Intellectual Property Checklist for Start-Up

Adapted from The Entrepreneur's Intellectual Property & Business Handbook[1]

Jon M. Garon

Even the smallest of start-ups have intellectual property (IP) worth protecting. From your business name to the innovative design of your product, you will have assets that set you apart from other businesses in the market. The importance of these IP assets will only grow as your business matures, so it is important to get things right from the start.

There are six categories of IP and related rights to consider in your business strategy: Trademarks; patents; copyrights; trade secrets; publicity rights; and internet domains. A successful IP strategy integrates all six of these assets for maximum value. A business without any of these IP rights is a commodity that will not be able to gain market share from away from established competitors.

Trademarks may be comprised of simple text or they may be comprised of graphical images, pictures, sounds, or other works that are also protected by copyright. The company must be sure to acquire both the copyright and trademark right in the image used to become a trademark. If the trademark is comprised of a name or image of a person, such as the restaurant Wendy's, then the publicity rights of the person depicted must also be obtained to be used in the trademark.

The selected trademark and domain should be integrated to the greatest extent possible, though they do not need to be identical. For example, either can be an abbreviation for the other.

Copyright law protects an author's or artist's expression. It includes literary, pictorial, graphic, music, and similar works. Copyright does not protect the underlying ideas, however, only the particular means of expressing those ideas. Registration is not required to protect a copyrighted work, but registration is required to file a lawsuit to protect the rights, so the most important copyrighted photographs and manuals should be registered.

Publicity Rights protect the commercial use of a person's name, likeness, or other attributes of identity. A person's rights of publicity cannot be commercially used without permission. Properly licensed, they create an important exclusive relationship between a celebrity endorser and company selling a product or brand. Publicity rights are protected by a combination of state laws and federal unfair competition laws.

Trade Secret laws protect confidential information that derives its value from its secrecy so long as reasonable efforts have been made by the owner of the trade secret to protect the confidentiality in the information. Examples include financial, business, scientific, engineering, marketing, or technical plans. A start-up company's business plan may be its first trade secret. At the same time, however, most potential investors, banks, and landlords will want to review the business plan and will not be willing to sign a nondisclosure agreement (NDA). By disseminating the business plan without an NDA, the company has generally failed to take the reasonable steps needed to secure the trade secrets embodied in the business plan. To resolve this problem, sophisticated start-ups will separate out the truly confidential aspects of the business plan from the general document,

[1] For a Free PDF Copy: https://garondigital.com/the-entrepreneurs-intellectual-property-business-handbook-2nd-edition/.

reserving the disclosure of those critical components to the smaller group of potential investors who are sufficiently committed to the project to sign an NDA.

Patents are the most expensive and broadest form of intellectual property. Patents protect new, useful, and nonobvious inventions, processes, or compositions of matter. Anyone who makes, uses, offers to sell, sells, or imports a patented invention infringes the patent. As such, the patent even stops an independent inventor or the lawful owner of the invention from another country. Unlike the other forms of IP, patents are highly technical, and a company should only file a patent through an experienced patent attorney or patent agent. Because the patent rights are so powerful, the law makes it very difficult to claim and defend patent rights. Moreover, patent litigation is extremely expensive, so the scope of a patent should be carefully considered when developing a start-up based on a new invention.

Internet domains (e.g. URLs) are not IP rights, but the Internet is the front door to the business. Ownership of the company's name or key attribute in the domain is very helpful. The social media names and domain addresses should all be consistent and unified. Toll-free phone numbers are less important but still useful. The domain name is generally not a trademark, but it can incorporate the trademark of the company. For example, www.autotrader.com is comprised of the trademark Autotrader® with the top-level domain of ".com." There are now hundreds of other top-level domains, but .com still dominates U.S. markets.

Steps to Prepare the Start-Up[2]

1. Pick & Prioritize the Right Intellectual Property for Your Company: The right combination of IP rights provides the key to business success. IP rights are about exclusivity. It does not, however, take too much separation to claim space in the market. A strong trademark is often more valuable than a weak patent. Copyrighted images, stories, and support material can distinguish one business from another. Trade secrets protect a business without disclosing the information to the public and can last indefinitely, provided the secret can be kept.

