A Startups Guide to Implementing a Security Program

Vanessa Pegueros

A Startups Guide to Implementing a Security Program

GIAC (GSEC) Gold Certification

Author: Vanessa Pegueros, vpegueros@gmail.com
Advisor: Mohammed Haron
Accepted: September 26th, 2020

Abstract

Startups struggle to balance survival with the practical implementation of a security program. There are numerous obstacles facing founders who want to generate a solid security foundation, including limited cash, lack of support from investors or the board, and conflicting priorities such as generating revenue. Despite these obstacles, customers and potential customers continue to demand a base level of security controls. This drive from customers, especially enterprise customers, for solid security programs has forced startups to develop a practical approach to security that works within the boundaries of their constraints. Implementation of key controls and processes can establish a solid security foundation and meet the needs of customers.

1. Introduction

This paper is based on both Vanessa's eighteen years of experience in security and interviews she conducted with six Founders/CEOs. Additionally, she has been working as an advisor to various startups for the past six years. Vanessa has mainly advised startups in the technology space, and one of those startups is currently a unicorn. Additionally, she joined a Venture Capital (VC) firm in 2018 as a venture partner and assists with investment due diligence focusing on Security, Risk, Compliance, and Privacy.

Throughout her career, she has heard security practitioners express frustration and disapproval of the lack of the attention that startups have paid to security. As a security professional, she was confused by the lack of focus startups gave to the security of their product and company operations. It wasn't until she started to work with startups and understand the challenges they faced that she began to understand this lack of focus. She realized the root cause was not a lack of desire to focus on security; it was a desire to survive that drove their actions.

During her work with startups, she developed a set of minimum requirements in security processes and controls required to ensure the startup's future success. This paper codifies Vanessa's recommendations to startups, backed up by interviews with Founders/CEOs.

Vanessa Pegueros, vpegueros@gmail.com

2. Overview of the startup community

A major concern for startups is raising money to fund the operations. There are several options for startups to raise money, and those options generally fall into the categories of debt (loans) or equity (shares of stock). Banks are a common source for debt, and Angel Investors and VCs are a common source of cash in exchange for equity. Typically, Angels (Seed Investors) are high net worth individuals who invest in the very early stages of a company, often before a VC invests in exchange for some equity. VCs typically manage a pool of money on behalf of various organizations such as Foundations, Pension Funds, Wealthy Families, and Insurance companies. Since most startups are not generating cash, and most banks do not want to take on a startup's risk in the form of a loan, Angels/VCs are a common source of funds. As was mentioned above, investing in startups is very risky. For every ten companies, a VC invests in, five will fail, two to three will return some modest multiple (2 to 4 times) of the initial investment, and one to two will be a wild success. Basically, there is a 10% to 20% chance of making anywhere from 10 to 100 times what was invested by the VC.

When deciding which company to invest in, VCs consider three main factors: 1) the people and the team, 2) the product, and 3) the market size for the product. Once a VC has decided to invest in a company, they will likely get a seat on the private company's board. The Board of a company is a group of individuals who have responsibilities that provide overall strategic guidance and direction to the company leaders, primarily the CEO/Founder. The Board also has the important role of evaluating the performance of the CEO. If the Founder does not have a controlling interest (own at least 51% of the company's equity), the Board could fire the CEO. Because of the relationship between the Board and the CEO/Founder, the VC/Investor has a great influence relative to the company and its priorities.

Different VCs have different styles relative to "overseeing" their investment. Vanessa has worked with VCs who are very hands-on and will dive deep in problem-solving with its leadership. Other VCs are very hands-off and just want to see the numbers and results. Regardless of style, all VCs are motivated by the same principle, which is to maximize the returns on their investment. Due to this motivation, they are far more concerned about sales and selling into the target market than they are about security. Most VCs are not very technical, or their technical knowledge is stale, having been away from an operating role for some extended

period of time. Security can be a very complex topic that is not easy to explain to an audience at the board/investor level. Additionally, unless a direct correlation can be made between security and sales, there will be little interest in security by the Board.

This disinterest by VC/Investors/Board members creates a challenge for a startup that has aspirations to build a strong security culture and the associated technical controls. Investors may challenge initiatives relative to security as they may not view allocating funds to security as a good use of funds. This challenge creates friction between security-minded Founders and their Investors.

3. The struggle of the startup – why security is not a priority

Based on Vanessa's experiences working with startups in the early phases, they often have priorities other than security. They are focused on growing revenues, capturing marquee customer brands, and ensuring that they can make payroll and continue to retain their most valued employees to drive product enhancements.

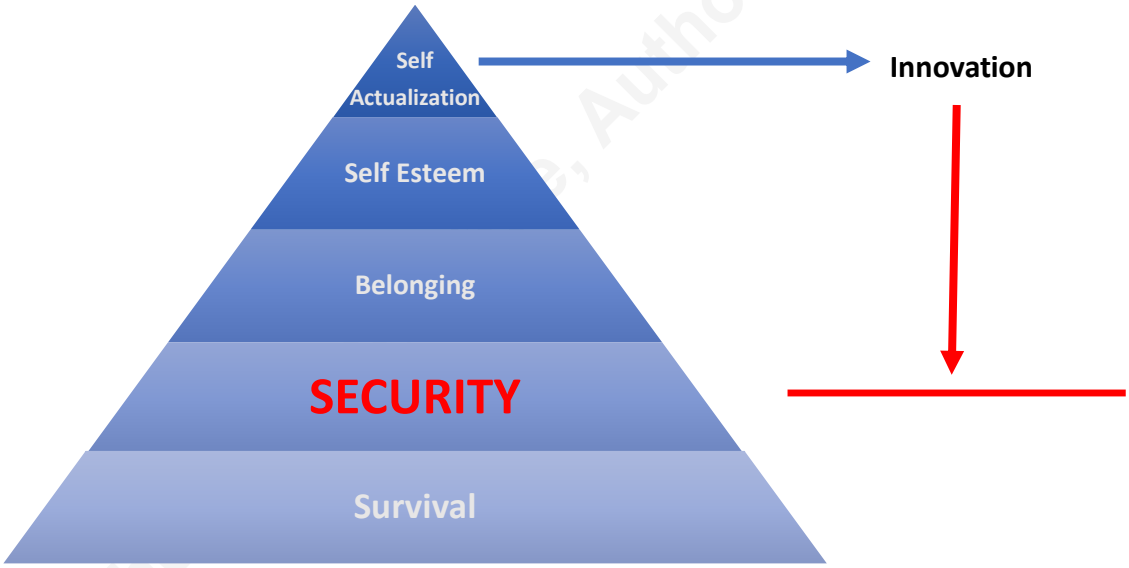
Vanessa believes there are two main reasons security is not considered as a top priority with startups. One relates to the priorities of customers, and the other relates to Maslow's hierarchy of needs. In 1943, Abraham Maslow published a paper in Psychological Review entitled, "A Theory of Human Motivation." As a result of his paper, the pyramid of human needs was developed as pictured below.

