What Every Tech Startup Should Know About Security, Privacy, and Compliance

GIAC SEC566 Gold Certification

Author: Kenneth G. Hartman, kgh@kennethghartman.com
Advisor: Stephen Northcutt

Accepted: February 17, 2015

Abstract

The brilliant innovators who launch tech startups may not have significant experience managing the security, privacy, or compliance issues that are inherent with a growing technology business. Although these businesses are able to attract considerable amounts of funding and woo well-known customers, there may be material issues under the surface that would seriously undermine the trust of their investors and customers. Businesses that lack a mature information security program may experience security breaches, mishandle their customers' personally identifiable information, or fail to meet compliance requirements. Management will need to address security, privacy, and compliance considerations throughout the life cycle of the company, starting with the initial business plan. How the company will manage security, privacy, and compliance will evolve as the company matures. This paper presents actionable recommendations supported by academic literature, with the goal of preventing business organizers from learning these same lessons the hard way.

1. Introduction

Not everyone has what it takes to launch a successful tech startup. A compelling vision must propel the founder, fueled by unstoppable passion. This person must have a risk tolerance that would keep the average person awake every night. Not only that, the founder must also be able to identify and attract top talent while putting together just the right organizational structure to achieve his or her mission (Stillman, n.d.).

The brilliant innovators who launch tech startups may not have significant experience managing the security, privacy, or compliance issues that are inherent with a growing technology company (Harroch, 2013). Although these businesses are able to attract considerable amounts of funding and woo well-known customers, there may be material issues under the surface that would seriously undermine the trust of their investors and customers (InfoLawGroup LLP, 2011; Verizon, 2014). Companies that lack a mature information security program experience security breaches, too many of which go unreported (Pitchford, 2012). Without knowing better, they may mishandle their customers' personally identifiable information or fail to meet compliance requirements (US Small Business Association [SBA], n.d.c).

Management must build security into the startup throughout the life cycle of the company, and this starts with the business plan. While numerous security standards exist and countless security consultants abound, there are certain insights and ways to think about security, privacy, and compliance that can equip founders and executive leadership to maximize their deployment of these resources. The purpose of this paper is to serve as one of the many sources that founders can reference while planning the strategy, organizational structure, and staffing of the fledgling technology organization.

This paper will build a case for incorporating security, privacy, and compliance considerations into the culture and design of the organization, the features of its products and services, as well as the way it goes to market. This paper presents actionable recomendations supported by academic literature, with the goal of preventing business founders from learning these lessons the hard way.

2. Business Planning

In the United States, virtually anyone can file papers of incorporation (SBA, n.d.b) and print business cards with the title of Chief Executive Officer; however the real challenges lie in creating a product that actual customers will want (Goodman, 2014) and finding the capital to fund that endeavor (Gleeson, 2014). Typically, any company that is seeking funding will be required to have a business plan (Berry, n.d.; SBA, n.d.a). The business plan will articulate the business concept, express the company's mission, and define a strategy to realize that mission. The process of creating the business plan requires important consideration of the business climate in which the organization will operate, resulting in a more comprehensive understanding of what it will take to be successful (Rule, 2005).

3. Why Manage Security, Privacy, & Compliance?

Why should high tech founders consider information security, privacy, and compliance when launching their business? The most concise answer is because it matters to the customers of the business as well as its investors, employees, and trading partners. The company must safegaurd trade secrets, protect privacy, and maintain its reputation.

3.1. Trade Secrets & Know-How

In addition to being the catalyst that has spawned new types of businesses, the information revolution of the past few decades has altered the way that traditional companies compete by creating new ways to outperform their rivals (Porter & Millar, 1985). In fact, it is Wal-Mart's logistics and information systems that are credited with propelling it past Sears and Kmart (Flamholtz & Randle, 2007).

Trade secrets are a special type of intangible asset that gives the company competitive advantage. *Know-how* is one of the most common types of knowledge protected as a trade secret, and it is simply defined as the unique knowledge of how to do something (Jorda, n.d.). Trade secrets can include formulas, inventions, programs, methods, techniques, and processes. Unlike other types of intellectual property, such as copyrights and patents, trade secrets are protected by preventing them from becoming publicly known (Cornell University Law School, n.d.). In the US, trade secrets enjoy legal protection from misappropriation under the Uniform Trade Secrets Act, but only if the company can establish that it took appropriate actions to protect the information from disclosure (National Conference of Commissioners on Uniform State Laws, 1985).

Know-how is only considered a trade secret if it is truly a secret, has economic value, and is properly protected (Jorda, n.d.). For a company to remain competitive, it must carefully control who has access to its trade secrets. Certain authorized individuals need access to that information to exploit it for the company's best interest, but if unauthorized individuals gain access to that information, it can jeopardize the company's competitive advantage.

In short, *access control* is making sure that only the right people can access and use the company's secrets and that the wrong people cannot. *Information security* is the protection of the confidentiality, availability, and integrity of information and the protection of information systems from unauthorized access, use, disclosure, disruption, alteration, or destruction (44 U.S.C, Sec 35421).

3.2. Privacy

In addition to trade secrets, the company must also safeguard the personal information given to it by its customers. Generally, when a customer shares his or her private information with a company, it is only in exchange for a good or service from the company. For example, consider the extensive medical information a patient must give to a surgeon. Most patients are reluctant to give this information but will do so willingly when they need surgery and when they trust the healthcare provider (Hartman, 2012).

