaps most famously the XPRIZE, which awarded $10 million for the successful launch in 2004 of the first commercially-developed passenger vehicle for space travel, SpaceShipOne. These efforts succeed not by sharing secrets but by publishing specifications and rules for everyone to see.

Buy vs. build

The basic question behind every collaboration is whether to build it yourself, to buy it from someone else, or to work with someone else to create it, where the "it" is typically some new product or technology.

Building it yourself increases control over the development, the intellectual property and the market opportunity, but represents the highest risks, with potentially higher costs and time to market. Buying shortens the time to market, but you face acquisition costs and inefficiencies of integration. Collaboration, while reducing control and profit opportunity, lowers most risks and costs, potentially speeding time to market and increasing credibility.

In the world of trade secrets, buying comes with a special set of risks. These arise when you begin to search, or "scout" for the best available alternatives. This can take the form of buying a license, buying a product line or even buying a company. The risks come in how you conduct the search. In order to assess the value of each of multiple options, you will likely be required to sign NDAs that restrict your ability to use the information you learn for any purpose other than evaluating that potential acquisition or license. (See the sample nondisclosure agreement in Appendix 2 for typical wording.) Therefore, you need to manage that process to minimize unnecessary exposure to others' information, and to be sure that you comply with the obligations in each NDA you sign. I will say more about this subject in Chapter 8 on avoiding contamination.

Managing collaborative work

Collaboration in its many forms also carries its own set of risks. Recall that trade secrets, unlike other types of intellectual property that come with a government-certified description, are inherently vague and difficult to define. In the course of a collaborative project, ideas move freely in the possession of many individuals, and any misuse by a recipient may be unknown to you, and perhaps unappreciated by them. Casual communication can become sloppy. This is why the most important aspect of any collaboration is the know-your-partner rule. In other words, make sure that the relationship is mutually respectful and that you have a solid basis for trusting this company or person.

And don't forget to follow up when the relationship is ending, so that confidentiality expectations are clear.

That doesn't mean that the law can't help. In fact, the second most important rule is to be careful about your contracts. A collaborative business relationship often proceeds like a romantic one: courtship, commitment, (open) marriage, and divorce. Each of these phases requires a clear understanding about trade secret and other IP issues, and we will discuss the specific contract issues in the next chapter. But for many of the same reasons, the relationship requires more than contracts; it needs close management.

At the outset, team members on both sides tend to be a bit emotional: positively with love and anticipation, or negatively with jealousy or resentment. ("We should have done this on our own; why are we involving these idiots?") So you need to ground everyone (and be sure that your business partner does the same) with an appreciation of why the decision was made, what the goals and strategies are, and what the likely challenges will be in making it work. Do all the managers understand what must be shared, may be shared, can't be shared? Do they know how to document the specific contributions made by each side? Do they know how to communicate with the partner in a secure way? (There are software packages with encryption designed for collaborations.) As in any project, attention to these issues may flag from time to time, and so you should periodically perform a review to make sure that everything is on track.

Consultants and Contractors

As we've already seen, managing your employees and their attention to security issues is a challenge in part because of turnover: the average employee changes jobs eleven times during a career. Well, the consultant who you have working on your project may be juggling eleven others at the *same time*. And some of those projects may be for competitors, or for others who might be able to make use of your secret

data. So from the employer's point of view, these relationships deserve very special attention. This starts with deciding whether and to what extent to use outside or temporary resources on any given project, while taking into account the security risk. If you accept that risk, it will be partly because you mitigate it by choosing carefully, by discussing with the candidate how they intend to assure protection for your data, by preparing an airtight contract, and by managing their work and information exposure accordingly. See more on this in Chapter 6.

These same issues will surface, from a different perspective, for consultants themselves. As a consultant, you need to confront a tension-filled reality: you typically serve a series of short-term bosses, some simultaneously, in closely related businesses. In fact, it is your ability to "cross-pollinate" good ideas that may make you attractive to some of your clients. But frequently people become more focused on who owns the "pollen" that you pick up in your various assignments, and that can get tricky. As a result, one of your most important business survival techniques has to be clarifying your relationships with the utmost precision. This should begin with a frank discussion about the possibilities for conflicts of interest and how you intend to deal with them. Your objective in these talks should be to identify the information you learn or generate on this project that can't be characterized as just skill or experience; and then to come up with very specific ways that you will be able to separate and protect that information from misuse on other projects. Finally, these understandings need to be recorded in your contract. In this way, the problem will be out on the table and much less likely to lead to mistakes and litigation.

Commercializing Secrets

As a manager of your business, it is your responsibility to make sure that your trade secrets – your information assets – are actually exploited, to realize the competitive advantage that they represent. To

fail in that task would be worse than the money manager who just parks cash where it's safe but earns nothing. With trade secrets, you have to assume a rapidly deteriorating asset. The trick is to deploy that asset while it holds value, in order to sell a better product or service, or to leverage relationships with others who can use it themselves or in cooperation with you.