To summarize Maslow's hierarchy of needs, a human being can not focus on the areas above its current state until the needs of that current state are met. If we start at the very base of the model, if a human being does not have enough food to survive, then they will take incredible risks to obtain that food and will not focus on the needs related to security or anything above security. Psychologically and physiologically, the human needs to focus and put all his/her energy into survival.

An organization and, more specifically, a startup organization are no different. As seen from the previous section, startups are focused on survival. They are worried about meeting payroll and having enough cash to survive into the next week or maybe even day was a very real concern since "In 2018, 82% of businesses that went under did so because of cash flow problems." (Embroker, 2020). If a startup is not even sure it will survive into the next week, why would it spend any money on security? Being secure in and of itself will not stop a startup from failing and may even have assisted in failure as precious cash resources are spent on implementing security controls.

A reverse Maslow's Hierarchy of Needs factor play into why startups do not focus on security even when they are not in the "survival mode." When individuals are at a higher level of Maslow's hierarchy, they will resist moving down the pyramid. When a high-tech startup is successful; and is riding the wave of success, they live at the top of Maslow's hierarchy. They are part of a team with a strong mission (Belonging), they feel good about themselves because of

their success (Self Esteem), and they can create and innovate (Self Actualization). When the topic of security is brought up, that pushes them down the pyramid and is no longer fun, since now they need to think about the bad things that could happen to the company, product, or employees. Additionally, a bad enough security breach could threaten the survival of the company.



In addition to the factors related to Maslow's Hierarchy of Needs, another main factor influences the focus of a startup relative to security. This factor relates to how much the customers of that company care about security. Based on Vanessa's experience, consumers generally do not care about security as much as enterprise customers. If a business will be successful with their customers, they need to focus on their customers' care.

Generally, consumers don't focus on security itself but care more about issues of privacy. Based on Vanessa's observations and experiences, consumers' security and privacy maturity has grown significantly over the last ten years. She believes a major contributor to that maturity has been the very public and prevalent news on large data breaches. There seems to be weekly news on television related to security or some data breach. The movie "The Great Hack" brought to the public the very troubling nature of how data can be used to manipulate the outcomes of public elections. The average consumer is much more aware of how their data can be used for identity

theft and how they can be influenced through online channels. Despite this new awareness, Vanessa still believes consumers are motivated by the price, functionality, and convenience of most products and services and not as focused on the product or service's security. For these reasons, companies focused on the consumer segment have fewer expectations relative to security and, therefore, will most likely focus less on it as a priority. This reality will change over time and more will be required by companies in terms of security when operating in the consumer space. At some point, US will adopt a national privacy law similar to GDPR, and elements of security, as they relate to privacy, will be mandated for all companies, including those that only deal with the consumer space.

Enterprise customers have a completely different set of expectations relative to security. Their reputation with their customers is at stake if they choose to operate with subpar security practices. They are also driven by compliance with regulations and laws within the industry vertical in which they operate. An enterprise may choose not to do business with a startup that has insufficient security controls and maturity. As a startup focused on the enterprise space, security is a critical element of success built in from the start.

For the reasons noted above, being focused on survival and being consumed by the euphoria, some startups avoid spending time on security and end up inadvertently orchestrating their demise. There are well-documented instances of startups who failed due to security missteps:

- Code Spaces, which was founded in 2007, closed its doors in 2014 after an AWS instance breach. (Mimosa, Michael, 2014).
- MyBizHomePage was shut down after numerous cyberattacks by a disgruntled former CTO against the company's website. (Pro OnCall Technologies, 2014).
- Distribute.IT, a domain registrar and hosting, company sustained a cyberattack that forced them out of business in 2011. (Connolly, Bryon, and Gardiner, Bonnie, 2015)

Additionally, to the psychological challenge of not wanting to deal with security, the security team is then challenged by seeing the risks present in their company and addressing them. Either they were ignored, resourced constrained, or buried in the organization where they cannot be heard. The one team that can help the organization is essentially neutralized and ignored.

4. Research: What Founders Say

Vanessa interviewed six CEO/Founders from various verticals, including hospitality services, security, learning, and services/consulting. Five of these companies were pre-series B in the funding process, less than seven years old, and had less than 100 employees. Through the rest of this paper, she will refer to these five companies as the target group. One of the companies was 16 years old and backed by private equity. She decided to talk to this more mature company founder compared to the other five companies and will refer to this as the control group or company. She conducted hour-long interviews with each of the CEO/Founder with a questionnaire located in Appendix A.

These interviews took place during the Covid-19 crisis, and for some of the companies, these impacts were quite dramatic, including having to layoff significant portions of their employee base. This crisis seemed to have crystalized priorities for these leaders and turned out to be good timing in testing Vanessa's assumptions relative to Maslow's hierarchy of needs.

