Security for Startups:

The Affordable Ten-Step Plan for Survival in Cyberspace

by David Cowan

The Ten Step Plan

Introduction

“We’re Too Small to Worry About Security…”

Focus is the key to startup success. With limited resources, a short runway, and formidable competition, entrepreneurial teams must drive relentlessly to engineer compelling customer experiences. Startup cultures dismiss other concerns as corporate bureaucracy, be they dress codes, 401K plans, corner offices, or GAAP accounting. So naturally, startups have typically deferred investments in cyber security as a corporate indulgence that can wait. After all, who would bother attacking a startup anyway?

“Startups don't like friction to get their job done. Security feels like friction.”
- Ajay Varia, VP Engineering, Piazza

Even just a couple of years ago, it may not have seemed unreasonable for most company founders to completely ignore cybersecurity threats. But cyberspace has changed a lot since then, in ways that touch and threaten every online business, big or small. Startups now use the same networks and cloud infrastructure that mature companies do, and can quickly aggregate large, juicy caches of their users’ personal data and payment credentials. As malware infestations crawl the web, scaling up in scope to scour through the “long tail” of targets, they do not discriminate between the Fortune 50 and the TechCrunch 50.

In fact, some increasingly common cyber attacks (e.g. DDoS extortion schemes) specifically target smaller, more vulnerable businesses: the loose cowboy culture of startups, combined with a lack of security expertise, fragile infrastructure and fresh venture capital, make for easy pickings.

“Startups are incredibly vulnerable to cyber attacks in their first 18 months. If a business thinks that it's too small to matter to cybercriminals, then it's fooling itself with a false sense of security."[1] – Brian Birch, Symantec

Jeremy Grant, an adviser at the Department of Commerce’s National Institute of Standards and Technology has, in the past two years, seen "a relatively sharp increase in hackers and adversaries targeting small businesses."[2] According to a recent survey, 20% of small businesses in Canada reported falling victim to cyber crimes in the prior 12 months.[3] Who knows how many more fell victim and just

[1] http://money.cnn.com/2013/05/23/technology/startup-cyberattack/
[2] http://www.inc.com/magazine/201312/john-brandon/hackers-target-small-business.html
[3] http://www.betakit.com/20-of-canadian-businesses-fell-victim-to-cybercriminals-last-year/

don’t know it?

For many of these attacks—API disruption, marketplace fraud, IP theft—the smaller the target, the more damage they inflict. We have seen startups set back as much as a year, or even fail altogether, as the consequence of a cyber attack from identity thieves, nation state warriors, hacktivists, aggressive competitors, disgruntled employees, IP thieves, fraudsters and Bitcoin miners — in some cases barely surviving the barrage. Evernote, Meetup, Vimeo, BaseCamp, Shutterstock and Bit.ly all fell victim to extortion rackets,[4] and Code Spaces shut down altogether. “When our API collapsed under a DDoS attack, we experienced more customer churn in that one day than we had in the entire two years since our launch,” recalled one CEO.

Stubhub,[5] Uber,[6] and Tinder[7] struggle to battle fraud in their marketplaces. Uber employees themselves were caught defrauding competitor Gett. Evernote, Bit.ly, Formspring, Dropbox, Cupid Media, Snapchat, MeetMe,[8] LastPass (a password security company) and many others have had to tell users they lost their passwords or payment credentials to hackers. Cyber thieves put high-flying Bitcoin startup Mt. Gox out of business. Hackers exposed the content and identities of Yik Yak accounts.[9] The CEOs of Clinkle, HB Gary, Snapchat and many other startups have been vilified in public following the theft and publication of embarrassing emails. Many startups like Appstudio, SendGrid and HB Gary have been defaced or even permanently shut down by anti-Western hactivists for political reasons; for OnlyHonest.com, the damage appears to have been fatal.

And even if your startup beats the odds and survives its infancy without (an awareness of) a serious incident, playing catch up later will cost you many times more in time, money, reputation and distraction as you change architectures, re-write code, move infrastructure, re-image laptops, migrate email boxes, and replace billing systems.

