Jonathan Siegel

Final Report

A GDPR-Ready Cybersecurity and Privacy Plan for B2B SaaS Startups.

Abstract

B2B SaaS startups struggle to comply with regulatory requirements. There are many evolving standards that require documentation and controls. These requirements overwhelm startups, to the extent that they do not even attempt to comply. In fact, however, the practices of these startups often do follow best practices in security. The difficulties are in closing the gaps between requirements and practices and in creating the documentation to support the startups' decisions. The paper investigates whether template plan and practice documents can be constructed for use by B2B SaaS startups to complete their alignment and gain GDPR compliance.

Introduction

Young and inexperienced teams are creating software companies every day. It is exciting to see young leaders enter the business world and thrive. But, these same leaders lack experience and mentorship. They lack a healthy respect for privacy, security and regulation. The repercussions are scary—and they are impacting business

and society. To create a better outcome for all parties, a digestible cybersecurity plan is needed, which can form the basis of a more security and privacy aware community.

The topic of this paper is timely, as security breaches continue, public perception is increasingly aware of privacy issues and new regulation creates exacting economic consequences.

Background

A young company is called a startup. Startup companies struggle to create and implement security and privacy policies.[1] A class of these startups provide Software as a Service (SaaS). A further refined class of startups provide these SaaS services from their business to other businesses (B2B). B2B SaaS startups use similar practices and often have a baseline of security in their implementation.[2] It is a challenge to document these practices and understand what gaps exist. There is little expertise in a startup to implement this.[3]

[1] Robehmed, Natalie, "What Is A Startup?" Forbes, (May 15, 2015), accessed January 23, 2019: https://www.forbes.com/sites/natalierobehmed/2013/12/16/what-is-a-startup/.
[2] Wang, Kaitlyn, and Kaitlyn Wang. "So Long, Copycats. Warby Parker Is Already Onto Its Next Big Thing." Inc.com, (November 29, 2017), accessed January 23, 2019: https://www.inc.com/kaitlyn-wang/warby-parker-2017-company-of-the-year-nominee.html.
[3] Cowan, David. "Security for Startups," Bessemer Ventures, (2015), accessed February 1, 2019: https://www.bvp.com/sites/default/files/files/strategy-resource/SecurityforStartups-TheAffordableTenStepPlantoSurvivinginCyberspace.pdf.

According to Ready.gov, cybersecurity involves "preventing, detecting, and responding to cyberattacks that can have wide ranging effects on the individual, organizations, the community, and at the national level."[4] According to Merriam Webster, cybersecurity is "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack."[5] Privacy is, among other things, the ability to limit the access to one's data. Startups do not have the resources to staff a variety of security professionals and typically, a single teammate may handle concerns regarding privacy and cybersecurity. With limited resources, these teams tend to focus on implementation concerns rather than the documentation typically required for compliance.

The General Data Protection Regulation (GDPR) was adopted by the European Union and went fully into effect in May 2018.[6] This regulation highlights the difficulty that SaaS startups face in complying with regulations. In a January 2018 poll of 4,000 startups, only 33% were compliant with the GDPR.[7]

The GDPR was cited by several startups that shut down rather than work towards compliance. Streetlend.com shut down after five years of operation claiming "due to uncertainty and risk created by the GDPR." They added that "the penalties associated

[4] "Cybersecurity." Citizen Corps, accessed January 23, 2019: https://www.ready.gov/cybersecurity.

[5] "Cybersecurity." Merriam-Webster, accessed January 31, 2019: https://www.merriam-webster.com/dictionary/cybersecurity.

[6] "EUR-Lex Access to European Union Law." EUR-Lex - 52011DC0681, accessed January 31, 2019: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX:32016R0679.

[7] Kurzer, Robin. "Only 1/3 of Startups Are GDPR-compliant, Study Finds." MarTech Today, (August 14, 2018), accessed January 23, 2019: https://martechtoday.com/international-study-reveals-one-third-startups-gdpr-compliant-210104.

with the Regulation made it too costly for Streetlend.com to remain active."[8] Another startup, Tunngle shut down citing "pending requirements of the new European General Data Protection Regulation."[9]

Even when a startup does not go out of business because of regulations, it is clear that startups do not relish the challenges of meeting regulatory requirements. The website Calm.com said, "GDPR, the new EU legal regulation on data privacy, has been keeping many folks awake at night of late." And "our eyes glazed over reading this 57,509-word, 209-page document" which got them "excited by the sleep aid potential of GDPR." Ultimately, they turned the document into a spoken word sleep aid because the "GDPR could sedate a buffalo."[10]