When asked how much the leaders thought about security when they first founded the company, three out of the five target group companies did not focus on security. The two companies who did focus on security early did so because they knew that security would be important to selling their product and building the brand reputation. The three companies' priority not focused on security was on; proving out there was a market for their product/service, getting the product to work, and plain survival. One leader commented, "My conversations were focused on whether we would be able to keep the lights on, I can't think about art if I don't have enough to eat." Another leader commented, "Security was not top of mind; I had other short-term goals, and gates for survival that were the priority."

The two target group companies who did think about security early did so because they knew their market demanded it. They would need to establish a strong brand reputation around security to enable sales. One target group leader commented, "I focused on security early on as I knew I wanted to sell my product to the enterprise segment right out of the gate. If I had wanted to go business to consumer, not sure I would have thought the same way." The other target group leader commented, "I knew we had to prioritize security due to reputational issues, but pressure

from the investors was forcing us to be lean, we needed to be secure but had to be practical on what we did relative to security." So even though these target group leaders focused on security, they mainly did it to enable sales and drive revenue.

The next relevant question was focused on how the target group leaders talk to their employees about security. The importance of this question goes to the point of establishing culture and values around security early. Two of the target group companies did not have a strong emphasis on security when talking to their teams. When they did talk to their teams, it was more around compliance and some basic best practices. One target group leader commented, "The Sales team in the company did not care about security. Security wasn't completely off the radar, but because our customers (consumer-focused company) didn't care, we just did what others in our space did to meet the minimum requirements."

Three of the target group companies did take a stronger approach to communicating with employees. One leader commented, "I told the team if we want to do this then we need to do this, we need to earn the business and security was a requirement." This same leader commented that it was not easy to set the tone, especially early in the company, asking himself, "if spending money on security was the right thing to do right now?" Another leader commented, "Security, privacy, and confidentiality were a cornerstone for the company from the beginning to build an effective brand." The leader commented that because of establishing these values, she was able to attract security talent easier. Presently in her company, she commented, "I talk about security like it is everyone's job. I frequently talk about it on weekly calls, and there is high accountability around it in terms of each employee doing their jobs. You need to practice what you preach, and it is a topic for all employee reviews."

The control group company had a much more mature approach to the culture, as would be expected. This leader commented, "I drive accountability to everyone. I help employees understand how important security is by bringing real-life examples to the team and discussing those examples in stand-ups. Then I invest in training and give people rewards and recognition for the desired behavior. I have established a culture of constant learning around security, not based on punitive action when mistakes are made. It has taken me two years to develop the culture around security." This comment establishes the challenges around building a culture of security, and for many startups, it is just too early to have the culture take root to the extent it needs to be established.

The third relevant question that Vanessa discussed was the priority customers placed on security and how that has changed over time. Two of the target group companies started in the consumer space and then pivoted to the enterprise space. Their experience considerably varied when working with Consumers versus the enterprise. One leader commented, "Security was not something they (consumers) talked about." A security services company's leaders noted, "Consumers were hard to convince on security. There were lot of hand-holding in convincing. It was a huge hurdle, even if you could demonstrate experiences they had in losses due to a lack of security." As these two companies pivoted to the enterprise space, their experiences and expectations relative to security changed, and privacy seemed to take a more prominent role. One of the leaders commented, "Security expectations are ever-changing, GDPR is taking a top priority for us. We will need to stay up to date on security challenges and learn from others." The other leader commented, "COVID has changed everything, privacy events have driven questions around security. People don't understand security, as privacy is more relatable."

When asking the control group company about the priority of security with her customers; the leader commented, "The priority has changed over the past decade. In the beginning, we focused on basic security controls, and customers gave their suppliers the benefit of the doubt. Now customers expect security as a baseline. Startups still have not caught up with the fact that customers expect security now. In her observations, later-stage startups are thinking more about security today than they did previously."

Relative to the question, "was there a pivotal event that shifted their priority of security and the support they received around security", four out of the five target group companies said large enterprise deal was a pivotal point and was a catalyst for a shift and focus around security. "When we first talked to Walmart, they had a ton of questions around security, and this helped me realize (as the leader), we didn't know what we were talking about relative to security. I decided to dedicate someone to security as a result of that experience." Another leader commented that security requirements from prospective enterprise customers forced the processes to change at his company. "I only started thinking about it when it came to enterprise sales. SLA requirements around penetration tests, questionnaires, security scorecards. The shift was customer-driven."

The role of the Board/Investors relative to security was the next relevant question. Vanessa asked how that role has changed from the early phase of the company till now. Of the five target

group companies, only one company said the Board/Investors asked about security, "They asked about SOC2 certification to enable sales, I also got a sense that they were concerned about risk mitigation." Some other interesting quotes from the leaders included, "The Board only focused on revenue and executing the plan,"; "Product marketing fit and raising money were the important topics, sometimes hiring,"; "Investors see security as a necessary evil." Even in the present day, the Board still had little to no interest in security. One target group company that had early interest from the Board continues to discuss security with the Board, "I produce regular security updates, we think more about risk and they want to see the due diligence around security, they want to hear about issues and what is being done to address the issues." Another target group leaders noted, “Models and pressures from LPs drive VC and Institutional Investors. Their push is to have companies grow and not focus on security.”

This lack of interest/involvement around security by the Board/Investors produces major conflicts for a leader who does want to drive a priority and focus around security. As one leader commented, "The Board had zero to say about security, anyone investing in a business model that is direct to consumers has no clue on security. They had no real appreciation for the work needed to establish a consumer brand with security. They consistently challenged my focus on security." How does a startup leader place the right priority or resources around security if not supported by the Board/Investors?