But it takes years for startups to grow to the point where they can afford a Chief Information Security Officer, so until then how can entrepreneurs do their jobs of protecting their mission, the company’s assets, the employees’ livelihoods, and their investors’ capital from the threats of cyberspace? For startups with

[4] http://bits.blogs.nytimes.com/2014/04/03/tech-start-ups-are-targets-of-ransom-cyberattacks/?_php=true&_type=blogs&_r=0

[5] http://www.nbcnews.com/tech/tech-news/stubhub-ticket-reseller-says-its-victim-massive-cyber-fraud-n162676

[6] http://www.dailymail.co.uk/news/article-2601891/Man-managed-inappropriately-rack-50-000-dollars-worth-Uber-credit-slashed-500-leaving-bad-review.html

[7] http://www.alleywatch.com/2014/06/how-cyber-thieves-are-targeting-online-daters/

[8] http://www.databreaches.net/meetmes-notification-to-california-attorney-generals-office/

[9] https://gigaom.com/2014/12/08/yik-yak-shown-no-slack-in-intern-hack-attack/

limited resources and intense focus, what is the right measured response to these threats?

To help answer these questions, I surveyed the security practices of Silicon Valley startups to understand both their regrets and successes in mitigating the impact of cyber attacks on their businesses. I interviewed mostly the technical founders behind startups that flourished into successful companies, but I also interviewed some of the people hired later as Vice President Engineering, Chief Technology Officer, or Chief Information Security Officer to get a perspective looking back on what measures should have been taken sooner, or in some cases, later.

It became clear to me that adopting strong security practices is much easier to do when a company is young, while they still enjoy the advantages of a smaller attack surface and a manageable number of devices to track. Despite the onslaught of new threats and perils that increasingly characterize online commerce, I was encouraged to learn that some basic, affordable practices – both technical and cultural – can mitigate the greatest risks to startups and position them well for developing a strong cyber posture as they scale. So we now advise founders to consider these recommendations from Day One, and revisit the overall plan quarterly to review their team's progress in taking these steps.

A secure organization starts at the top with the CEO, but it demands a team effort with contributions from everyone. So whether you are in a leadership position in finance, engineering, operations or finance, or simply in a position to influence those who are, this "ten step plan" could potentially save your startup. The title of each chapter parenthetically indicates the role most suited to take the lead on that step of your startup's survival in cyberspace.

Any original wisdom you encounter likely came from one of the following experts who assisted me in this endeavor: Dan Farmer (author, and inventor of SATAN), Sunil James (who fought the cyberwars at Mandiant and iDefense), Barrett Lyon (the original anti-DDoS warrior and hero of the book Fatal System Error), Richard Clarke (author and top intelligence and cybersecurity officer in the White House and State Department), Nils Puhlman (CISO of Zynga), Sunil Nagaraj (security venture investor at BVP) and startup CTOs Shankar Srinivasan, Ajay Varia, Peter Offringa, Mike Tans, and Alex Li.

Cyber security is a moving target, and it will remain so for as long as human beings compete for resources on a planet with digital assets. So as you read, please think about what may be missing, and share your feedback with cyber@bvp.com. This is a challenge that we all face together!

At Bessemer, our goal is the same as the entrepreneur's – to minimize the distraction of cyber threats so each startup can focus on its mission. Just keep in mind that if you want your startup to make a dent in the world, you can't let hackers make a dent in you.

Step 1. Business Cyber Risk Analysis (CFO or GC)

> *Securing digital assets is a daunting challenge for everyone from large corporations to governments, individuals and startups precisely because there are so many vulnerabilities and defenses that it's hard to know where to start. With so many ways to hack our systems, why do we even bother?*

We need a plan, and it starts with an enumeration of all the cyber risks at a business level. What really bad things could befall our startup as a result of a cyber attack? The purpose here is not to develop a plan to eliminate all these risks – that would be a folly even for wealthy corporations with extensive security teams – but rather to identify, quantify and thereby prioritize the risks we should and can mitigate with minimal distractions from the core mission. Only then can we make intelligent decisions about defense, and confidently assess our state of readiness.

There are well established models for analyzing an organization's security needs and capabilities, such as the NIST Cybersecurity Framework.[10] But these frameworks are overkill for understaffed startups. As a simpler alternative, I recommend focusing your efforts on creating a Business Cyber Risk Analysis (BCRA), consisting of a Threatscape and Defense Plans.