3.3. Branding, Reputation, and Customer Trust

Seth Godin, a highly respected blogger and author of 17 books, defines a brand as "the set of expectations, memories, stories and relationships that, taken together, account for a consumer's decision to choose one product or service over another. If the consumer (whether it's a business, a buyer, a voter or a donor) doesn't pay a premium, make a selection, or spread the word, then no brand value exists for that consumer" (Godin, 2009).

A powerful brand conveys a promise to its customers that the company keeps consistently over time (Argenti & Druckenmiller, 2004). Trust is tied very closely with the persistent keeping of a promise and building a reputation for being trustworthy (McLeod, 2011).

Businesses spend millions of dollars building their brands to differentiate their products and services (MarketingCharts, 2014). However, certain companies have incurred significant damage to their brand and company reputation because of data security breaches, resulting in the loss of sizable amounts of money as customers shift to competitors and the company repairs the damage (Verizon, 2014).

4. The Important Role of Leadership

Jack Welch, the celebrated ex-CEO of General Electric, gave his thoughts on business leadership during an interview: “Good business leaders create a vision, articulate the vision, passionately own the vision, and relentlessly drive it to completion” (Tichy & Charan, 1989). Because the top executive drives the vision for the company, this individual should also articulate the importance of protecting the reputation of the company and the trust of its customers. In addition, he or she should explain the role of information security in providing that protection (International Standards Organization [ISO], 2013). Employees know what matters most to their management based upon what managers talk about and what they check up on (Oncken, 1984). It is for this reason that the most effective security awareness programs incorporate regular and frequent discussions about information security at all levels of the organization (Robinson, 2013).

The top executive is accountable to the investors who provide funding to start the business and enable its ongoing operations. As part of creating the organizational structure, the top executive designates specific management roles to be accountable for their portion of running the business. Some of these roles may be dedicated to directing a particular business unit while others may be responsible for functional departments such as human resources or information technology (Hax & Majluf, 1981), but all senior management positions should have documented responsibility for managing risks pertaining to the security, privacy, and compliance posture of the part of the company that they control (ISO, 2013).

5. Risk Management

Leadership will need to make multiple tough decisions pertaining to the direction of the company throughout the life cycle of the company (Williams et al., 2008). Many of these decisions will involve threats and opportunities facing the business. Information security risks are just one of the many types of organizational risks that the senior management must address. Other types of risk include investment risk, legal liability risk, safety risk, and supply chain risks among others (National Institute of Standards and Technology [NIST], 2011). Risk is considered to be a function of both the *likelihood of occurrence* and the *adverse impact* that would arise if the event occurs (NIST, 2013). ISO defines information security risk as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization" (ISO, 2004). For the most part, a company does not have control over the methods or motivations of the various threat actors. Therefore it is important to focus on what can be controlled — the vulnerability and weaknesses of the information systems containing the company's sensitive information (Palmaers, 2013).

Because decisions pertaining to risk are an important and reoccurring part of management's duties, it is important to establish an operational process to assess risk, respond to risk, and to monitor risk (NIST, 2011). The CISSP Common Body of Knowledge (CBK) states that it is also important to identify the most appropriate executive in the organization who owns each identified risk (Fitzgerald et al., 2009).

The CBK states management should systematically address risk in one or more of the following ways:

- **Risk Acceptance** — It may be appropriate for decision-makers to accept some risks for a variety of reasons, including a cost versus benefit analysis. This is commonly done for lower impact risks that do not meet a predetermined threshold. Risk acceptance should not be done lightly and should only be done by the risk owner who is accountable for the security of the system involved.

- **Risk Mitigation** — Frequently it is possible to reduce risk to an acceptable level even if it is not possible to eliminate the risk altogether.
- **Risk Transfer —** Under certain circumstances it may be possible to transfer risk to another entity, such as an insurance company or service provider with the appropriate contractual guarantees.
- **Risk Avoidance —** In other cases it may be able to avoid a risk altogether by taking a different course of action or decommissioning a system, for example.

In all cases, the decisions pertaining to risk treatment should be documented to improve transparency into the process for the decision-makers at the top of the company (NIST, 2011). It is a common practice to quantitatively or qualitatively assess risk, require formal risk acceptance of the risks to be accepted, and formally approve the project plans that are created to treat risk (ISO, 2013). Naturally, management will accept more risks in the early stages of a startup because less risk treatment can be performed immediately.

Information security is primarily concerned with managing risk to information assets. A framework that addresses security threats based on risk priority allows management to determine the right amount of security for their company commensurate with the business's budget and risk appetite, within the limits of due care.

Due care is a legal concept by which negligence is tested. If an organization treats risks in the same manner as reasonable organizations would in a similar situation, then it is exercising due care (Hill & Hill, 2002). For this reason, it is a best practice to stay abreast with how other companies in your industry are addressing security and privacy threats and to involve legal council as appropriate.

6. Organizational Capability Maturity

In the 1990s, the Software Engineering Institute (SEI) introduced the Capability Maturity Model *(CMM)* to assess and improve software developed for the federal government. Since that time, many other organizations have adapted and extended the concepts to address process maturity beyond software development. For most companies it would be cost-prohibitive and unnecessary to properly implement the formal CMM. However, the CMM did introduce the extremely valuable concept of "maturity levels" with respect to organizational process maturity. These are:

- **Initial** – Few processes are defined and success depends on individual effort and heroics.
- **Repeatable** – Basic processes are in place with enough discipline to repeat earlier successes.
- **Defined** – The processes are documented, standardized, and integrated across the organization.
- **Managed** – Quantitative measures are used to understand the process and product quality.
- **Optimizing**—Innovative continuous improvement is enabled by quantitative feedback.