The lack of interest in regulatory requirements is a problem today as many young startups are gaining ad hoc usage within security-conscious, primarily larger enterprises. Last year, Greylock Venture Partner, Sarah Guo, wrote an article on "Startups serving the Enterprise." This article covered over a dozen topics. The top item? Security. Her article included a customer quote to sum up the perspective, "we see startups repeatedly miss on security and resiliency—they have the functionality and

[8] "R/Games - Tunngle Is Shutting down Tomorrow (30/04/2018) 'due to Pending Requirements of the New European General Data Protection Regulation.'" Reddit, accessed January 23, 2019: https://www.reddit.com/r/Games/comments/8fli1t/tunngle_is_shutting_down_tomorrow_30042018_due_to/.
[9] Bisson, David. "Lending Website Cites GDPR Concerns as Reason Why It Shut Down." The State of Security, (April 30, 2018), accessed January 23, 2019: https://www.tripwire.com/state-of-security/latest-security-news/lending-website-cites-gdpr-concerns-as-reason-why-it-shut-down/.
[10] "The Ultimate Insomnia Cure? New GDPR Law Becomes Bedtime Story for Grown-ups." Calm Blog, (May 24, 2018), accessed January 23, 2019: https://blog.calm.com/relax/once-upon-a-gdpr.

agility we want but they don't understand the rigor around security we need. It's not a choice we have, it's regulatory."[11]

This is a recent phenomenon because of the way Software as a Service is adopted.[12] Traditionally, enterprise software sales required the C-suite to review and approve software in a hub and spoke model. Software was sold to the hub and pushed to the organizational periphery. This was necessary when software was installed behind the firewall and required ongoing maintenance by an internal operations team. Software as a Service changes the paradigm. By definition SaaS is a hosted service which requires no internal operations and is hosted outside the firewall. This enables individual business units to adopt SaaS without C-level review. Services like DropBox, RightSignature and GoToMyPC spread within organizations because of their accessible price and immediate availability—and often their features rival behind-the-firewall alternatives. This adoption cycle reverses the hub and spoke model—teams at the organizational periphery make choices that ultimately force the hand of the C-suite hub. Ultimately, this adoption pattern encourages SaaS adoption into the enterprise without the express permission of the CIO/CSO officers.

[11] Guo, Sarah. "Startups Serving The Enterprise: – Greylock Perspectives." Greylock Perspectives, (July 26, 2018), accessed December 15, 2018: https://news.greylock.com/startups-serving-the-enterprise-6d318fd15c04.
[12] Forrest, Conner. "Businesses Are Adopting SaaS Too Fast to Properly Secure It." TechRepublic, (April 10, 2018), accessed December 12, 2018: https://www.techrepublic.com/article/businesses-are-adopting-saas-too-fast-to-properly-secure-it/.

For young startups, the state of the art today is to defer the security conversation as long as possible to avoid the investment in creating a policy. This does not mean that startups do not act secure. It is often the opposite. Startups are quick to adopt new standards (PGP, Secure Browsers, 2FA, SSL, etc), but they lack the business resources to staff and document their choices. Chase Cunningham, Forrester Principal Analyst, participated in one of the security industry's most attended conferences, the RSA conference. It is expected that all companies present are aware of security best practices. However, in a recent article, Mr. Cunningham described his experience interviewing startups at the RSA conference. He calls this the "Self-Licking Ice Cream Cone of Misery."

> It sounds like a joke, but there were 130 startups at the event. I made it a point to ask every third team about security, privacy, and GDPR. I had five responses that I would say were even in the ballpark of security; only two even knew what GDPR was. Seriously, only two! Most of them thought it was an acronym for a protocol that they would 'ask their devs about.'[13]

Startups facing the challenge of regulatory compliance are typically startups that are one to two years old, have raised venture funding and are starting to find product market fit and grow their team. FirstRound Capital identifies this startup stage by

[13] Forrest, Conner. "Businesses Are Adopting SaaS Too Fast to Properly Secure It." TechRepublic, (April 10, 2018), accessed December 19, 2018: https://www.techrepublic.com/article/businesses-are-adopting-saas-too-fast-to-properly-secure-it/.

headcount “10-19 employees” and describes how “you want to have someone who’s responsible for security,” but you will not have a full-time role. “It’s likely your CTO or whomever might grow into that title.” And at “this stage, the company is in a vulnerable, asynchronous relationship with anyone who threatens it. Attackers have infinitely more resources and time than the startup does to defend against breaches.”[14]

Although an investment in security is a clear advantage to customers, it is not yet obvious whether this would also encourage investors. Let’s imagine two startups with one million dollars in funding. One spends all of the funds on cybersecurity and the other spends all the funds on go-to-market. The latter company would have more revenues and likely have stronger investment potential even if it were structurally unsound from a security perspective. Security issues tend to be latent until they wreak their damage.