Threatscape

The BCRA Threatscape can start as a simple spreadsheet with four columns: threat; likelihood (i.e. expected incidents per year); full dollar loss per incident (assuming no defenses); and expected loss (calculated as the product of the prior two fields). Independently estimate the likelihood and loss for each threat because, while all businesses face similar threats, the impact from each varies greatly from one type of business to another. A marketplace cares more about fraud, a technical service provider cares more about DDoS, and a biotech team cares more about IP. And as our businesses grow, the risk and damage from each threat changes, and so this analysis needs to be a custom, living document managed by Finance or Legal but ultimately owned by the CEO.

The most common security threats facing startups are:

[10] http://www.nist.gov/cyberframework/

- Stolen or Leaked IP: How bad would it be if someone else (or everybody else) had access to your intellectual property? Consider the damages from increased competition (lost sales, lower pricing, less access to PR, talent and capital) and the loss of opportunity to file for or enforce patents. For some startups this threat is existential, and for others less important.

- Stolen funds: how bad would it be if either an insider or outsider embezzled corporate cash or other currency flowing through your startup's infrastructure? This may be immaterial to a developer tools company, but it poses an existential threat to a Bitcoin service provider.

- Stolen computer resources: if hackers commandeered your infrastructure to mine bitcoin, or steal network bandwidth, would the increased performance load and costs impact your business in a material way? Stated another way, how critical are application performance and cost of delivery?

- Stolen business information: if your competition had access to your sales pipeline, contract bids, product plans, sales strategies, and financial statements how damaging would that be?

- Account data breach: if you had to recover from a breach of your customer account data (including passwords and payment credentials if you have them), how badly would that damage your business? Consider the customer churn, remediation costs (e.g. assuming responsibility for identity theft over a large population), regulatory fines, and class action lawsuits. This threat is material to anyone with an e-commerce component, and existential to security and financial service companies.

- Employee information: how would your employees react to the compromise of your HR data, which would expose their job performance, compensation, and health-related data? Consider the loss of morale, impaired productivity, employee turnover and lawsuits. We have even seen employees of one security startup personally targeted by Chinese state hackers who had compromised the HR database.

- Email Dump: it doesn't take illegal activity to embarrass a company or an individual. Every challenge you face – even those of a personal nature – may one day be dumped on TOR for everyone to read. How will that damage your startup's brand with customers, investors, acquirers, and prospective hires?

- <u>DDoS attacks</u>: A common regret of startup CTO's is their past complacency around DDoS. Even moderate-sized attacks will take down your site, mobile app, and APIs. The lost revenue is the least of your problems that day, followed by the costs of remediation and technical support. The largest damage is the churn you experience from customers who cannot tolerate downtime.

- <u>Cyber bombs and back doors</u>: how critical is your business to national security and safety? Would a nation-state or other geopolitical player ever wish to sabotage your business as a way of attacking a population? If so, then you need extra restrictive access to your code, and a vigilant pursuit of zero-day vulnerabilities.

- <u>Marketplace fraud</u>: So many startups today depend upon a community of users, where trust is critical. When hackers hijack your application through spam, fake profiles, and fraudulent transactions, they jeopardize the entire community. Zoosk, for example, prioritized this threat above all others in their Threatscape, since trusted profiles are paramount in a dating service.

- <u>Conduit to attack</u>: Hackers often target large organizations through suppliers who have access to the institutional partner's network or data. A fledgling company's reputation can be ruined, and customers lost, once it is viewed as a vector for cyber attacks. This is especially relevant for cloud-based technology companies that store proprietary data for businesses and governments.

There are other types of cyber threats as well that do not pose existential threats but can still cost a great deal of time and money, such as physical theft, sabotage of computing assets, ransomware attacks (which are more common than you might think), audio surveillance of employee conversations, and phishing attacks on your customers that hurt your brand. It's a good team-building exercise as you talk to your key personnel and collectively think through all the possibilities that are relevant to your business.