In the context of a tech startup, the maturity levels provide a useful model that company leadership can use to intentionally guide their company to develop mature capabilities. Each of the maturity levels has specific characteristics unique to that level as shown in Figure 1 below. In addition, managers must employ different tactics to shift from one level to the next (Hartman, CMM & Organizational Process Maturity, 2012).

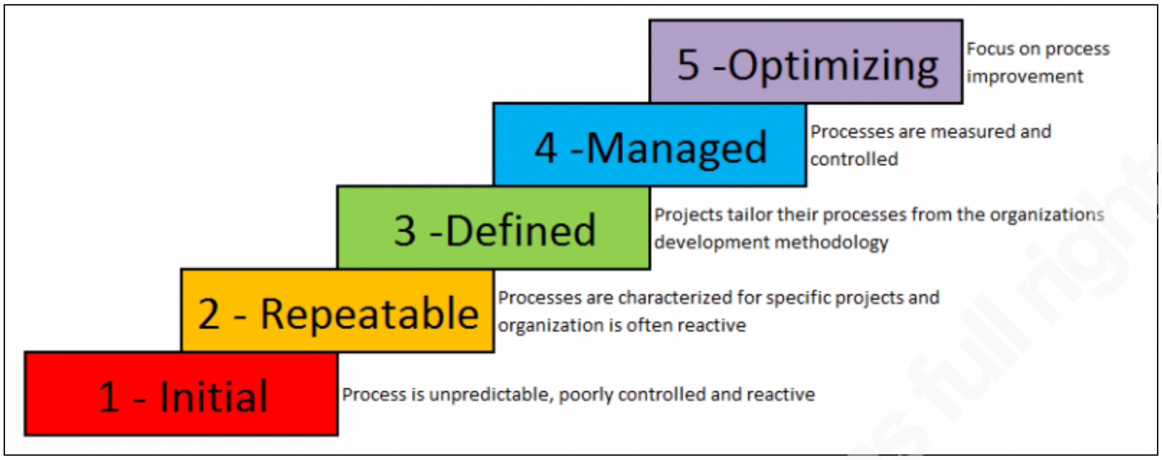
5 -Optimizing
Focus on process improvement
4 -Managed
Processes are measured and controlled
3 -Defined
Projects tailor their processes from the organizations development methodology
2 - Repeatable
Processes are characterized for specific projects and organization is often reactive
1 - Initial
Process is unpredictable, poorly controlled and reactive

Figure 1 - The five CMM maturity levels

The word "capability" has a very specific meaning that can be lost on the casual reader. The Information Technology Infrastructure Library (ITIL) defines it as "the ability of an organization, person, process, application, configuration item or IT service to carry out an activity. Capabilities are intangible assets of an organization" (Cannon, 2011). This definition connotes that capabilities are assets that can be intentionally cultivated and managed in furtherance of the company's mission. Ideally, the startup business plan should identify the outlines of capability maturity at each of the intended growth points (S. Northcutt, personal communication, February 3, 2015).

7. Security Capabilities and Controls

The NIST Special Publication 800-53R4 expands upon the concept of security capabilities by stating that a security capability generally results from the selection and implementation of a set of mutually reinforcing security controls. Using secure remote authentication as an example capability, the document shows how this capability can be achieved by implementing five security controls from the catalog of security controls in its appendix F. To address all of its security requirements, the company will need to define and implement several security capabilities each comprised of multiple complementary and reinforcing security controls. (NIST, 2013)

A *security control* is simply a safeguard or countermeasure designed to meet a set of security requirements. A security control must be granular enough that it can be assessed individually to determine if it is effective or not. Furthermore, assign each control to the appropriate organizational entity for implementation and maintenance. (NIST, 2013)

To illustrate this concept of multiple controls being combined to create a security capability, consider the example of remote access that was mentioned previously. One security control may be stated as:

> *The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and to detect changes to information during transmission (NIST, 2013).*

Another control might be:

> *The information system implements multifactor authentication for network access to privileged accounts (NIST, 2013).*

Although both controls are clearly required, an auditor can evaluate each control separately.

Security capabilities can be designed with reinforcing security controls to achieve defense in depth. This way if a single control fails, other controls may possibly minimize the impact. There are different types of controls and each control should have a specific objective. The CISSP Study Guide (Conrad et al., 2010) provides a common way to classify security controls:

- **Preventive Controls** — A preventive control aims to prevent the adverse event from happening, such as a lock on a door.
- **Detective Controls** — Detective controls alert you that a preventive control has failed. For example, a burglar alarm that indicates an intruder broke through the locked front door. Generally speaking, the faster a security incident is detected, the less damage will be incurred.
- **Deterrent Controls** — While not providing much protection from a motivated attacker, deterrent controls help keep people honest and may improve your legal position to prosecute an intrusion. Common examples of this would be “no trespassing” signs and login banners.

- **Corrective or Recovery Controls —** A corrective control is activated once a security incident has been detected to minimize and contain damage as well as restore normal business operations. An example of this would be an incident response plan.

- **Forensic Controls** — Forensic controls allow investigators to determine the extent of a security incident after the fact. Security event logs are example of this. Unfortunately, the logging at many organizations is inadequate to reconstruct the details of a security breach.

- **Compensating Controls** — A compensating control is used temporarily when another control is not in place or is not effective. An example of this would be to station a guard outside a door when the locking mechanism is broken.