In the hands of the right celebrity, a simple product can come to life. The value of that celebrity can transform a generic product into an in-demand top seller. As such, each of the five forms of intellectual property plays an important role. Patents are the strongest form of IP protection, but they are the most expensive to establish and the most expensive to defend. For a truly new invention or composition, however, patents are the best solution.

Alternatively, if you think that competitors will not be able to copy or reverse engineer the technology, then you might consider safeguarding it as a trade secret, which will require certain steps to maintain its secrecy.

[2] Steps to Prepare the Start-Up adapted and reprinted from:

- NI Business Info, https://www.nibusinessinfo.co.uk/content/intellectual-property-checklist-start-ups
- Intellepro, IP Protection, https://www.intellepro.com.au/new-business-here-is-your-ip-checklist/
- Sam Wu, Innovation Capital Law Group

Otherwise, pursue patents. Think of a patent as a tradeoff – in exchange for disclosing your invention to the government and general public, the government offers you the right to exclude others from practicing your invention for a period of time. Of course, your invention must meet certain requirements in order to be patentable, such as being unique and not obvious over the prior art.

Before launching, consider whether you want to pursue any foreign patent protection. If so, you must secure a patent filing date before disclosing the invention to the public. If you're concerned about patent protection in the US only, keep in mind that you must apply for a patent within 1 year of your earliest disclosure of the invention.

2. Get All Founders to Assign Intellectual Property to Company: Why should anyone believe in a startup where the founders have not given their relevant intellectual property to the company? Imagine trying to raise capital, and a potential investor asks what would prevent any one of the co-founders from departing and starting a competing business.

- Each co-founder should sign a legal document transferring their relevant intellectual property to the company. While you're at it, any signed employment agreements with the founders' former employers should be reexamined to see if a potential ownership dispute may arise over the IP to be assigned to the startup. Do this at the earliest possible stage of your company, which means now if you haven't done so already.
- Also be sure to have all employment, freelance and consultancy contracts clearly state your ownership of all intellectual property developed for you.
- The agreement should also be clear that there are no valid legal claims that can be made by any other parties. If there are former participants that are not part of the current team, then those individuals should sign releases regarding any ownership interest.

3. Carry out clearance searches: Before you invest time and money building up your business under a particular name, check that this name isn't already in use. Search for trademarks that are in use, both registered and unregistered, and remember to check names as well as logos. This will help avoid unnecessary conflict with any pre-existing rights.

4. Check if a domain name is available: Before you decide on your trademark, you may want to check if a suitable domain name is available. You will want one that relates to your chosen trademark and hasn't already been taken up. You may want to check for and register variants of your chosen domain name.

5. Budget & Funding for Intellectual Property: Protecting your startup's intellectual property on a limited budget can be difficult, but not impossible. Of the 3 types of IP filings – patents, trademarks & copyrights – utility patents take the most time and money to obtain.

- Start with the simpler IP filings that require little to no funding: trademark, copyright, design patent and provisional patent applications.
- If you're willing to spend the time to figure out how to file a trademark application properly, then skip middlemen services and proceed directly to the USPTO site. If not, go with an experienced IP attorney who will perform at least a preliminary USPTO search prior to filing. There are experienced trademark attorneys who will prepare and file your trademark application at a fixed rate (Trademark app form). Fixed trademark attorney fees

typically exclude responses to USPTO rejections (i.e., trademark Office Actions) that require legal arguments and/or research.