Here's an example of a line item that may appear at the top of the Threatscape for a startup that delivers real-time services to other businesses primarily through an API:

THREAT	LIKELIHOOD	LOSS / INCIDENT	EXPECTED LOSS
Large DDoS Attack (50+ Gbps for 2+ hours)	1.2 incidents / year (based on industry averages)	Lost gross margin $2k Remediation $100k 10% churn $2,000k (based on 10% drop in market value)	$2.522M / year

Defense Plans

Once you have completed the Threatscape, rank the threats by expected loss, and you are ready to start drafting a Defense Plan for each one. Each threat defense plan consists of seven fields: preventive measures, detection measures, pre-remediation measures, post-remediation measures, the revised forecast for expected attack frequency, the revised loss per incident, and the revised expected loss from that threat. Pick up most of the defensive measures you'll need within the next nine steps of this paper. As for the numbers, do not worry too much about precision; it's fine to estimate. Just run them by your teammates and investors to make sure they're in the ballpark.

With threats ranked by expected cost, you can now rationally decide which preventive measures make sense for your business. Preventive measures are the most expensive and so you will need to look carefully at costs here. No doubt you will want firewalls around your network and URL filtering, but other preventive measures will be selected to match your Threatscape and budget. For example, if stolen IP or stolen business information rank highly in your BCRA, then you could use Data Loss Protection (DLP), remote device wipe and strong multi-factor authentication. If marketplace fraud ranks highly, than you need device ID technology to keep fraudsters off the system. If account data breach is your principal concern, than static analysis and web firewalls will be needed to filter out SQL injection attacks.

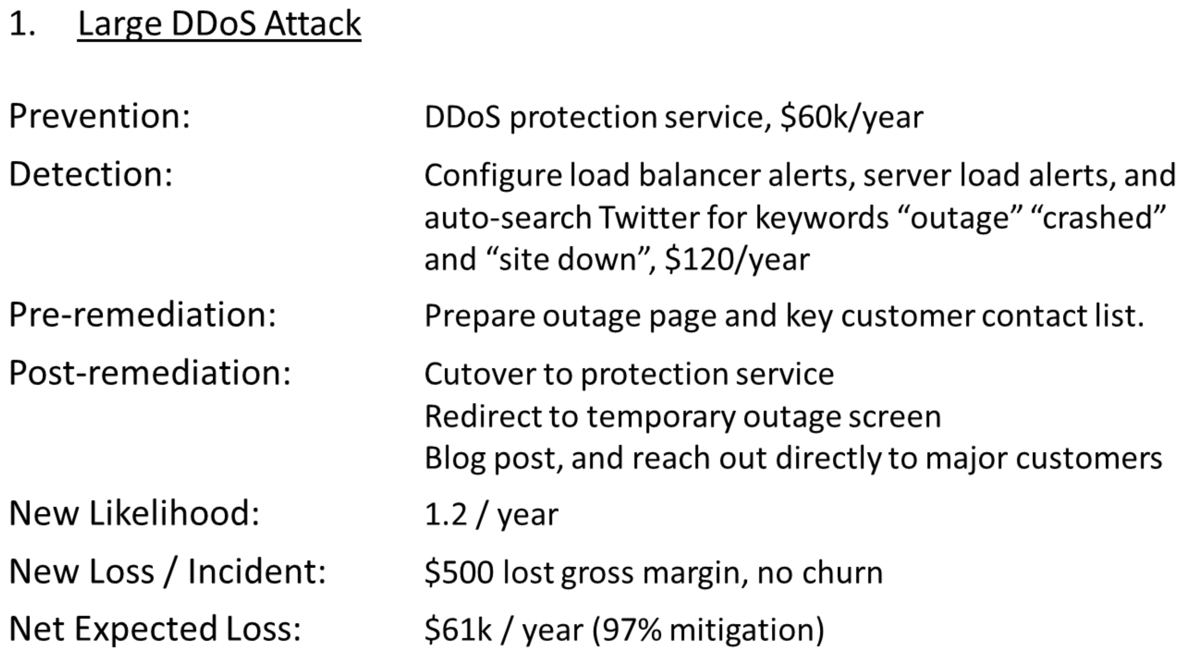
Often detection measures are easier to implement and have a higher ROI. Most attacks will go undetected without detection measures like log analytics, site scanners and endpoint malware sensors. Some attacks are obvious, but even then you benefit from early detection. For example, some DDoS attacks can be detected before they reach the point of shutting down your servers. For other attacks, you will never know you are a victim unless you look. If stolen IP and business information are priority threats for you, services like MarkMonitor, Tiversa and Digital Shadows will find leaked documents on the web or dark nets.