Dr. Eric Cole, a SANS Fellow, has been credited with an axiom that states, "prevention is good, but detection is a must" (Miessler, n.d.). By thoughtfully combining deterrent and detective controls with preventive controls, a company can focus on true threats and respond much more swiftly with planned recovery controls when an intrusion is detected.

8. Security Assurance

Trust is the belief that something will behave in a predictable manner within specific conditions or circumstances. With respect to information systems, trustworthiness expresses the extent to which one can expect systems to preserve the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted by the system. (NIST, 2013)

Trust must be earned. Organizations gain security assurance by collecting evidence that supports the trustworthiness of the security capability being assessed. Much of this evidence consists of the artifacts that are produced as a part of the design and development process, artifacts that are produced as a result of following documented policies and procedures, or the results of testing specific security controls. (NIST, 2013)

9. Compliance Audits

Only a portion of tech businesses are required to implement the controls in NIST SP 800-53R4 for compliance purposes, but the vast majority will be required to comply with either HIPAA, PCI-DSS, or Service Organization Controls *(SOC)*. In many of these cases, an independent auditor will be hired to test the company's compliance with the relevant standard.

Compliance audits may be required by government regulation as in the case of HIPAA, or industry self-regulation like PCI-DSS. A third case arises when important customers impose a contractual requirement to produce something like a SOC Report.

Essentially, an audit uses the scientific method. The hypothesis is that the security control is effective and mature. The auditor examines evidence to confirm or disprove the hypothesis and records the findings in a manner such that another auditor would draw the same conclusions. (Hartman, 2011).

On the Internet, there are many claims that "compliance does not equal security" and many of the assertions may be valid (Chuvakin, 20014). However, it is important to remember that customers ask for your third party audit report because they are looking for evidence to trust your company. The company executive that signs the audit report has a legal duty to affirm that he or she believes the controls are appropriately designed and operating effectively (Hoehl, 2013; PCI Security Standards Council, 2010).

In addition to the third party audits that your customers frequently ask about, there may be a variety of other compliance requirements to which the company is subject. These may include the European Union Safe Harbor Framework, breach notification laws, state-specific privacy laws, the Gramm-Leach-Bliley Act, International Traffic in Arms Regulations, and possibly even the Sarbanes Oxley Act, if the tech startup intends to launch an initial public offering. If the compliance workload is substantial, it may be prudent to hire one or more internal auditors or to retain an external audit firm.

It is highly recommended that management re-evaluate the compliance requirements that the organization is subject to on an annual basis (ISO, 2013). To be proactive, determine in advance the evidence that will be proffered in support of each individual compliance control. Audits can be disruptive and this will minimize last minute scrambling. This exercise should become more routine year after year, but it is important to budget for it at the beginning of operations.

10. Information Security Management System

The various security, privacy, and compliance considerations discussed so far would be impossible to handle without a management system. Some companies will create a rudimentary information security management system *(ISMS)* without much guidance or planning. In this reactionary mode, policies are created to address a compliance check box.

Some may consider ISO 27001 to be just another compliance framework. However, it provides detailed guidance on how to set up an effective ISMS that is tailored to the unique needs of any company. An important part of the ISO 27001:2005 implementation philosophy was the Plan-Do-Check-Act cycle. The basic premise is that you separate the planning from execution work. After the planned work has been executed, next comes a check to see if the desired results are achieved. After that, the process is tweaked based on any lessons learned and then the cycle is repeated. (ISO, 2005)

A crucial component of the initial planning stage is to properly charter the launch of the ISMS. This document should spell out top management's support for the ISMS and assign accountability for its operation to a specific job role or named individual. (ISO, 2013)

10.1. Policies and Procedures

Policies and procedures are major elements of the ISMS. Security policies define management's expectations and rules that are to be followed in order to ensure the confidentiality, integrity, and availability of the information assets within the scope of the ISMS. Furthermore, policies assign responsibility and grant authority as appropriate to carry out those expectations. Management's approval of the policies is further evidence of the company's commitment to information security. (Albright, 2002)

Procedures provide additional mandatory direction on how to comply with security policy. Procedures are revised more frequently than policies because implementation details change more frequently than strategic direction. To enhance the company's audit readiness, consider requiring that the company's procedures define the artifacts created as a result of following the procedure. Taken together, policies, procedures, and the process artifacts create important evidence to evaluate the trustworthiness of the ISMS. These documents also create a foundation to improve upon with subsequent iterations of the Plan-Do-Check-Act cycle, resulting in capability maturity over time.

10.2. Change Management

Controlling and managing change is an important part of managing security. In fact, virtually all security incidents are the result of attempting or successfully making an unauthorized change. From the very start of the company, it is critical to set up an effective and efficient system to document and approve changes to policies, procedures, system configurations, security and privacy controls, and anything else the company puts its trust in (ISO, 2013). It is also important to apply technology to detect unauthorized change, such as file integrity monitoring on critical systems such as firewalls and servers (Behr et al., 2005).

10.3. Risk Assessment

An information system management system based on ISO 27001 will have documented procedures to ensure that risk is systematically assessed on at least an annual basis in accordance with many of the concepts discussed previously in Section 5.

10.4. Corrective & Preventive Actions

Companies that are not seeking formal ISO 27001 certification may be tempted to skip the ISO requirement to establish a formal system for documenting and implementing corrective and preventive actions. If they do, they are missing a chance to institutionalize continuous improvement and reach Maturity Level 4.