- While a single copyright application is not a huge expense, the costs can add up if you have multiple works to register. You can save money by using an experienced IP attorney to help you group multiple works into a single copyright application if certain qualifications are met. Consult with an IP attorney preferably before launching because works that are unpublished may be easier to consolidate into a single copyright filing. Plus, a copyright owner will have additional rights to attorney's fees and/or statutory money damages if the effective date of registration is prior to the time when an infringer begins copying the copyrighted work.
- The variable cost in design patent applications depends on whether the required patent drawings may be avoided and replaced with photographs of the design, thus saving on patent illustrator fees. The USPTO may allow photos if they show the design more clearly than line drawings. So, a few thousand dollars may sufficiently cover the IP filings that should be made during the early stage of your business.

6. Register your trade name, brand and logo: This will help secure your rights and protect your assets from misuse. Remember that trademarks are territorial, so you will need to register them in territories that are relevant to your business.

7. Identify other types of IP assets you may have: As well as trademarks, you may have other types of intellectual property worth protecting. For example, design assets which you can register or innovative processes and equipment which you can patent.

- You should consider carrying out an intellectual property audit to help you identify the IP that you have and its value to your business.
- Keep a log of evidence recording the development of intellectual property: for example, dated and signed copies of drawings and drafts.

8. Keep information confidential: Take care not to disclose information about any new ideas or inventions before you've applied for protection. This is especially important in case of patents, as disclosure can make your application invalid. Read about getting patent protection for your business. Consider different ways of securing confidential information - for example non-disclosure agreements.

- Keep new inventions secret until you have decided whether their commercial viability justifies the cost of patent protection.
- Consider whether new designs for the appearance of part or all of a product are worth protecting with stronger design registration.
- Enforce your rights by identifying breaches and pursuing offenders but think carefully before initiating uncertain and expensive legal action.

9. Avoid infringing other people's rights: If you wish to use IP rights that you don't own, make sure that you seek necessary permissions in advance since this can lead to reputational damage, legal action as well as potential fines and penalties. You can license the rights or buy them outright. Be sure not to copy images from the Internet unless they are in the public domain. Even "free" images are often only free for noncommercial use. Failure to pay vendors for their work on copyrighted materials, trademarks, and patents can turn the breach of contract into a cause of action for IP infringement costing thousands times more for the business.

At-a-Glance Chart of Intellectual Property

	Utility Patents	Copyrights	Trademarks	Trade Secrets	Publicity Rights
Subject Matter:	Inventions or discoveries of any new and useful process, act or method, machine, manufacture, or composition of matter, or any new and useful improvement thereof	"original works of authorship," including literary, dramatic, musical, artistic, and certain other intellectual works	A word, phrase, symbol or design, or a combination of such, that identifies and distinguishes the source of the goods	A formula, pattern, compilation, program device, method, technique, or process, that: (i) derives economic value, being generally unknown and (ii) subject to reasonable efforts to maintain the secrecy	Name, nickname, likeness, biography, voice, and identity
Method Acquired:	Applied for by the inventor or joint inventors to the PTO. The entrepreneur or financing entity does not apply An employee "employed to invent" does so for the benefit of the employer, which will own the patent	Automatically acquired upon fixation of the work (paper, disk, computer memory, sculpture, etc.)	Through usage. ® May only be used after federal registration, but TM and SM may be used at any time	Initially, through usage, but maintained only through necessary steps to protect the secret	Varies by state. In most states, rights are automatic, but others require actual use of rights in commerce
Term:	20 years from the date on which the application for the patent was filed in the United States	Life of the author plus 70 years or works-for-hire have a term of 95 years from publication or 120 years from creation, whichever is shorter	Indefinite, trademark will continue so long as usage continues	Indefinite, trade secret will continue so long as secret maintains economic value and secrecy	Throughout lifespan of person in all states where recognized. States differ on length of protection after death
Time needed to acquire:	A patent application is generally published 18 months following the filing. The time for the issuance of the patent may be much longer	No waiting period. Registration with Copyright Office confers additional protections	May be acquired as early as 6 months prior to use in commerce, but generally acquired when mark is used in conjunction with the use of goods or services	No waiting period	No waiting period