In asking the leaders around priority and how it was set relative to security, there were various responses and approaches. One leader described his priorities in this way, “My priorities are business focused: generating revenue, validating the solution, raising money, and meeting requirements of my customers." Another leader had a very hands-off approach to security, “My CTO handles all the security priorities, I trust him and his decisions, I have a lot of confidence in him.”.

When Vanessa asked the target group how they determine how many resources to allocate to security, none had a structured approach to this decision. The leaders’ following statements reflect this conclusion: "There is no process or approach in place. Right now, I just try to optimize the money spent and keep it to a minimum. Every time we turn around, there is a new compliance framework to comply to; this burden is a big challenge for the future.”; “I rely on the team to do the right thing and have the right plans.”; “There is no firm metric on security spend. The biggest challenge is the competition for security resources and the high salaries of security

professionals. I also need to control the sprawl of tools and applications." Unlike the target group companies, the control group company did have a specific number, which was tied to a percent of R&D spend.

Finally, Vanessa asked the target group what they viewed as the key to their success relative to security in the future. One leader in the target group commented that she was not thinking about security; she was thinking about survival (the company just went through a layoff due to COVID). Therefore, this reinforces Vanessa's earlier points about Maslow's Hierarchy of Needs and this leader being in the survival mode and not thinking about security at all. Other leaders highlighted the need to continue funding security, baking security early in the culture, and ensuring the culture doesn't take short cuts. One leader emphasized not turning a blind eye to things, not in their control, be realistic to what is going on and find solutions to the challenges. The control group leader commented, "I need to hire people who know more than I do about security; are connected to the right networks; leverage all the resources I have including the Board; being humble and making sure I always connect security to the strategic company priorities."

5.0 Process and Controls Recommendations

Implementing the right set of security measures within a startup is a delicate balance between minimizing risk and optimizing spend. Often Vanessa has heard those less knowledgeable in the security space minimize the complexity of the security challenges. Purchasing one particular tool is not going to solve the complex challenge of security. Security is far more than a tool; it is a mindset, a culture, a set of values, processes, skilled people, and obviously, technology. Founders must think about each of these areas when addressing the future security maturation of their companies. Vanessa has noted the general cost estimate gauged by *high, medium*, and *low* investment rating at the end of each of these recommendations.

5.1 Culture/Setting the tone

The establishment of a startup is exciting; the founders are immersed in self-actualization at the top of the pyramid. They are optimistic and wondering if they are starting the next big

thing that will change the world or a unicorn that will bring them incredible wealth and financial independence. This is the phase of the company where security should be introduced into the culture, and it is the least expensive point to begin introducing security.

In defining the tone around security in the company, there are a few important data points that must be understood in establishing whether your company primarily serves the enterprise segment or the Consumer segment. If your company primarily serves the enterprise segment, security will likely be an important element of selling into that segment. As was evidenced in the research, Vanessa did with the Founders; most remarked that the turning point for them was trying to meet the security requirements of the potential enterprise customers. It will be important to establish a strong brand that is associated with security if you want to be successful in the enterprise space.

If the product or service is targeted at the consumer segment, whether security will be important to your customer depends on the product or service. For example, if you are selling a Fintech service to consumers to help them consolidate debt, then security will likely be important. However, if you are selling a new type of sports clothing, security might not be as important to the customer in forming a perception of the brand. Again, as noted in the interviews with Founders, while security may not have been a concern of consumers, privacy is a concern of consumers. Therefore, the principles of privacy (which include security requirements) should be a priority and something to emphasize in the culture of the company.

Cost: *Low*. The Founder needs to take time to talk to the team and establish the values of the organization.

5.2 Governance

Why should a startup need governance? Governance can be a complex and heavyweight process in larger and mature organizations. Vanessa would recommend a much lighter weight approach to governance in a startup. The main reason she recommends having a governance process in a startup is similar to recommendations by several of the founders she interviewed; you want to build security in early.

Governance is a set of processes and approaches to assist with defining risk tolerance, managing risk, sorting out roles and responsibilities, generating policies, establishing priorities, and

resourcing the priorities properly. This sounds like a lot of work, but it can be achieved in a very efficient manner. Vanessa recommends initially establishing a monthly meeting with the right attendees, including the Founder/CEO, head of technology, a key security resource, and legal if you have in-house legal. This small group will discuss current security risks, the acceptability of those risks, and, if not acceptable, what will be done about those risks. This group can also discuss current customer security/privacy requirements and how those will be prioritized. These meetings should have documented minutes that can be used to demonstrate a level of governance to potential auditors.

Cost: *Low*. Founder should ensure these meetings happen and should be facilitated by them or another strong leader.

5.3 Minimizing the creation of technical debt

When a company is innovating and growing fast, short cuts are taken. There is never time to do it completely right, especially early in the company, when there are minimal resources available, and they must be focused on the highest value work. Unfortunately, the attitude, "we can fix that later" can have very costly and damaging impacts on the company in the future. This accumulated short cut decision making leads to a dangerous inefficiency within the business termed "technical debt." Technical debt can take on many forms, including sub-optimal software architecture, poor asset management, lack of scalable processes, unmanaged access control, and security vulnerabilities. According to Dag Liodden (Firstmark, 2018), there are three reasons for technical debt:

1. Deliberate technical debt- technical decisions made to reduce time to market.
2. Accidental/outdated design tech debt- system evolution and requirements changes cause the original design to no longer appropriate.
3. Bit rot technical debt – numerous patches/updates done by different people who don't understand the end design

If left unresolved and unmitigated, technical debt can become the greatest risk to the company. Some of the most pernicious technical debt comes when the fundamental architecture of the product presents serious security vulnerabilities, and the only way to address the vulnerabilities is to completely re-architect the product. This remediation effort could be so great; the company may not be able to afford the resolution of the security issues. The lack of remediation will result in an inherently insecure product, with the only recourse being to implement sometimes costly mitigating controls to lessen the security risk.