If a security incident occurs or if a policy/procedure/control is circumvented, an appropriate member of management needs to make a determination of the root cause and put a plan of action in motion to make the appropriate correction. If a formalized system is established, these activities can be delegated to the appropriate levels in the organization creating a powerful system of checks and balances.

10.5. Control Effectiveness & Maturity Metrics

Measuring each security control for effectiveness and maturity is another characteristic of a mature ISMS. Since the company is placing a considerable amount of trust in its security controls, metrics will help the organization determine if its security capability is improving or if its trust is misplaced. H. James Harrington is quoted as saying, “Measurement is the first step that leads to control and eventually to improvement. If you can’t measure something, you can’t understand it. If you can’t understand it, you can’t control it. If you can’t control it, you can’t improve it.” (Harrington, n.d.). While ISO 27004:2009 and NIST SP 800-55R1 can give detailed guidance on measuring security, it may be totally appropriate to start with qualitative ratings on a 1-5 point scale. The goal is to generate data to make sure that management has a clear picture of where to allocate resources as they adjust the Information Security Management Program (ISO, 2013). The ability to manage the ISMS according to metrics is another characteristic of Maturity Level 4.

10.6. Comprehensive Management Review

Many compliance frameworks require an annual review of policies (PCI Security Standards Council, 2013; U.S. Dept of Health & Human Services, n.d.). This is because companies change and threats constantly evolve. However, it is not just the policies but the whole ISMS that must adapt over time to protect the business (ISO, 2013). In addition to policies and procedures, ISO 27001 requires regular management review of the following items to make recommendations on how to improve the ISMS:

- All recent audits and assessments, internal and external
- Corrective and preventive action records
- Risk assessments and risk treatment plans
- Effectiveness and maturity metrics

- Security incidents

In a tech startup, everyone is busy and forced to perform many different job roles, but it is essential that the individual designated to operate the ISMS schedule this important review meeting with top management on at least an annual basis. When the management reviews are used to optimize the ISMS using the qualitative and quantitative data generated by the Plan-Do-Check-Act cycles, the ISMS will have reached Maturity Level 5.

11. Application Security

Many tech startups are launched to bring a software product or web aplication to market. If the application processes credit cards or contains personally sensitive information such as medical or financial information, it will be subject to specific compliance and security requirements. However, even if the application is a computer game, it may still be the target of attacks (BBC, 2014). During the inception of the company, tech founders will want to consider how they will ensure the security of their software products.

11.1. Separation of Duties

Separation of duties (SoD) is an important security principle that can be challenging to implement in a small company. Managers with a financial background realize that the purchasing function is separate from the accounts payable function to reduce the risk of fraud. Seperation of duties should be considered whenever there is a potential conflict of interest and this technique can be judiciously applied to improve software development (Gregg et al., n.d.).

It is a wellknown best practice to prevent software developers from having access to production systems. Similarly development and quality assurance environments should be completely seperated from production environments. (Gregg et al., n.d.). If the company is serious about application security and change control, it must not compromise on this requirement. Security incidents are the result of unauthorized change. Therefore, treat all unauthorized changes as a security incident, even if it was made by a well-intentioned insider (Behr et al., 2005). The best way to achieve this separation is to have two distinct job roles—production system administrators and software engineers. Production system administrators are not permitted to write production code. They can only install it from the source code repository. Conversely, software engineers write the production code and check it into the source code repository, but are not allowed to install it. Ideally, the company will handle system configurations the same way using automated configuration management tools, such as Puppet, so that configurations can be controlled just like source code.

The best time to establish SoD is when the company is being designed. Do not hire the executive to lead your software development program if he or she does not totally embrace this philosophy. While you are at it, create a third role, a "security analyst," that is independent from both the production system administrators and the software engineers to detect unauthorized change in production systems and other signs of attack. All three of these important roles should report to different managers and should embrace the dialectic nature of their job duties.

Development teams may raise a common objection to separation of duties citing the need to troubleshoot live production systems. After all, it is unlikely that no one understands the code as well as the person who wrote it. Although the need to perform "live surgery" on production systems should diminish as the development processes mature, there are creative solutions to maintain SoD in cases of an emergency. One possibility is that the production systems administrator enables an emergency access account and grants access for the software developer to the production systems via a recorded web conferencing session. Ideally, all keystrokes are logged on the emergency access account. Of course, this work is done only after an emergency change request has been approved. After the emergency repair, document all changes and merge the modified and approved code back into the source code repository.

11.2. Software Development Lifecycle

A software development life cycle *(SDLC)* is the documented process that a company uses to develop, maintain and replace its software (Janssen, n.d.). In a SANS whitepaper, James Purcell performed a comparison of the most common SDLC models but emphasized that the purpose of a SDLC is to have a repeatable process that builds security into the software throughout the development lifecycle (Purcell, n.d.).

The SDLC documentation should address security considerations in all phases through which a software development project will transition. These are Project Initiation, Design Analysis, System Design Specification, Programming and Testing, Installation and Maintenance, and Destruction/Decommissioning. (Purcell, n.d.).

Programmers love to write code and typically despise testing, debugging, and documentation. Frederick Brooks in his seminal essay, "A Mythical Man Month" claimed the following breakdown of software development tasks should be: one-third planning, one-sixth coding, one-fourth component testing and one-fourth system testing. While actual results today may vary, his point is that too much emphasis is given to coding and not enough time is scheduled for proper planning or testing. (Brooks, 1995). Recall that the SEI CMM, discussed previously, was one approach developed during this time period to address this problem.