Renewals:	Renewal not required but payment of “maintenance” fee is required Maintenance fees are due at 3 ½, 7 ½ and 11 ½ years from the date the patent is granted, due during a six month period preceding each period	None required for works created beginning 1978; renewal required for works published before 1964	An Affidavit of Use ("Section 8 Affidavit") must be filed between the fifth and sixth year following initial registration, and within the year before the end of every ten-year period thereafter	Not applicable	Not applicable
Federal Government Office and website:	United States Patent and Trademark Office www.uspto.gov	Copyright Office, a division of the Library of Congress www.copyright.gov	United States Patent and Trademark Office www.uspto.gov	None	None (some similar protection under trademark law) State law protection only
Applicable Law:	U.S. Patent Act, 35 U.S.C. §1, et. sec.	1976 Copyright Act, 17 U.S.C. §101, et. sec.	Trademark Act of 1946, 15 U.S.C. §1051, et. sec.	The Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836 Uniform State Trademarks Act (41 states)	Examples of state law: CA: Cal Civ. Code §3344; NY: NY CLS Civ R § 50 (2019)
Transfer:	Fully transferable, through a signed writing. It should be recorded with the PTO within three months of execution	Fully transferable, exclusive transfer only in writing signed by transferring party. Registration of transfer helpful but not required	Assignable. Registration available through USPTO	Fully transferable Care must be taken not to disclose the information before the transfer is complete	Owner of publicity rights may license use; licenses may be transferable
Property excluded from protection:	Laws of nature; Physical phenomena; Abstract ideas; Works of authorship; Any machine, process that is not new or non-obvious	Ideas, procedures, methods, systems, processes, concepts, principles, discoveries, or devices, listings of ingredients or contents; and Titles, names, short phrases, and slogans; typefaces; familiar symbols or designs	No protection for inventions, ideas, or products protected; Limited to protect the marks when used to designate the goods and services rather than exclusive ownership of the mark Trademarks do not prevent others from making or selling the same goods or services under a different mark	Any publicly disclosed information; Any information without economic value; and Any information independently created	Does not extend to non-commercial use of name, likeness, etc. One cannot stop news sources or unauthorized biographies, etc.

IP Licensing Fundamentals

1. An IP owner grants third parties the right to use its IP, while retaining their ownership.
    - Usually, the IP owner (the licensor) receives payment for granting another person (the licensee) the right to use their IP.
    - Payment may be in the form of advance, royalties, and fees.
2. IP Rights are divisible
    - "Channels," fields of use, product lines, medium lines, etc.
    - Geography, at the national or state level
    - Time
3. There are 3 primary forms of licensing agreements – each providing slightly different rights, advantages, and disadvantages.
    - **Exclusive Licenses**: grant a third party the exclusive right to use the intellectual property. The IP owner cannot use the IP or grant any other third parties the right to use the IP.
    - **Sole Licenses**: grant a third party the right to use intellectual property, while prohibiting the owner from allowing other third parties to use the IP. The IP owner may still use the intellectual property themselves, however.
    - **Non-exclusive Licenses**: grant others the right to use intellectual property, without restricting the owner from using the IP themselves or granting licenses to other third parties.

IP Business Planning in Practice

1. What is the problem being solved?
2. Who needs the solution the most?
3. How is the solution unique from that provided by the competition, and what IP is required to keep the competition from copying the solution?
4. What are the essential requirements to provide the solution, including the 5 IP rights, materials, distribution, partnerships, marketing, overhead and operations, etc.?
5. What does each of the essential requirements cost, so the cost of the solution can be calculated?
6. What is the revenue and in what channels?

Lean Business Planning Highlighting IP among Key Assets

1. **Value Proposition**: The business purpose is about satisfying a customer need or problem. It is not about an idea or product.
2. **Customer Segments**: These focus on social or demographic criteria that are uniquely suited or interested in the product or service. Few companies can sell everything to everyone. IP can help shape solutions into specific segments.
3. **Key Resources**: What are the most important assets required to make the business model work? Finance, facilities, location, customer lists, IP, human resources, etc.
4. **Channels**: How to get products to customers: Retail, online, events, more.
5. **Customer Relationships**: How the company acquires, keeps, and grows the customer base.
6. **Revenue Streams**: How to monetize each customer and business segment.
7. **Key Partnerships:** What are the key partners and suppliers needed to make the business work? What activities do they perform?
8. **Key Activities:** What are the most important things the company must do to make the business model work? What problems are being solved? Timeline?
9. **Cost Structure:** What are the costs to operate the business model? Which activities are most expensive; which might be optional?