The Founder must ensure that they are looking at decisions from a medium/long term perspective. They must weigh out the risks of accepting technical debt with meeting deadlines and other revenue-generating activities. The more successful the company becomes, the more critical sound decision-making in this area becomes. If the Founder continues to take on risk related to the technical debt, it could come back to hurt the company later. As one of the interview candidates noted, "It's a lot easier to struggle now (with security) than suffer later."

Cost: *Medium to High*. The Founder should keep track of the risks taken and have a plan to address those risks at some point. These risks can be discussed in the governance meetings.

5.4 Investing in security resources

At some point, a startup will realize they need a dedicated security resource(s) to focus on security. This realization will likely be driven by either a security incident or a customer request. Most startups Vanessa has dealt with, were driven to hire security resources through the questions or concerns expressed by a potential or existing customer. As one target group leaders noted above, "It wasn't till the Walmart deal that I decided to dedicate resources to security." The enterprise customers are most likely to drive this requirement as their standards for security are much higher than the startup likely has for themselves.

During the vendor vetting process by the enterprise customer, they will ask the startup numerous security and compliance questions. Questionnaires from the Financial Services sector can be quite onerous, some exceeding 50 pages of questions. It is usually at that point that most startups realize they need some help with security, and they need to hire someone. Who is hired

as a security leader will be largely dependent on the items Vanessa previously discussed, including culture and the amount of technical debt in the company.

When Vanessa asks startups what they are looking for in a security leader, she hears many requirements, including someone versed in technology, communicates well, can talk with the Board, can inspire people, and can talk to customers and help with sales. There are very few individuals that meet all these requirements, and if they were found, the startup probably would not be able to afford them. According to Salary.com, the median salary plus bonus for CISOs in the US is $276,000 (not including benefits) (Salary.com, 2020). In Vanessa's experience, top security engineers and architects can range between $170k- 230k/year.

A critical decision a startup must make is when to hire security resources and specifically what type of resources to hire. Vanessa recommendation around security hiring for a startup depends on a few factors noted below:

- If the company has a large percentage of developers and the company is primarily a software product serving the enterprise space, she would recommend hiring two people to focus on security. The first person would be a developer with a strong security skill set, someone who could evangelize and educate the rest of the developer community relative to security. The second person should be strong in the Compliance and Privacy space and will interface with customers and prospects to address their concerns around compliance and security. This second person will also help the company achieve compliance certifications mandated by the enterprise customer.
- If the company is mainly focused on the Consumer space, she would recommend hiring one resource who is strong in the Compliance and Privacy space. She would also recommend working with a security consultant (outsource) to perform any technical security work needed, such as penetration tests.

Cost: *High*. Founders selling into the enterprise space must invest in security early.

5.5 Compliance Certifications and Privacy Laws

If the startup is focused on selling to the enterprise space, there will be numerous compliance certifications required by the customers depending on customer verticals. Below are some examples of vertical industry requirements:

- Financial services: FFIEC standards and guidance
- Healthcare: HIPAA and HiTRUST
- Biopharma: CFR part 11
- Federal Government: FedRAMP and NIST 800-53

Obtaining certifications present a real cost to startups, and there should be a solid strategy around which certifications to pursue. Costs include new processes, tools, and auditor/certification fees. Vanessa would recommend that a startup look at the following certifications and prioritize compliance to those compliance frameworks:

- Service Organization Control- SOC 1 and SOC 2. Enterprise customers ask to see the SOC reports routinely. Startups should prioritize this as one of the first certification efforts they pursue.
- ISO 27001. As an international standard, ISO 27001 is helpful if the business is done globally. Actual certification at the early stage is not recommended, but aligning the security program to the framework would be important.
- GDPR and ISO 27701 for Privacy
- Payment Card Industry (PCI), if the startup accepts or processes credit cards.

Cost: *Medium-High*. The Founder should help the organization focus relative to compliance certifications. If the startup works across verticals, this focus will be even more important. It can be tempting to commit to a customer prospect as the focus will be on the potential revenues and not the costs related to the compliance effort.

5.6 Board management

The Founder must work with the Board members 1 on 1 and outside of the actual Board meeting to evangelize her/his priorities around security. There will likely be a component of the education of the Board member in these conversations. Finding a Board ally in the security journey will be critical to generate the support the Founder will need to execute on their plans.

Cost: *Low*. Return on investment very high.

6.0 Key Technical Controls

Startups need to implement some basic level of technical security controls, especially in light of the challenging threat environment in which they all operate. To do this effectively, investors need to support the implementation of basic security controls. Contrary to the research found in the interviews where investors had little interest in security, Vanessa believes investors should view these controls as protecting their investments. Protecting intellectual property and customer information should become an imperative of investors, and spending some level of funds on security should be prioritized.

Determining what is the right level of funds to invest in security is the challenging part. A majority of the Founders interviewed (5 out of 6) did not have a specific way to measure or determine if they were investing the right amount of resources into security. This is not just a challenge for startups, but it is also a challenge for mature public companies. It is particularly challenging for startups as cash is a precious resource that must be managed carefully; the very survival of the company depends on it.

Vanessa believes the Center for Internet Security (CIS) Controls (Appendix B) is a practical framework to utilize when deciding which security controls to implement. The current version of CIS Controls, version 7.1, encompasses a concept of Implementation Groups (IGs). Implementation groups outline a phased approach to implementing the 20 control areas based on the maturity and resources available to your organization to devote to security.

Before analyzing these recommendations and offering thoughts on key controls for a startup, Vanessa would like to make a few foundational notes relative to technology and its use in a startup:

- Leverage Cloud and SaaS applications as a priority, avoid on-prem systems as much as possible.
- Leverage the security tools available on the Cloud provider when possible.
- With a high concentration of Cloud and SaaS applications, ensure that there is a strong skill set in the company to manage these suppliers effectively.