Pre-remediation defenses are measures you can take now to be prepared to remediate incidents. For example, if account data breaches pose a threat to your business, you can prepare yourself now for remediation by researching your legal obligations of notification and signing a contingency contract for ID theft protection for the victims (see the chapter below, Plan for Breaches). The up-front cost of these measures is minimal.

Finally, prescribe post-remediation measures (even for threats that you are not defending against preventively). For example, to mitigate the threat of account data breach, find a strong forensics team nearby that you know you can activate on short notice, and plan out all the steps you will take, including a communications plan with regulators, auditors, customers, and journalists. This plan will save you significant time in the event of an incident, dramatically curbing the damage at no up front cost.

As you add each measure to your Defense Plans, it's a good idea to include figures on the expected cost of that measure. Hopefully you will get some good ideas of affordable defensive measures from the chapters below.

Here is an example of a Defense Plan corresponding to the sample Threatscape item above, Large DDoS Attack, and drawing from advice from some of the chapters to follow (so don't dwell yet on the specifics):



1. Large DDoS Attack

Prevention:	DDoS protection service, $60k/year
Detection:	Configure load balancer alerts, server load alerts, and auto-search Twitter for keywords "outage" "crashed" and "site down", $120/year
Pre-remediation:	Prepare outage page and key customer contact list.
Post-remediation:	Cutover to protection service Redirect to temporary outage screen Blog post, and reach out directly to major customers
New Likelihood:	1.2 / year
New Loss / Incident:	$500 lost gross margin, no churn
Net Expected Loss:	$61k / year (97% mitigation)

Crafting and maintaining a BCRA is the foundation of a strong security posture, and it needn't cost your startup anything to create one. However, if you would like expert help to ensure completeness and steady attention to it, cyber readiness consulting firms Good Harbor Security and Black Hills Security provide excellent guidance. Until you have a dedicated security team, consider hiring them to help you adopt the ten steps in this plan, and to perform an independent security review annually to ensure that you are deploying the right measures to secure the crown jewels of your business.

Step 2. Embrace Security in Your Culture (CEO, CTO, IT)

Each startup's culture sets a tone in the organization for years, impacting who joins you, what values they embrace, and the individual judgments they make on a daily basis. The culture can be deliberately crafted, or it can simply emanate from the founders' own behavior.

> *Thousands of decisions are made every day. Culture is how you, as say a leader of the company, are confident that every one of those decisions is the right one.*[11]
>
> *– Jeff Lawson, Founder of Twilio*

It is NOT uncool or too "corporate" to care about security. Google and Facebook, for example, embraced security in their cultures early on, and today those companies boast two of the strongest cyber teams in the industry. If you think your company is doing something important, then you only reinforce that idea with others by showing that you value security.

Employees will take their cues from the founders. If the founders scoff at security policy and make a point of bypassing it, undoubtedly others will take license to do the same. For security to work, every person in the company must not only comply with the policies, but should be vigilant in discovering cyber incursions, and participate creatively in the common defense. While few of us are security experts, we can all keep our eyes open for suspicious activity.

Here are five ways reinforce security within the startup culture:

- Share the BCRA with all employees, so that they inherently appreciate the threats to your business, and why you have chosen to focus on certain defenses and not others.

- Schedule periodic training sessions, which the founders and executives actually attend! Not only is training necessary for some defensive measures, but it mitigates the friction that security imposes on the workplace. Group training sessions are a great venue to work through

[11] http://www.wired.com/2013/09/how-do-you-define-startup-culture/

issues that encumber productivity. You can supplement training sessions with training videos like ones at SANS.[12]

- Create an easy reporting mechanism (e.g. security@yourstartup.com) for any employee to report suspicious activities. Be sure that there is a response and follow-up to all legitimate queries. (Any email communication internally in response to a Security issue or breach should always include the general counsel and be clearly marked as “attorney client privileged”.)

- Adopt a platform either for single-sign-on like Okta or Ping, or for password management like LastPass or DashLane,[13] to make it easy for everyone to follow good password hygiene.