The IP Exclusivity and Relevance model by Jon Garon incorporates and expands on the Score Business Model Canvas and the lean start-up guide of the US Small Business Administration.

Step 1: Get the Concept Right: The Value Proposition means the Idea is Highly Relevant to a Particular Market Segment that can be Identified, Nurtured, and Maintained.

Value Proposition The business purpose is about satisfying a customer need or problem period it is not about an idea or product.	**Customer Segments/Target Market** These focus on social or demographic criteria that are uniquely suited or interested in the product or service. Few companies can sell everything to everyone.
Channels How the company gets the product to the customer.	**Customer Relationships** How the company acquires, keeps, and grows the customer base.
Competition and Barriers Identifying the current market leaders. Answering how the business how the business will overcome the existing market dominance.	**Revenue streams** How the company makes money from each customer and business segment.
Step 2: From Concept to Business Plan: Translate the Idea into an Action Plan	
Key Resources What are the most important assets required to make the business model work? Finance, facilities, location, customer lists, IP, and human resources are part of this.	**Cost Structure and Expenses** What are the costs to operate the business model? Which activities are most expensive; which might be optional?
Key Partnerships What are the key partners and suppliers needed to make the business work? What activities do they perform?	**Key Activities and Milestones** What are the most important things the company must do to make the business model work? What problems are being solved? What is the timeline?
Distinguishing URLs and Trademarks A distinctive name and associated domain have been selected that are not infringing others. Also consider marks for products.	**Key Trade Secrets and Key Employees** Essential processes, formulae, and strategies are identified. Confidentiality agreements have been created. Key employees and know-how have been identified and will be secured.
Registered Patents and Copyrights Business based on acquiring or creating copyrights and patents have applied for registration or entered licensing agreements.	**Marketing activities** Plan for promotion and marketing of products and services has been developed and incorporated into expense model.

Running a Data Secure Business

Adapted from the Short & Happy Guide to Privacy and Cybersecurity

Jon M. Garon

The FTC has published very useful guides instructing small businesses on how to manage a secure business to avoid violating the privacy rights of customers and to avoid the various attacks and scams that could harm the small business. Some business operations rely on data analytics much more heavily than others and some business models incorporate sharing information much more actively than others.

These eight key lessons for small business are simple, and they provide an outline that will help most businesses improve customer privacy and data security without sacrificing the use of information helpful to the company. Although these key lessons are simple to outline, they require diligence to maintain:

- *Be transparent about privacy practices*. If the company sells or shares customer information, disclose that clearly. Most consumers don't object most of the time.
- *Only make promises that the company can keep*. Some information sharing is outside the control of the business, so do not over-promise the company's ability to restrict disclosure of private information.
- *Avoid collecting information that is not used*. The company is responsible for the data security of all personal information it collects, both from third parties and from misuse within the business. If information is not collected, it cannot be lost, stolen, or misused.
- *Institute appropriate administrative, technical, and physical data security systems*. The data security used for each business must be appropriate for the size of the company, but all companies need physical security, appropriate policies, training, audits, and assessments. At a minimum, this includes always installing security updates and planning on financing updates and upgrades to key software tools.
- *Provide employees both their rights as consumers and with the protections for employees*. Legal protections provided to employees are in addition to the protections afforded to all consumers. Even the smallest company needs a clear, written employee manual and needs to follow it.
- *Work closely with the PCI security, staying current on all security updates*. Small businesses are often targeted around credit card payment systems. Keeping the pay terminals and other payment systems up-to-date will significantly reduce exposure to theft and loss.
- *Manage vendors and contractors carefully*. Small businesses rely on their contracts with service providers to enable them to compete. But these contracts come with risks for privacy and security. Companies must be diligent in picking the companies with which to do business and focused on the contractual terms of these relationships.
- *Do not implement any policy you would not want to see on the front page of the local newspaper*. The best advice for small business is to approach its business model and its customers as a tight-knit community. If there is a practice that would embarrass its owners when made public, then the owners should choose another approach. Small business is the financial