- Equip your workforce with devices that enable mobility and freedom to conduct business in a flexible way.
- To the extent, developers are needed, interview, and hire developers that have a security mindset.
- While there are many nice tools available to manage Governance, Compliance, and Risk (GRC), a simple excel spreadsheet or google sheet is adequate to manage GRC in a startup.
- Consider joining an ISAC, https://www.nationalisacs.org/, to obtain low-cost threat intelligence.

Assuming the foundational elements noted above, Vanessa would recommend that the CIS control focus areas for a startup in the chart below. The CIS Control framework includes many of these as a part of Implementation Group 1, which are suited for "small to medium-sized companies with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel." For any that are noted below that are not a part of IG1, Vanessa distinguished those with an asterisk in the sub-control. Additionally, she has omitted some of the IG1 controls based on assumptions above and experience in working with startups.

CIS Control	CIS Sub-control	Description	Implementation Note
1	1.1*	Utilize an active directory tool to identify devices connected to the organization's network and update the hardware asset inventory	Leverage a cloud-based directory, MS, Okta, and OneLogin are tools in this space
	1.4	Maintain a detailed asset inventory	Implement a tool such as JAMF (for Macs) or SCCM (for Windows)
	1.8*	Use client certificates to authenticate hardware assets connecting to the organization's trusted network	This can be the same tool used for 1.1
2	2.1	Maintain an up to date list of all authorized software that is required in the enterprise for any business purpose or any business system	This should include software on the endpoints as well as SaaS applications
	2.6	Ensure that unauthorized software is uninstalled, or the inventory is updated promptly	The tools noted in 1.4 can assist with this control
3	3.4	Deploy automated software update tools to ensure that the OS is running the most recent security updates provided by the software vendor	The tools noted in 1.4 can help accomplish this control
	3.5	Deploy automated software update tools to ensure that 3rd party software on all systems is running the most recent security updates provided by the software vendor	The tools noted in 1.4 can help accomplish this control
	3.7*	Utilize a risk rating process to prioritize the remediation of discovered vulnerabilities	This can be developed in the security governance meeting

4	4.1*	Maintain inventory of Administrative accounts	While automation of this is desirable, a quarterly access review on critical systems can be the starting point
	4.2	Before deploying any new asset, change the default passwords to have values consistent with administrative level accounts	This should be a distributed responsibility with each system administrator taking ownership for this task
	4.5*	Use multi-factor authentication and encrypted channels for all administrative account access	Tools implemented in 1.1 can help with this control
	4.8*	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges	These logs can be sent to the system in control 6.5
	4.9*	Configure systems to issue log entry and alert on unsuccessful logins to an administrative account	These logs can be sent to the system in control 6.5
5	5.4*	Deploy system configuration tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals	Tools implemented in 1.4 can assist with this control
6	6.2	Ensure that local logging has been enabled on all systems and networking devices	This should be a responsibility of the system administrator work with the security resource to determine which logs to enable
	6.5*	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review	Look to leverage open source systems or outsource centralized log management
	6.6*	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis	Look to leverage open source systems or outsource centralized log management
7	7.1	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization	The tools noted in 1.4 can help accomplish this control
	7.7	Use the Domain Name System (DNS) filtering services to block access to known malicious domains	The tools in 8.1 can help accomplish this control
8	8.1*	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers	Many anti-malware providers have outsourced monitoring and response capabilities
	8.6*	Send all malware detection events to enterprise anti-malware administrative tools and event log servers for analysis and alerting	Many anti-malware providers have outsourced monitoring and response capabilities
9	9.4	Apply host-based firewalls or port filtering on end systems, with a default deny rule that drops all traffic except those services and ports that are explicitly allowed	The tools in 8.1 can help accomplish this control
10	10.1	Ensure that all systems data is automatically backed up regularly	Leverage Cloud and SaaS services to accomplish this
11	11.4	Install the latest stable version of any security-related updates on all network devices	The number of these devices will be limited as there should be a minimum footprint on actual office space
	11.5*	Manage all network devices using multi-factor authentication (MFA) and encrypted sessions	This can be the same tool used for 1.1
13	13.1	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider	This control can be accomplished by an excel spreadsheet which is reviewed every 6-months
	13.5	Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices	Tools implemented in 1.4 can assist with this control

14	14.6	Protect all information stored on systems with the file system, network share, claims, application, or database-specific access control lists	This is largely a manual effort reviewing all systems where sensitive data resides
15	15.7	Leverage AES to encrypt wireless data in transit	
16	16.3*	Require MFA for all user accounts, on all systems, whether managed on-site or by a 3rd party provider	This can be the same tool used for 1.1
	16.7*	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination of employee or contractor	There may be manual elements of this process
	16.13*	Alert when users deviate from normal login behavior, such as time of day, workstation location, and duration	These alerts should be sent to the tool in control 6.6
17	17.6	Train the workforce on how to identify different forms of social engineering	This can be accomplished through discussions with the team and showing them examples
	17.9	Train the workforce members to be able to identify the most common indicators of an incident and be able to report such an incident	Implement an email alias that employees can use to alert the right individuals in the event of a suspected incident
18	18.6*	Ensure that software development personnel receive training in writing secure code for their specific development environment and responsibilities	Free online training is available for developers to take
	18.9*	Maintain separate environments for production and non-production systems.	This is an important control to establish from the beginning and can be easily achieved in a cloud environment
19	19.1	Ensure there are written incident response plans that define roles of personnel as well as phases of incident handling/management	Involve all key people in generating the plan
	19.7*	Plan and conduct routine incident response exercises	Start with two table-top exercises a year
20	20.2*	Conduct regular external penetration tests	Hire an external party to conduct two pen tests of the product code as applicable

To summarize, some key tools will help a startup accomplish many of these security controls:

- **Cloud Directory provider**
- **Identity and access management cloud solution**
- **Endpoint management tool**
- **Endpoint advanced malware tool**
- **DNS Filtering tool**
- **Log collection and correlation tool**

Vanessa recommends focusing on this toolset primarily as a first phase of building technical controls.