11.3. Agile Development

Many software development companies have transitioned to agile programming. It is important to stress that it is possible to develop secure code using agile development methodologies (Keramati & Mirian-Hosseinabadi, 2008). At a minimum, a company should have a security design review when the system is being architected and after any substantial change, a code review at the end of each coding phase, and vulnerability testing prior to being released to production (Council on Cyber Security, n.d.).

11.4. Threat Modeling

Threat modeling is an excellent approach for analyzing the security of an application. The Open Web Application Security Project [OWASP] has created valuable guidance on how to perform application threat modeling. In a nutshell, the process involves diagramming how information flows through the system, highlighting the transfers across trust boundaries, categorizing and ranking threats, and determining countermeasures and mitigation strategies. Threats are typically categorized using the

STRIDE model. STRIDE is an acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege. (OWASP, 2013).

12. Procurement

All companies, and especially startups need to rely on vendors to perform important services. There is a contracting life cycle (Berkx, n.d.), just like there is a life cycle for software development, and this life cycle must be managed as well. While the specific models espoused by vendors of contract management software may differ, they typically all address negotiation, contract creation, managing contract change, compliance monitoring, and contract renewal or termination.

12.1. Vendor Selection

Although an in-depth discussion regarding vendor selection is beyond the scope of this paper, it is of utmost importance to thoroughly evaluate the security program of the vendors that your company intends to contract with. The Santa Fe Group has created a spreadsheet called the "Standard Information Gathering Questionnaire" which they make freely available to simplify vendor security assessments (Santa Fe Group, 2012).

12.2. Contracting

Contracts should clearly describe the vendors' specific obligations to protect security and privacy as well as to maintain compliance with regard to the vendors' use of company data. Frequently, this is in the form of an addendum (University of Washington, n.d.).

12.3. Contract Compliance Monitoring

If a company has done an excellent job at vendor selection and contracting yet fails to monitor compliance with the terms of the contract, it has no basis for the trust is placing in the vendor to keep the company's confidential information secret. The contract language should clearly state how the company will audit contract compliance. Then, qualified representatives from the company must do so, per the contract.

13. Organizational Development

Flamholtz and Randle (2007, pp. 9-18) define six key organizational development tasks in their book titled "Growing Pains." These tasks are typically addressed in the business plan, but remain areas of focus throughout the life of the company. These key tasks are:

- Identify and Define a Market
- Develop Products and Services
- Acquire Resources
- Develop Operational Systems
- Develop Management Systems
- Manage the Corporate Culture

There are security, privacy, and compliance ramifications to each of these bullet points and how the company will manage these tasks will change at each stage of maturity. Table 1 lists some questions for the founders to consider as a recap of the previous sections.

Identify and Define a Market	• How will you protect the customer trust in your brand? • How will you maintain your competitive advantage? • How will you protect your secrets?
Develop Products and Services	• Will you use a SDLC to build security into the products? • Will you insist upon separate development and production environments and enforce separation of duties in key job roles?
Acquire Resources	• Will you address security throughout the contract life cycle? • Will management roles have documented responsibility for security, privacy, and compliance?
Develop Operational Systems	• As you build your operational systems, processes, and procedures, will you treat capabilities as assets that can mature in support of the company mission? • How will you manage risks to privacy and security?

Develop Management Systems	- Will you devote the effort to measure, evaluate, and refine your security management system? - Will you perform a periodic comprehensive management review of your ISMS?
Manage the Corporate Culture	- How will you manage the corporate culture? - As the leader, will you lay the foundation for continuous improvement and articulate how to protect customer trust?

Table 1 – List of organizational development considerations

14. Conclusion

Without a doubt, founders have a lot to consider when launching a tech startup. Security, privacy, and compliance are important to everyone supporting or depending on your business. Therefore, founders should weave the important considerations discussed above into the company during the creation of the business plan and maintain focus on them throughout the life of the company.

Figure 2 – The construction of a skyscraper is a metaphor for the early stages of a startup.

The great thing about being the founding leader of a tech startup, is that you get to decide the answers to the important questions pertaining to the direction of the company. The construction of a skyscraper can be a good metaphor for launching a startup. (See Figure 2.) At the beginning, the wind may blow through the structure, but the builders are undaunted because they are proceeding according to a plan based on experience and proven practices.

The goal of this paper was not to make anyone an information security expert, but to raise awareness so that tech startup leaders can get additional guidance to address these considerations in the manner most appropriate for their business. Often, it starts by asking the right questions.

References

44 U.S.C, Sec 35421. (n.d.).

Albright, J. G. (2002, March 25). *The basics of an IT security policy.* Retrieved January 25, 2015, from Global Information Assurance Certification: http://www.giac.org/paper/gsec/1863/basics-security-policy/103278

Argenti, P. A., & Druckenmiller, B. (2004). Reputation and the corporate brand. *Corporate Reputation Review*, 368-374.

BBC. (2014, August 25). *Sony PlayStation Network and other game services attacked*. Retrieved January 31, 2015, from BBC.com: http://www.bbc.com/news/technology-28925052

Behr, K., Kim, G., & Spafford, G. (2005). *The visible ops handbook: Implementing ITIL in 4 practical and auditable steps.* Eugene, OR: IT Process Institute.

Berkx. (n.d.). *Contract lifecycle management*. Retrieved January 31, 2015, from Berkx.com: http://www.berkx.com/knowledge-base/contract-lifecycle-management/

Berry, T. (n.d.). *Do I need a business plan?* Retrieved January 21, 2015, from Bplans.com: http://articles.bplans.com/do-i-need-a-business-plan/

Brooks, F. P. (1995). *The mythical man-month; Essays on software engineering, Anniversary edition.* Boston, MA: Addison Wesley Longman, Inc.