If a startup today wants to develop a security policy, they must: start from scratch; hire an expensive consulting firm (estimates of $30k to produce elementary documents for just one regulatory perspective); employ an expert. Starting from scratch has harsh time and cost consequences—upwards of six to 18 months for an organization to develop expertise. Meanwhile, there is a dearth of cybersecurity experts—available either for consulting or employment. At the same time, the regulatory environment is a moving

[14] Graham, Michael. "How Early-Stage Startups Can Enlist The Right Amount of Security As They Grow." First Round Review, (March 29, 2016), accessed January 15, 2019: https://firstround.com/review/how-early-stage-startups-can-enlist-the-right-amount-of-security-as-they-grow/.

target (SAS70 or SOC? SOC I or SOC II? SOC II or ISO? PCI-DSSX? GDPR?). These factors conspire to create a real and tangible barrier to capturing and encouraging efforts in the young SaaS community.[15]

While there are many vendors that support security best practices, there is no single vendor that can provide 100% cybersecurity best practices within the reach of a startup and its budget. For instance, Amazon Web Services (AWS) is often used by startups, and AWS is GDPR compliant when used correctly. But, using AWS correctly and documenting that process is exactly the struggle the startup has in the first place. Even when they make good technical decisions, they do not have the wherewithal to construct a complete set of practices and documentation to meet the needs of their customers, particularly where regulation like the GDPR is involved.

Materials and Methods

Saas B2B Startups

A prototypical startup can be used as a model to create a template security policy that shows the compliance strengths and weaknesses of these businesses. The methods examine whether a template security policy tied to common implementation schemes can support the GDPR compliance needs for B2B SaaS businesses. In other words,

[15] NeSmith, Brian. "The Cybersecurity Talent Gap Is An Industry Crisis." Forbes, (August 13, 2018), accessed December 19, 2018: https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis/#61c3ec1fa6b3.

can assumptions be made about B2B SaaS startups and their choices, and can these assumptions be used to derive a standard cybersecurity and privacy plan?

The prototypical startup makes consistent choices. There are many factors that influence these choices. Startups tend to have younger technology teammates who have recently adopted their skills. These teammates often have a passion for technology and look to emulate best practices. The abundance of startup documentation makes assumptions that there are little to no fixed assets in the business. This means that there are few restrictions on accommodating existing vendor choices. For instance, there are no mainframes in startups, so applications do not have to target legacy systems. The opposite is often the case in existing businesses. Because a startup inherits essentially nothing, they may make best of breed choices. Startups are often capital starved, so they choose to move their expenses to operational expenses rather than capital ones. For instance, instead of buying server hardware, a startup will likely rent that hardware through a cloud infrastructure vendor.

Young SaaS businesses often adhere to a pattern of practices: a consistent choice for their web hosting needs (e.g. Amazon Web Services), using the same service for source code management (e.g. GitHub.com), using common workstations (e.g. Apple MacBook) and security practices (e.g. encrypted filesystems and two factor authentication).

Startups are more and more coming from incubators that train a specific set of technology choices. The vendors providing technologies have recognized these patterns and provide high levels of subsidy through these incubators. For instance, AWS provides up to $100,000 of infrastructure credits to startups, which consequently encourages cash-strapped startups to use AWS services.[16]

The proposed Plan makes assumptions about the tools used by startups. The assumptions are made since otherwise the Plan will not be able to address details. Details are probably more meaningful than generalizations. The assumed tools used by startups need to be validated. Review of StackShare.io, which uses a number of methods to determine the type of technologies in use by a particular technology company, validated that the technologies assumed in the Plan were in common use by startups. For instance, AWS is used by more than 10,000 companies.[17]

GDPR-Ready Cybersecurity and Privacy Plan for B2B SaaS Startups and the Cybersecurity Practices

Assuming that a young startup had no documentation, many documents might be developed to provide a minimal security and privacy perspective. For instance, there could be a Cybersecurity Policy, a Privacy Policy, a BYOD Policy, a SDLC plan, etc. Each of these documents must be drafted to reflect the capabilities of the business as

[16] "AWS Activate Providers." Amazon, accessed January 23, 2019: https://aws.amazon.com/activate/providers/.
[17] "Why Developers like Amazon EC2." StackShare, accessed January 23, 2019: https://stackshare.io/amazon-ec2.

well as the regulatory environment in which the business operates. Moreover, these documents should not become "proud words on a dusty shelf,"[18] but active documents reflecting the operational ability of the team. New teammates need to become aware of the documents and operate accordingly. Given the barriers to survival faced by a young startup, creating awareness and compliance around many security documents is yet another challenge. As a result, the goal has been creation of a simplified pair of documents, which will encompass all aspects of cybersecurity, privacy and implementation concerns.