and social backbone of America, so the business owners should always stand proud in how they adopt and implement policies.

These eight rules provide companies a useful strategy for protecting the privacy of the business customers, maintaining trust between the customer and the company, and minimizing the risk of data breach or other liability. While nothing is foolproof, these rules create an approach that should minimize risk. Each of these is discussed below.

1. Be Transparent About Privacy Practices

To the extent that information is collected and identified with an individual consumer, the business should include that in its posted privacy policy. Most customers barely glance at these disclosures, so companies rarely get in trouble by including too much information. On the other hand, if something goes wrong and the company did not disclose that it collected the data that was later stolen, there can be many negative consequences.

This also requires that companies understand how their technologies work. A company may hire a third party service provider as web host. The web host may be collecting data for its own use that the company does not utilize, but the customer is still having personal information gathered and sold because of the small business.

Companies must also implement do-not-track technology and make customers' profiles available to them, at least where the law requires these additional steps.

2. Only Make Promises That the Company Can Keep

A company must be sure that any promises it makes about use of information is consistent with the use to which the company's vendors and partners have access and make use of the information. The types of information collected may also vary significantly depending on the nature of the engagement. For companies that have a presence on Facebook, Instagram, Twitter, or other online services, the online service company will have its own privacy policy and relationship with the customer. Statements in the privacy policy should recognize that information collected by the company through social media will be subject to the social media site policies as well.

3. Avoid Collecting Information That Is Not Used

Accurate data are extremely helpful for decision making. The single best way for a small business to avoid liability regarding customer information is to avoid collecting the customer's personal information. Many businesses do very well by minimizing the customer information collected and keeping all tracking information separate from personally identifiable information. Unless there is a present business purpose for collecting certain types of information, do not collect the information.

Once data are collected, the data must be stored, maintained, and updated. There is a cost for man-hours and for technology to collect information. When a business case develops for tracking a particular kind of information, then that data should be tracked. But collecting data with the thought that there might someday be a business use is very insufficient.

Consumer data become stale quite quickly. Emails and addresses change, customers age, product lines evolve, and the information that can be learned becomes inaccurate. Companies that collect data

often find they are making decisions based on outdated information or information that becomes misleading because of the aging of the data.

4. Institute Appropriate Administrative, Technical, and Physical Data Security Systems

Every business must develop and adopt the appropriate set of safeguards necessary to protect the company. For many small businesses, they run everything from a single desktop computer or single server. The loss of the central business computer could mean the loss of all orders, inventory tracking, customer lists, and personnel records. If it were to crash without backups or become infected with malware, the loss of central business computer would become the point of failure for all business operations. Whether the company runs on a single computer or operates in a complex cloud-based infrastructure, the company must manage its infrastructure to eliminate the possibility that a single point of failure could shut down the business.

Physical safeguards must include locked print files and/or encrypted storage of key documents; controlled and limited access to sensitive files; regular backups of all computer records that are tested to be sure they will restore properly; and physical protection of information so that trade secrets, customer lists, supplier lists and other key information cannot be copied by unauthorized employees or third parties. As companies become larger and more sophisticated, there must be additional physical safeguards to the information stored, but locked files and resilient, working backups are the starting point for all businesses.

The technical measures will include, at a minimum, the use of firewalls, encryption, and strong passphrases to avoid simple attacks. Access to various computer systems should not be given to all employees. Instead, each employee should have access only to those computers, programs, and networks related to the person's job duties. Administrative access should be even more carefully limited. For slightly larger organizations, networks should be separated so public facing systems never can be used to breach the corporate, financial, operational, employee, or customer data.