We have already looked at how open innovation and collaboration have changed the landscape of industry. The point here is that you need to think beyond the creation of information that you know has value, and focus on how you're going to extract that value. Consider for example the energy sector. Maps are one of the classical repositories of trade secrets, and oil companies spend huge resources in seismic studies and other investigations yielding potentially useful clues to what lies beneath the surface and how it might be extracted. According to McKinsey, when an energy company combines its own data with similar information from one or two other companies, this can reduce costs and time for development of the field by 15 to 25 percent.

In a similar vein, consider GoldCorp's variation on the XPRIZE: its Open Challenge in 2000 began when it put on the Internet 400 megabytes of valuable map data about its Canadian mining property, opening it all for geologists and engineers to take a look and identify promising sites. More than 1400 did (the winner was a group from Australia that had never visited the area), with the result that the mine paid off handsomely: $575,000 in prize money against $6 billion in gold extracted, and years faster than if they had used old-fashioned exploratory drilling. There are many ways to make money from secrets.

If your company doesn't have the complementary assets to build and market its own product based on your secret information, then you may well decide to exploit it by licensing it to someone who can take it to market, in return for royalties or some other consideration. It's generally agreed that trade secrets have enough of the attributes of "property" that they can be sold or rented. (They can also be taxed like other property.) So in many ways the trade secret license is similar to

any other business transaction where the owner parts with rights in something of value.

But remember this special characteristic of trade secrets: they have a potentially perpetual life. This has important implications, particularly if your information or innovation is sufficiently desirable that the licensee is willing to take the risk that it may become generally known over time. This apparently was the situation back in 1881 when Dr. J.J. Lawrence licensed to Jordan Lambert the secret formula for what was to become one of the most successful over-the-counter pharmaceuticals of all time, the antiseptic mouthwash called Listerine. Lambert, who later formed a company that became Warner-Lambert, agreed – in a contract that ran for all of two sentences and 127 words – to pay Dr. Lawrence twenty dollars for every 144 bottles sold. The deal helped make Lambert and his company wealthy. Dr. Lawrence also did well, as did his heirs, who continued to collect millions in royalties through the middle of the last century. In the meantime, during the 1930s the formula became known, through no fault of either side. Listerine was still enormously popular, and profitable, but in the 1950s Warner-Lambert sued for an order that it shouldn't have to pay any more because the secret had been destroyed. The court refused, pointing out that Lambert had made his bargain and was stuck with it.

The Listerine case demonstrates the potentially enormous value of a "head start" in getting quickly into a market. You can easily imagine this principle being applied to a still-secret (that is, not yet published) patent application. The licensee may be counting on the hope of patent protection in the long term, but in the meantime, it believes that the first mover advantage offered by the secret will allow it to capture market share. The smartest move for the trade secret holder may be to negotiate for the biggest possible up-front payment for the trade secret rights, because the patent may never issue at all. The law will not enforce royalties on a patent that never issues or is found invalid, but the trade secret royalties may go on indefinitely.

While licensing trade secrets can be advantageous, there are serious challenges inherent in most transactions. The first of these is valuation. If you have a patent, you can at least assume that there is no one else with the same rights. But secrecy is not exclusive, and so it is impossible to know if the technology you're trying to license (or its equivalent) is known to, and perhaps being used by, other companies in your industry. Secrets frequently suffer a discount in valuation because of this uncertainty.

The other problem is transactional: the holder of the secret is reluctant to reveal everything until the potential buyer has committed; but the buyer will not commit without knowing exactly what is being offered. This conundrum, known as Arrow's Paradox, is a major reason why licensing a patent is less risky than licensing a secret: you can see it and understand how it works. In practice, trade secret transactions succeed through what I call "incremental partial disclosure." For example, consider the initial disclosure that takes place at a trade show where a prototype product is displayed, and the results of its use are described, but nothing is revealed about how it achieves them. Its design is sufficiently opaque that prospective buyers can't infer how it's done, or even whether it's some sort of trick. At this point, the buyer will ask some questions to derive a hint at how it works, or at least raise confidence that it's real. In the meantime, the owner, judging the sincerity and trustworthiness of the buyer, may be willing to risk saying slightly more in the hope of getting the deal done. This iteration continues until the buyer is sufficiently comfortable to sign a nondisclosure agreement, allowing an inside look at the prototype.

What I have just described as a hypothetical process at a trade show is the way that most trade secret deals are done, although they occur over weeks or months, with multiple meetings and exchange of correspondence. If the holder of the secret is a very small enterprise, or an individual, it may take longer, or not happen at all. (For a discussion of the realities of unsolicited idea submission programs, see Chapter 8.)