The first document, the GDPR-Ready Cybersecurity and Privacy Plan for B2B SaaS Startups (the "Plan") addresses regulatory compliance in abstracted terms. Abstracted means that the document does not need to reference implementation specifics. For instance, the Plan can state that "background checks are performed," without the need to detail the vendor that provides the background checks. This is the domain of another document. The Plan is twinned with the Cybersecurity Practices (the "Practices"). The Practices, the related document that accompanies the Plan, provides the implementation practices necessary to adhere to the Plan. In another example, the Plan lists the data storage goal, "store sensitive information encrypted at rest." For this element of the Plan, the Practices articulates the tactical requirement, "choose AES256 or better." The Plan is a customer-facing document, which outlines commitments relevant to clearing regulatory and organizational requirements, without the need to

[18] Hensley, Ken. "Proud Words On A Dusty Shelf." Albums - Proud Words On A Dusty Shelf, accessed January 23, 2019: http://www.ken-hensley.com/works/albums/proud-words.html.

understand implementation details within a particular vendor. In this way, a startup may publish their Cybersecurity plan for customer awareness, regulatory requirements, competitive differentiation, employee onboarding, and vendor review.

The Practices function as an inward-facing document, which a startup can use to cross-check its compliance with a strong security commitment. Finally, both the Plan and Practices are based on common implementation decisions made by startups. As stated before, startups often make secure technical decisions, but lack the sophistication and expertise to map those choices to the regulatory environment. Through use of the Plan and Practices, the startup will have confidence that it is complying with the requirements of applicable regulations.

In an ideal world this pair of documents would be compliant with all possible regulations. However, this paper focuses only on the GDPR. This simplifies the problem, adds clear expectations and aligns the work to a current challenge.

To understand how the GDPR was used to guide the Plan, let's look at GDPR Article 5. GDPR Article 5 sets out the principles relating to processing of personal data. This article discusses how data is collected, data transparency, as well as data minimization. These topics were used to articulate the Plan. Specifically, the Plan incorporates this regulation in a section titled "Principles."

> Our security principle is the golden rule: Treat others as you'd like to be treated. We are a technical team building technical products that primarily serve small teams like our own. We are always short resources, but we are staffed similar to our industry peers. We aim to direct our resources to the best use--and this holds true in a cybersecurity context. For instance, we have a portion of our team that works remotely. Do we require our teammates to work inside a secure environment? No. It's impractical and not our industry norm. However, we do not encourage private data to be left unsecured on a personal device with an easy opportunity for theft. Why? Because we would not want our data treated like that--and with a small bit of preparation, it is reasonable to never arrive in this type of situation. When in doubt, return to our security principle. It will always provide authentic guidance.
>
> We intend to treat customer data fairly, transparently and securely.

This is reinforced through further sections in the Plan. One section discusses the "Data We Collect." Since this is a generic plan, the section defers to a separate listing that the business using the Plan would edit:

> We collect data for our core service, we collect our direct user and account data and we keep third party data where relevant to our operations. By default, we attempt to minimize the data we collect.

> See more details on the data we collect.

There is a corresponding section that covers “Data We Do Not Collect.” This section not only responds to GDPR Article 5, but also to GDPR Articles 25 and 32:

> We do not store data of the following flavors and ask that our customers ensure that they do not send to us: personal health information, credit card or other sensitive personal or financial information. For our own credit card processing, we use a PCI-compliant third party, who manages credit card details. We do not store them ourselves.

Although this is a template plan, there are assumptions that match the practices of our candidate B2B SaaS startup.

Existing SaaS security documentation, SaaS startup practices, vendor security reviews and GDPR requirements were reviewed to create this Plan. Starting with the authored SaaS security document, the plan was separated from the Practices, creating the base Plan and Practices. Using these initial drafts, three vendor security review questionnaires were reviewed: One from a Fortune 500 enterprise customer, one from a thriving startup bound for an IPO and one from a mid-size business. These

questionnaires served as a stress test for the documents to help flesh out new requirements as well as refine what already existed.