The administrative safeguards are just as critical. If a company has employees, it must have employment policies. As discussed in earlier chapters, the employer can establish the company's ownership of computer systems and disclose how it monitors the workforce to assure compliance with state and federal law, minimize theft, and improve customer satisfaction. Computer usage policies, and workplace monitoring policies are included along with sick leave, health and safety, benefits, and other important policies for the employees. The employees must be trained and updated on each of the physical and technical safeguards regularly to assure that passwords and authentication steps remain secure, and that good data hygiene is being followed.

The administrative safeguards will also include policies on how data security is maintained. One person within the company should be identified as primarily responsible for all privacy and data security issues, even if that person is also responsible for many other aspects of the business operations. For larger companies, that position will become a full-time job, but for small companies, it should still be highlighted as a priority among the designated employee's duties.

The administrative policies should detail how the owners or key management of the business takes responsibility for privacy and data security. If the company is large enough to have a board of directors that holds regular meetings, then the board of directors should receive periodic updates on the privacy and data security measures. The administrative procedures should include training for all

employees on how to identify attempts to breach the computer systems, including threats from phishing, malware, and weak passwords.

The cost and scale of the technical measures will vary dramatically depending on the operations of the business and the size of the company. As companies grow and evolve, they must regularly update their security to meet the current needs of the business and the nature of the ever-evolving threat.

5. Provide Employees with Both Their Rights as Consumers and with their Protections as Employees

Employees have all the rights of customers and the protections as employees. Small employers rely very heavily on their key employees. Customers all judge a business based on the last interaction they had with an employee. Even the smallest company needs a clear, written employee manual and needs to follow it. At a minimum, companies should keep employee records separately from other business records. The employee records may have protected health information that requires additional security.

Employee handbooks and other documents should make clear that the policies apply to both full-time and part-time employees. Where certain provisions apply differently for part-time employees rather than full-time employees, those differences should be clearly explained.

Employee handbooks do not apply to independent contractors, since these are not employees. A contractual addendum related to data privacy and the use of the computer systems for the company should be included in all hiring of independent contractors.

6. Work Closely with the PCI Security, Staying Current on All Security Updates

Most small businesses operate by taking funds in person and online through credit cards and other payment systems. While a few check-only offices remain, those are increasingly rare and a testament to customer disregard. At the same time, payment systems are a focus for thieves, since they are the most direct opportunity to steal money from a company.

The PCI banking consortium has developed the PCI DSS as a business-friendly tool for data security compliance for financial transactions. Businesses that take credit cards are required to comply with the PCI DSS. Nonetheless, companies will sometimes buy used equipment or skip mandatory updates. These cost-shaving efforts can put the entire business at risk. Companies should be diligent on staying up to date with the PCI DSS.

7. Manage Vendors and Contractors Carefully

No business is an island. Companies often lease their property, outsource their cleaning services, utilize service providers for websites, cloud storage, computer processing, conduct financial transactions through banks, and hire independent contractors. Product supply chains may include dozens of companies for manufacturing, assembly, and transport. Each of these vendors and contractors is a business ally and a potential source for data breach risks. The risks will flow from one of three general insecurities: the inadequacy of the vendor's software hygiene, the inconsistency in policies for shared data access, and the misuse of protected, private information.

Although there should be a contractual addendum for independent contractors that restrict their use of confidential information and private information, such agreements are not that common. In addition, the ability to enforce the provisions of a restrictive contract against independent contractors are very difficult. To the greatest extent possible, companies should avoid giving independent contractors access to confidential information or to protected customer information.

The risks of misuse of the information is also present with employees and larger vendors, but the company has many avenues of recourse to deal with misuse of information by employees, and the ability to bring breach of contract actions against larger vendors.