- Schedule penetration testing on a regular basis – at least annually (about a $20k expense) – and each “pen test” should simulate targeted phishing attacks on your employees (Swan Island Networks and PhishMe specialize in this practice). Every time your employees click on a suspicious email, you have a chance to train them on what to look for before they open links or attachments. Rapid7, K2[14], Black Hills and Trustwave are examples of reputable pen testers.

[12] http://www.securingthehuman.org/enduser/demo-training-lab

[13] BVP is an investor in DashLane.

[14] BVP is an investor in K2 Intelligence.

Step 3. Select the Right Platforms (Engineering, IT, Ops)

> *Early on, startups make important decisions without necessarily thinking through the consequences. For example, founders usually choose a city without necessarily studying the costs of doing business, local taxes, or the availability of local talent. The same can be said for the computing devices and services used early on, even though these are effectively choices that have a profound impact on cybersecurity.*

Selecting the right computing platforms is a cheap and easy way to mitigate many cybersecurity threats.

Usually the first platform selected is the laptop computer, starting with the founders. You might consider using Apple products instead of Windows, since they have better application sandboxing as well as a track record of less malware (although the difference is fading now that Apple has 20% market share and hackers find it worthwhile to attack them). If you prefer a flavor of Linux, Chromebooks are a highly secure, affordable choice. Try to centralize administrative control of all software installations, limiting app downloads to an approved white list to any computers outside your development and design teams. To prevent most infections, restrict laptop use to work related applications – no gaming! And be sure to run an endpoint discovery tool that reveals new executables that may have slipped through.

As for smartphones, they are all notoriously insecure, but Apple iPhones are probably the best choice. Apple has closely moderated the App Store, routinely removing suspicious or malicious apps, while anyone can create an Android app store; even Google Play exercises minimal security oversight.

Startup employees – not always the most compliant workers – will naturally bring their own devices; they can connect to the Internet through the same wireless network that you cordon off for guests. (Use WPA2 encryption on all your WiFi networks.)

Also, favor open source products for both development and production stacks. Open source software benefits from broad scrutiny of its security, and it tends to get quickly patched. Also, selecting open source products will leave you more budget to spend on cyber infrastructure!

Although Google Apps isn't free, at $50 per user per year it's a bargain, and offers compelling security benefits. Google has implemented multi-factor authentication using your smartphone, and works well with single-sign-on across their apps.

With the proliferation of cloud-based computing, startups today are likely to adopt Software-as-a-Service (SaaS) for all business applications. As you select SaaS vendors, assess their security posture. Are they running in a private data center or on a third party cloud infrastructure, and if the latter, what is the security posture of that provider? Do they have multi-site backup? Are the data encrypted at rest, and can you connect through SSL? To what degree can you audit usage, and create notifications in the event of suspicious usage? Do they support their own multi-factor authentication or integrate with Google Apps or whatever you use internally for identity and access management? Do they have an API you can use to monitor usage and apply policies through a cloud security dashboard like Cloudlock?[15] Does the vendor have SOC-2 or other security certifications? Do they have a dedicated security team?

As for your own security infrastructure, it may be counter-intuitive to rely on cloud based vendors for security but in fact it is highly recommended. They will do a more expert job than you in safeguarding your data, and cloud-based vendors benefit from a broader perspective on attack patterns because they see so much data.

[15] BVP is an investor in Cloudlock.

Step 4. Your Email is the Master Key (IT)

We all have login credentials for dozens or even hundreds of applications and web sites, and we tend to think of email as just one more. But securing email is far more important than securing any other application, precisely because email has evolved into an authentication service for all others.

Because email addresses are unique, email has become the standard medium for resetting forgotten passwords, and so losing control of your email opens every door and window you have to attackers. Email is also the easiest and most common way to move files in and out of enterprises. It is therefore the key platform to secure in order to limit data leaks, repel malware, and secure your other passwords.

The first defensive measure every business needs is multi-factor authentication to access email. The cheapest, least intrusive option is to leverage text messaging to authenticate logins, with the option of bypassing the authentication step when users log in repeatedly from the same device. Based on your Business Cyber Risk Analysis, you may opt for stronger policies and factors, such as RSA tokens or smartphone certificates.