The Fortune 500 customer provided a document titled “Consensus Assessments Initiative Questionnaire.” This document exists as a spreadsheet with 299 rows. Each row contains a subsection requirement defined by the Cloud Security Alliance, such as “CCC-04.1 -- Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or -managed user endpoint devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.” Columns are included for a document-consistent taxonomy as well as work areas for a vendor to indicate their compliance, non-compliance, and notes on the response. Finally, the document includes columns that cross-link these 299 rows to their counterparts in many compliance frameworks: BITS Shared Assessments SIG v6.0, BSI Germany, Canada PIPEDA, COBIT 5.0, COPPA, CSA Enterprise Architecture, FedRAMP Security Controls (Final Release, Jan 2012), FERPA, GAPP (Aug 2009), HIPAA/HITECH, NERC CIP, NIST SP800-53 R3, NIST SP800-53 R4 Appendix J, NZISM, ODCA UM: PA R2.0, PCI DSS v3.0 and others.[19]

This customer-provided Consensus Assessments Initiative Questionnaire was reviewed and an original document from the Cloud Security Alliance was retrieved and it was

[19] "Consensus Assessments." Cloud Security Alliance, accessed January 14, 2019: https://cloudsecurityalliance.org/working-groups/consensus-assessments/#_overview.

found that little was changed on the vendor copy. Three things were particularly encouraging about the document: the document appeared to be exceedingly complete, customers were using the document "as-is," and it was extensively cross-linked. The completeness of the document meant that it was a strong candidate for finding missing aspects of the Plan and Practices. If the document was being used unchanged, then it meant that a Plan and Practices that satisfied the document would likely satisfy many vendor security reviews with little-to-no additional effort. Finally, although the cross-linked index could not help with GDPR (the document predates the GDPR release), it could provide additional compliance mapping if aligned with the Plan and Practices.

The Consensus Assessments Initiative Questionnaire taxonomy was adopted alongside the GDPR when indicating the controls within the Plan and Practices. Starting with documents from a real SaaS policy, a list of practices was determined that aid or detract from compliance. This in turn started a self-referencing editing session between the Plan and the Practices. For example, if SaaS practices generally do not support the expunging of consumer data, then the plan outlined why GDPR Article 17 (the "right to be forgotten") is noncompliant unless the startup makes modifications to its practices. Alternatively, if SaaS practices generally use access controls, because services tend to host on AWS and AWS offers this out-of-the-box, then the plan outlines why GDPR Article 25 (data protection by design and by default) is in compliance. A set of Practices tied to a Plan for compliance facilitates testing that the outputs are accurate.

Common questions asked in these vendor security reviews were reviewed as a starting point for the candidate documents. For example, a vendor security review might ask, "Do you use an automated source code analysis tool to detect security defects in code prior to production?" The answer requires some knowledge of the technology choices made by the responding startup. Startups use a common tool, GitHub.com, which provides static source code analysis to identify known defects. As a result, startups using GitHub.com can use a known answer to this question. It is straightforward to articulate a response in the Plan. Similarly, adding a corresponding practice of using GitHub.com in the Practices ensures the Plan requirements.[20]

The activity of reviewing vendor security review questions and responding with entries in the Plan as well as in the Practices continued until there were no questions left unanswered. The Plan includes the following topic areas: Schedule, Overview, Audience, Principle, Design Considerations, Data We Collect, Data We Do Not Collect, How Long We Keep Data, MetaData, and many more. The sections in the Practices include: Designing for Privacy and Security, Encryption, 2FA, Production Data, Workstations, Web Browsers, Data Organization, Background Checks, CI/CD, and many more. These documents were cross-linked where possible.

[20] Han, Miju. "Introducing Security Alerts on GitHub." The GitHub Blog, (January 04, 2019), accessed January 23, 2019: https://github.blog/2017-11-16-introducing-security-alerts-on-github/.

Results

The Plan and the Practices, in draft form, were submitted as responses to vendor security reviews by a startup advised by the author. Additionally, the Plan and Practices were submitted for review by an advisor at Google, as well as a number of startups in the author's network.

Discussion

One goal for the documents was to run through actual vendor security review materials from existing startups and from advisor contributions, and determine whether the documents adequately answer the vendor questionnaires in a satisfactory manner. This has been done for three vendor security reviews. It means that startups will benefit from an articulated security commitment, the vendor questionnaire questions were addressed and the (three) practices were sufficient to meet the expectations of the client.

Conclusion

The Plan, coupled with the Practices can meet the GDPR compliance needs of a B2B SaaS startup. Since, heretofore, SaaS B2B startups did not have a plan or the capability to produce one, the Plan and Practices provide a practical method for starting a security conversation, which will result in general improvement of this subindustry.