7.0 Working with Startups (Note to Large Enterprises)

The primarily benefit startups offer larger enterprise customers is innovation. They deliver new products and services to an enterprise that either is not focused on that innovation or may not have the capabilities to deliver that innovation. The startup community allows larger enterprises to offer differentiation (generate new revenue), disrupt inefficient processes (cost savings), or deliver a better customer experience (maintain revenue). An enterprise interested in the product or service the startup has to offer would have a vested interest in their success. There are specific steps an enterprise can take to help ensure the success of a startup they want to leverage.

The first important element of ensuring success is implementing the right supplier risk management process. Many large enterprises have an extensive supplier risk management process comprised of questionnaires, evidence gathering, contract negotiations, and audits (remote and on-site). When dealing with a startup, the enterprise should consider the amount of time and resources their supplier risk management process will take from the startup. Vanessa recommends that enterprises develop a scaled-down approach for their processes when dealing with the startup. The scaled-down process should omit questions that obviously would not apply to a company composed of less than 100 people. The decision on which questions to omit will depend on the vertical and the risk tolerance of the enterprise.

The second important element is to approach the relationship as a true partnership with a legitimate interest in seeing the startup be successful. A large enterprise has a lot of resources and experiences that can be useful to the startup, including providing them input on their roadmaps, offering to introduce them to key subject matter experts in the enterprise who could share their approach or solution on a particular initiative, allowing the startup to leverage the enterprise logo from a marketing perspective, and doing webinars in conjunction with the startup to highlight use cases.

Keep in mind the reason an enterprise chooses to do business with a startup is that they have some unique value to bring to the enterprise, not because they have the same level of maturity in security and other processes that the enterprise has in place. There will need to be some level of increased risk tolerance by the enterprise in exchange for innovation.

8.0 Conclusion

Founders have the difficult challenge of balancing the survival of the company with the needs and demands of their customer base. They often do not receive the support of their investors, and this compounds their challenges relative to security. While there are differences in customer expectations depending on whether the customer is in the enterprise or consumer space, the expectations around security and privacy are continuing to grow over time.

Interviews with Founders/CEOs have reinforced the hypothesis Vanessa laid out at the beginning of the paper. Startups are primarily focused on surviving, and not focused on security and when they were focused on security, it was to drive revenue, which is survival. Knowing that they need to survive, and security is a key element of that survival, founders need a set of foundational controls and processes on which to focus. These focus areas include:

- Setting the right tone and investing in the culture of security.
- Putting in place a basic Governance structure and associated processes.
- Minimizing technical debt and actively managing that debt.
- Investing in the right people.
- Focusing on a limited set of compliance certifications.
- Actively managing the Board/Investors.
- Implementing a key set of technical controls.

Enterprises rely on the innovation of the startup community, and they also must assist in their success. Startups will need the support of the enterprise space to deliver the security they demand.

Vanessa Pegueros, vpegueros@gmail.com

References

Kupor, Scott. (2019). *Secrets of Sand Hill Road.* Portfolio/Penguin.

Maslow, A.H. (1943). *A Theory of Human Motivation*. Psychological Review, 50, 370-396.

Embroker (2020). *106 Must-Know Startup Statistics for 2020*. Retrieved March 21, 2020, from https://www.embroker.com/blog/startup-statistics/#ss-1

Mimosa, Michael. (2014). *Hacker Puts Hosting Service Code Spaces Out of Business*. *Threatpost*. Retrieved March 21, 2020, from https://threatpost.com/hacker-puts-hosting-service-code-spaces-out-of-business/106761/

Pro OnCall Technologies (2014). *3 Companies that Went Out of Business Due to a Security Breach*. Retrieved on March 21, 2020, from https://prooncall.com/3-companies-went-business-due-security-breach/

Connolly, Bryon, and Gardiner, Bonnie. (2015). *Case study: When a hacker destroys your business*. *CIO*. Retrieved March 21, 2020, from https://www.cio.com/article/3497650/case-study-when-a-hacker-destroys-your-business.html

Firstmark (2018). *There are three main types of technical debt. Here's how to manage them*.. Retrieved on April 3, 2020, from https://hackernoon.com/there-are-3-main-types-of-technical-debt-heres-how-to-manage-them-4a3328a4c50c

Salary.com (2020). *Chief Information Security Officer Salary in the United States*.. Retrieved on March 27, 2020, from https://www.salary.com/research/salary/benchmark/chief-information-security-officer-salary

Center for Internet Security, (2020). *CIS Controls V7.1*. Retrieved on May 9, 2020, from https://learn.cisecurity.org/cis-controls-download

Charan, Ram, Carey, Dennis, Useem, Michael. (2014). *Boards That Lead*. Boston, Massachusetts, Harvard Business Review Press.

Nesheim, John L. (2000). *High Tech StartUp*. New York, The Free Press.