Cannon, D. (2011). *ITIL service strategy, 2011 edition.* Norwich, UK: The Stationery Office.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008, July). *NIST SP 800-55 rev. 1 - Performance measurement guide for information security.* Retrieved January 31, 2015, from Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

Chuvakin, A. (20014, April 28). *Security and/or/vs/not compliance?* Retrieved January 25, 2015, from Gartner: http://blogs.gartner.com/anton-chuvakin/2014/04/28/security-andorvsnot-compliance/

Conrad, E., Misenar, S., & Feldman, J. (2010). *CISSP study guide.* Burlington, MA: Elsever.

Cornell University Law School. (n.d.). *Trade secret*. Retrieved January 24, 2015, from Legal Information Institute: http://www.law.cornell.edu/wex/trade_secret

Council on Cyber Security. (n.d.). *The critical security controls effective cyber defense V5.1.* Retrieved from Council on Cyber Security: http://www.counciloncybersecurity.org/critical-controls/

Fitzgerald, T., Goins, B., Herold, R., & Shaurette, K. M. (2009). Information security governance and risk management. In H. F. Tipton (Ed.), *Official ISC2 guide to the CISSP CBK, second edition* (pp. 248-231). Boca Raton, FL: Auerbach Publications, Taylor & Francis Group.

Flamholtz, E. G., & Randle, Y. (2007). *Growing pains: Transitioning from an entrepreneurship to a professionally managed firm.* San Francisco, CA: Jossey-Bass.

Gleeson, B. (2014, October 15). *Need funding? The challenges and solutions to the obstacles of small business lending*. Retrieved January 21, 2015, from

Forbes.com: http://www.forbes.com/sites/brentgleeson/2014/10/15/need-funding-the-challenges-and-solutions-to-the-obstacles-of-small-business-lending/

Godin, S. (2009, December 13). *Define: Brand*. Retrieved January 24, 2015, from sethgodin.typepad.com: http://sethgodin.typepad.com/seths_blog/2009/12/define-brand.html

Goodman, H. (2014, February 5). *Building products that customers want*. Retrieved January 21, 2015, from Forbes.com: http://www.forbes.com/sites/harrisgoodman/2014/02/05/building-products-that-customers-want/

Gregg, J., Nam, M., Northcutt, S., & Pokladnik, M. (n.d.). *Separation of duties in information technology*. Retrieved January 26, 2015, from SANS Institute: http://www.sans.edu/research/security-laboratory/article/it-separation-duties

Harrington, H. J. (n.d.). *H. James Harrington quotes*. Retrieved January 26, 2015, from Goodreads: http://www.goodreads.com/quotes/632992-measurement-is-the-first-step-that-leads-to-control-and

Harroch, R. (2013, October 3). *10 big legal mistakes made by startups*. Retrieved January 21, 2014, from Forbes.com: http://www.forbes.com/sites/allbusiness/2013/10/03/big-legal-mistakes-made-by-start-ups/

Hartman, K. G. (2011, February 7). *Auditing essentials for small provider organizations.* Retrieved January 25, 2015, from HIMSS Privacy and Security Toolkit: http://www.himss.org/files/HIMSSorg/content/files/SP07_Security_Auditing_for_Small_Provider_Organizations_Final.pdf

Hartman, K. G. (2012, November 3). *CMM & organizational process maturity.* Retrieved January 25, 2015, from Kenneth G. Hartman, CISSP: http://www.kennethghartman.com/cmm-organizational-process-maturity/

Hartman, K. G. (2012, June 6). *Understanding the role of trust in the protection of privacy.* Retrieved January 24, 2014, from HIMSS.org: http://himss.files.cms-plus.com/HIMSSorg/content/files/UnderstandingtheRoleofTrustintheProtectionofPrivacy.pdf

Hax, A. C., & Majluf, N. S. (1981). Organizational design: A survey and an approach. *Operations research*, 417-447.

Hill, G., & Hill, K. (2002). *The people's law dictionary.* MJF Books.

Hoehl, M. (2013, December 23). *Understanding what service organizations are trying to SSAE.* Retrieved January 25, 2015, from SANS Institute Infosec Reading Room: http://www.sans.org/reading-room/whitepapers/auditing/understanding-service-organizations-ssae-34475

InfoLawGroup LLP. (2011, October 14). *SEC issues guidance concerning cyber security incident disclosure*. Retrieved January 21, 2015, from Information Law Group: http://www.infolawgroup.com/2011/10/articles/breach-notice/sec-issues-guidance-concerning-cyber-security-incident-disclosure/

International Standards Organization [ISO]. (2009). *ISO/IEC 27004:2009(en) Information technology — Security techniques — Information security management — Measurement.* Retrieved January 31, 2015, from ISO.org: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42106

International Standards Organization. (2004). *ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management.* Retrieved January 25, 2015, from ISO.org: http://www.iso.org/iso/catalogue_detail.htm?csnumber=39066

International Standards Organization. (2005). *ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements.* International Standards Organization.

International Standards Organization. (2013). *ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements.* Retrieved January 31, 2015, from ISO.org: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

Janssen, C. (n.d.). *Software development life cycle (SDLC)*. Retrieved January 26, 2015, from Techopedia: http://www.techopedia.com/definition/22193/software-development-life-cycle-sdlc

Jorda, K. F. (n.d.). *Trade secrets and trade-secret licensing*. Retrieved February 3, 2015, from IP handbook of best practices: http://www.iphandbook.org/handbook/ch11/p05/

Keramati, H., & Mirian-Hosseinabadi, S. (2008, March). Integrating software development security activities with agile methodologies. *Computer Systems and Applications, 2008. AICCSA 2008. IEEE/ACS International Conference on* (pp. 749-754). IEEE.