8. Do Not Implement Any Policy You Would Not Want to See on the Front Page of the Local Newspaper

This last rule is a general matter of sound advice for all business practices. Data privacy and cybersecurity are very complex areas of law and business practice. Clever attorneys and slick business operators can take advantage of the public by saying one thing and doing another. If an approach feels altogether too clever, it probably is and should be avoided. Small business owners should ask themselves if they are proud of each policy the company implements and if a particular policy would be an embarrassment, then the company should adopt a different strategy.

The successful small business is the pride of its community. The business should implement all its policies to make its community remain proud. The expectation of a corporation's reasonable behavior represents the trust between a company and its patrons. It is when a company violates this expectation that the public becomes upset. Customers expect the companies on which they rely to operate in a reasonable manner with regard to all its policies, including the policies on privacy and data security. Successful companies never breach this trust; the best companies manage to somehow exceed their customers' expectations.

Protecting Yourself at Work and at Home

Any guidance on personal privacy will be relevant in some situations but unhelpful for others. Nonetheless, there are some basic considerations that may prove helpful.

- *Prioritize where privacy matters the most*. Some people are most concerned about government surveillance, while others are more concerned about their employers' access to personal information or to the use of personal information by corporate advertisers.
- *Select vendors and technologies based on your own level of privacy concerns*. Privacy protection is a feature of smartphones, web browsers, payment providers, and communications apps. For consumers who prioritize privacy, they should select among the vendors that have made online anonymity and privacy protections a priority. In many cases, companies will offer an advertising-based version of a product and a more expensive version of the product without advertising and data tracking. Again, the consumer has the choice to pay for additional privacy. If an app requests more access to a smartphone than it should need to provide the service, uninstall the app.
- *Be on the lookout for phishing and other attacks*. Both at home and at work, people are inundated with fraudulent content. Avoid clicking on links in emails unless the sender is well known. If a bank or other company sends information, log in directly rather than

clicking the link to the email. If an email seems odd when sent by a friend or colleague, a person should always verify the legitimacy of the email before clicking on a link or sharing the information.

- *Use good data hygiene*. Personal data hygiene includes the use of strong passwords; never sharing passwords; encrypting data; avoiding untrustworthy websites; erasing all data on any equipment before selling or disposing it; not using public networks for sensitive information; and limiting the disclosure of Social Security numbers, drivers' license numbers, and account numbers. Good data hygiene includes the physical as well as the electronic, so the information in a person's wallet or purse should also be curated to avoid carrying a social security card.
- *Be sure to implement the privacy protections available*. Many products, websites, and apps have privacy settings that can increase the privacy for the user, but often these are not turned on by default. Each user must take the additional time and effort to turn on these settings.
- *Read the privacy policies or analysis of the privacy policies*. Most privacy policies are long, complex, and vague. For popular products and services, there are often published reviews of the privacy policies and settings to help cut quickly through the language of the policy. Consumers should read the policy or read the review to know what they are getting with each product and service.
- *Privacy protections will be breached, so only share content that can be public*. Sven the most diligent companies have experienced data breaches (and few companies are that diligent), the public should assume that anything posted or shared electronically might become public. Intimate photos and explicit personal details can do a great deal of harm if disseminated widely without authorization. The only guarantee that a photo will not be shared is to avoid taking the photo.
- *Assume personal profiles will be screened by employers*. Most employers look at the public social media profiles of employment candidates, and many candidates are online friends with people already employed by the potential employer. As a result, both the public facing information and often much of the nonpublic facing information might be available to the employer. Candidates should assume that employers are checking to see if the behavior of potential employees meets the corporate culture desired.
- *Be mindful of unauthorized access at home and at work*. For most people, the friends and family are their primary source of support and protection. Nonetheless, there are far too many people who are victims of fraud, violence, and abuse. Anyone who has even the slightest concerns over the trustworthiness of a family member or close friend should be careful to protect their passwords, secure their computers and devices, and take the same types of steps as do businesses to ensure that no one can get into their accounts. Many examples of identity theft, fraud, and abusive postings come because the attackers had access to the computers and phones of the victims.