National Council of ISACs. (2020). https://www.nationalisacs.org

FFIEC Information Technology Examination Handbook, Information Security. (2016). https://ithandbook.ffiec.gov/media/274793/ffiec_itbooklet_informationsecurity.pdf

FFIEC Information Technology Examination Handbook, Management. (2015). https://ithandbook.ffiec.gov/media/274809/ffiec_itbooklet_management.pdf

Gallagher, Bernard. (2018). *SOC 1 and SOC 2 Reports- Do You Know the Difference? Partners,* https://www.ispartnersllc.com/blog/soc-1-soc-2-reports-difference/

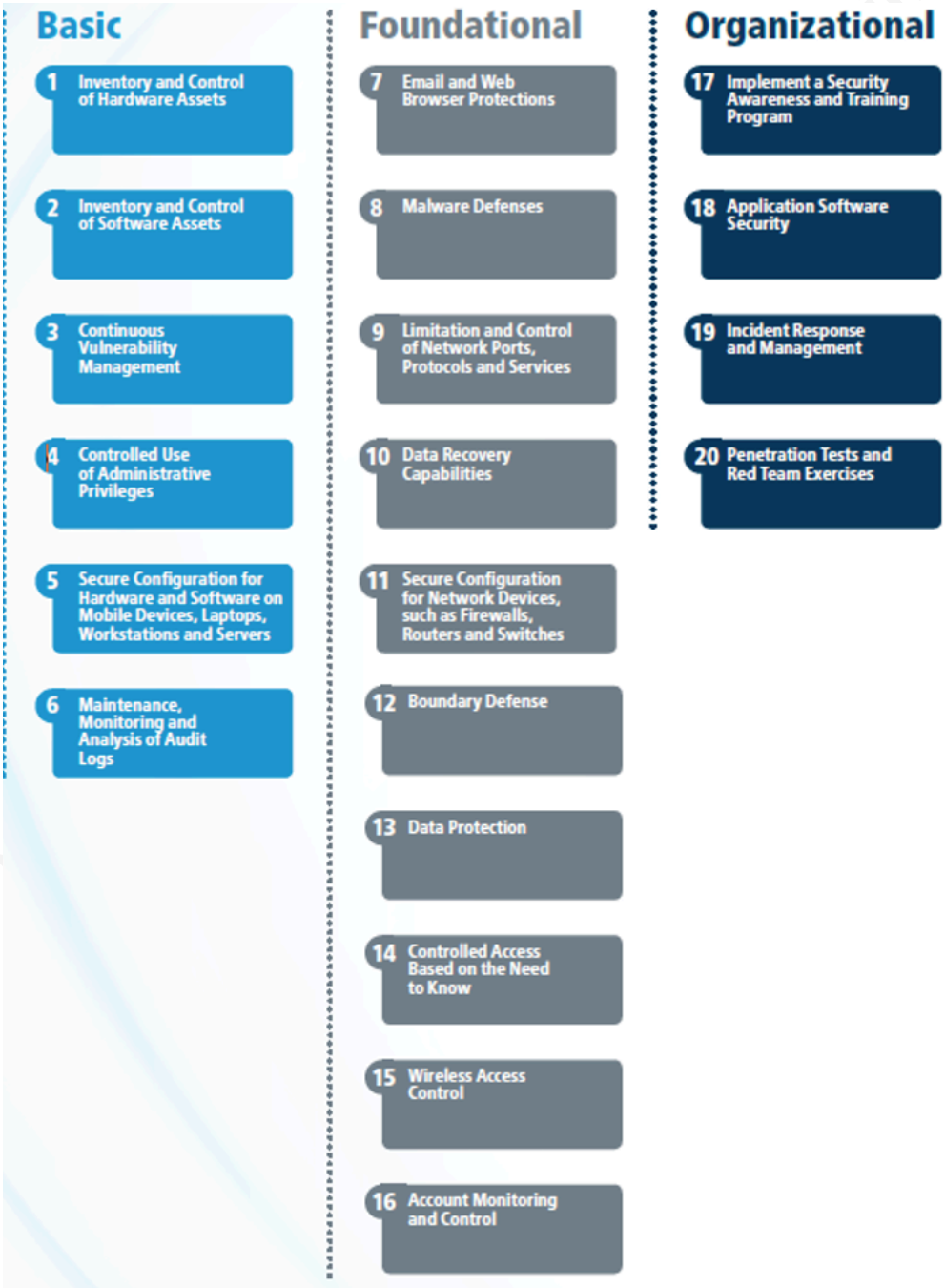
NIST Special Publication 800-53 Revision 4. *Security and Privacy Controls for Federal Information Systems and Organizations*. April 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Appendix A

Founder/CEO Questionnaire

1) Company profile
   a) When was your company founded?
   b) How many employees?
   c) What vertical do you operate in?
   d) When you founded the company, how much did you think about security? What did you think about it?
   e) What level of priority is security with your customers?
   f) Do your customers ask more about Compliance or Security?
2) Thinking about when you first started the company within the first 6 -18 months
   a) How much did you think about security?
   b) If you thought about security, how did you think about it, and why was it a priority?
   c) What were the priorities of what you thought about?
   d) Did you talk to your team about security, and if so, how?
   e) Did your Investors/Board ask about security?
   f) What was the Investors/Board's influence around security?
3) If you didn't think about security in the first 6 – 18 months
   a) When did you first start thinking about security?
   b) Was there an event that sparked your focus on security?
   c) Once you started thinking about security, how did you think about it? Do you think about people, process, and/or technology?
   d) How much do you equate Compliance to Security?
4) Presently
   a) What is your culture around security?
   b) Does your Board ask more about security?
   c) What is your role relative to security in your organization?
   d) What qualities do you look for in the person responsible for security in your organization?
   e) Do your customers ask more about security now compared to the first 6-18 months. If so, why do you think this has changed?
   f) How much resource (people and technology) should you devote to security?
   g) What is the key to your success around security in the future?

Appendix B
CIS Controls Version 7.1,(6.)



Vanessa Pegueros, vpegueros@gmail.com

Last Updated: October 25th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Sydney 2020	**Sydney, AU**	**Nov 02, 2020 - Nov 14, 2020**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**Nov 09, 2020 - Nov 14, 2020**	**Live Event**
APAC ICS Summit & Training 2020	**Singapore, SG**	**Nov 13, 2020 - Nov 28, 2020**	**Live Event**
SANS Community CTF	**,**	**Nov 19, 2020 - Nov 20, 2020**	**Self Paced**
SANS Local: Oslo November 2020	**Oslo, NO**	**Nov 23, 2020 - Nov 28, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**