MarketingCharts. (2014, June 25). *US ad spend trends in Q1*. Retrieved January 24, 2015, from MarketingCharts: http://www.marketingcharts.com/traditional/us-ad-spend-trends-in-q1-43546/

McLeod, C. (2011, February 7). *Trust*. Retrieved January 24, 2014, from Stanford Encyclopedia of Philosophy: http://plato.stanford.edu/entries/trust/

Miessler, D. (n.d.). *Information security concepts*. Retrieved February 5, 2015, from danielmiessler.com: https://danielmiessler.com/study/infosecconcepts/

National Conference of Commissioners on Uniform State Laws. (1985, August 9). *Uniform trade secrets act with 1985 amendments.* Retrieved February 3, 2015, from Uniform Law Commission: http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf

National Institute of Standards and Technology [NIST]. (2011, March). *NIST special publication 800 – 39: Managing information security risk.* Retrieved January 25, 2015, from Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

National Institute of Standards and Technology [NIST]. (2013, April). *NIST special publication 800 – 53 R4: Security and privacy controls for federal information systems and organizations.* Retrieved January 25, 2015, from Computer Security Resource Center: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Oncken, W. (1984). *Managing management time.* Englewood Cliffs, NJ: Prentice-Hall Inc.

Open Web Application Security Project [OWASP]. (2013, March 6). *Application threat modeling*. Retrieved January 26, 2015, from Open Web Application Security Project: https://www.owasp.org/index.php/Application_Threat_Modeling

Palmaers, T. (2013, March 23rd). *Implementing a vulnerability management process.* Retrieved January 25, 2015, from SANS Reading Room: http://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180

PCI Security Standards Council. (2010, October). *Attestation of compliance for self-assessment questionnaire D – Merchants.* Retrieved January 25, 2015, from PCI Security Standards Council: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_AOC_Merchant.docx

PCI Security Standards Council. (2013, November). *Payment card industry (PCI) data security standard version 3.0.* Retrieved January 31, 2015, from www.pcisecuritystandards.org: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Pitchford, M. (2012, June 18). *Former FBI cyber expert: 94% of cyber security breaches unreported.* Retrieved January 21, 2015, from The Daily Caller: http://dailycaller.com/2012/06/18/former-fbi-cyber-expert-94-of-cyber-security-breaches-unreported/

Porter, M. E., & Millar, V. E. (1985). How information gives you competitive advantage. *Harvard Business Review*, 149-174.

Purcell, J. E. (n.d.). *Comparison of software development lifecycle methodologies.* Retrieved January 26, 2015, from SANS Software Security: http://software-security.sans.org/resources/paper/cissp/comparison-software-development-lifecycle-methodologies

Robinson, A. (2013). *Using influence strategies to improve security awareness programs.* Retrieved January 31, 2015, from SANS.org: http://www.sans.org/reading-room/whitepapers/awareness/influence-strategies-improve-security-awareness-programs-34385

Rule, R. (2005, January 31). *Creating a winning startup business plan*. Retrieved January 17, 2015, from Entrepreneur.com: http://www.entrepreneur.com/article/76140

Santa Fe Group. (2012, 2 1). *Standard information gathering (SIG) questionnaire*. Retrieved January 31, 2015, from sharedassessments.org: http://sharedassessments.org/media/SIGv7_Overview_2_1_2012.xls"

Stillman, J. (n.d.). *Top 6 characteristics of the best startup CEOs*. Retrieved January 17, 2015, from Inc.com: http://www.inc.com/jessica-stillman/top-6-characteristics-of-the-best-startup-ceos.html

Tichy, N., & Charan, R. (1989). *Speed, simplicity, self-confidence: An interview with Jack Welch*. Retrieved January 24, 2015, from Harvard Business Review: https://hbr.org/1989/09/speed-simplicity-self-confidence-an-interview-with-jack-welch

U.S. Department of Health & Human Services. (n.d.). *Summary of the HIPAA security rule*. Retrieved January 31, 2015, from HHS.gov: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

University of Washington. (n.d.). *Data security agreement.* Retrieved January 31, 2015, from Office of the CISO, University of Washington: http://ciso.washington.edu/site/files/Data_Security_Agreement.pdf

US Small Business Administration [SBA]. (n.d.a). *What is a business plan and why do I need one?* Retrieved January 21, 2015, from US Small Business Administration: https://www.sba.gov/content/what-business-plan-and-why-do-i-need-one

US Small Business Association. (n.d.b). *Limited liability company*. Retrieved January 21, 2015, from US Small Business Association: http://www.sba.gov/content/limited-liability-company-llc

US Small Business Association. (n.d.c). *Privacy law*. Retrieved January 2015, 2014, from US Small Business Association: https://www.sba.gov/content/privacy-law

Verizon. (2014). *2014 Data breach investigations report.* Retrieved January 21, 2015, from Verizon: http://www.verizonenterprise.com/DBIR/2014/

Williams, S., Ledford , C., & Lockwood, N. R. (2008, March 1). *Leadership competencies*. Retrieved January 31, 2015, from Society for Human Resource Management: http://www.shrm.org/research/articles/articles/pages/leadershipcompetencies.aspx