Your email system must incorporate spam and malware filters, since email is the most common entry point for malware. There is no reason not to rely on cloud-based services for this, which are already included in web-based email services like Google Apps and Microsoft Office 365. Cloud-based services also work well for startups, which have a high cost of capital, so they can pay as they grow.

To lower the chance of spoofed e-mail messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers. DKIM and DMARC are also a good way to further ensure the authenticity and security of email traffic.

Surprisingly, email is still rarely encrypted, despite the critical role it plays in business communications. Some email vendors offer encryption options but each of them works only among users of that one email platform. Email is inherently a universal medium, and you need the ability to encrypt messages and files regardless of where you send them.

One option is OpenPGP,[16] which Google and Yahoo have both committed to support.[17] However, it is still quite difficult to use, which means that many

[16] https://code.google.com/p/end-to-end/

[17] http://www.cnet.com/news/yahoo-teams-up-with-google-on-encrypted-webmail/

recipients of your messages are unlikely to comply. Zix is a much easier server side solution that deploys on top of Google Apps and enables senders to restrict forwarding and revoke messages. Virtru[18] provides that same functionality to Google Apps users but also provides client-side plug-ins that encrypt end-to-end so even Google cannot access your content.

Although this recommendation focuses on email, it's important to note that text messaging among employees for work is growing, usually without any help from their enterprises. Text messages can include attachments, and they are also subject to legal discovery and account takeover. Text messages are sent in clear text over a provider's network. Since text messages are often used to authenticate logins, your texting platform is also a vector of attack to your other accounts. If your team relies on texting, consider using a secure platform like Silent Circle, RedBooth, Wickr, TigerText or Avaamo.

[18] BVP is an investor in Virtru and I serve on their board of directors.

Step 5. Your Web Site is the Front Door (Ops)

Your web site and mobile back-ends are akin to the storefronts of your business – the points of commerce for shoppers, as well as the points of entry for prospective employees, journalists, reviewers, partners, bloggers and investors. Like a retail operation, you need to consider the possibility of attackers raiding your cash register, harassing your customers, stealing the merchandise off your shelves, or even burning down the store. For each of these threats, there are defensive measures you can take.

Your payment infrastructure is the cash register, and fortunately there are several APIs today from Braintree, Stripe, CyberSource and others that will manage payments for you in an affordable and secure way. Use one. If you try to build your own payments infrastructure, you will spend far more time than you want just trying to comply with the Payment Card Industry (PCI) Data Security Standard. These services will also evolve faster than you can to support international cards, Paypal, Bitcoin, and other payment options.

If cyber thieves steal data from your site, and you have to notify your customers that you have exposed them to identity theft, your storefront will get awfully quiet. So deploy measures to defend against directory traversal attacks, cross-site scripting, and command and SQL injection attacks, which are usually available in the cloud from your infrastructure vendor in the forms of web application firewalls (WAF). If there is encrypted traffic that your WAF cannot see, you will need a host-based application firewall.

Your mobile app is your second storefront, so secure your API as well – they are generous with data, and are easy to reverse-engineer. API requests should require security tokens with a timed expiry to protect against forgery.[19] Code your critical security checks in C++, which is harder to decompile on Android phones. Validate Apple and Google store receipts, and check that the client phones haven't been jailbroken.

For many online businesses, fraud represents a major challenge, not only because it leads to theft of goods, but because it undermines confidence in the community. For any application with a social element, you must cultivate a level of trust among the users that fraudsters will try to squander for their own purposes. Think through and investigate all the schemes you can, and then use device ID technology from companies like ThreatMetrix, Kount, iovation, Device Authority and 41st Parameter (Experian) to keep serial fraudsters outside your store.

[19] This protects against Cross-Site Request Forgery attacks, explained here: https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet

There's more than one way to "burn down the store" in cyberspace. Sophisticated attackers can exploit vulnerabilities on your site to install "cyber bombs," or infectious malware that ultimately marks your site as malware within Google search; secure coding practices and IPS will mitigate these threats.

But the easy way to disable your application, or your API, is to overwhelm it with a Distributed Denial of Service (DDoS) attack. With bot armies readily available for rent, massive DDoS attacks are easy to launch, and so the occurrence of these attacks has skyrocketed in recent years. Don't even bother buying your own Arbor box to defend yourself – Arbor can handle 20Gbps attacks even though attackers today typically launch attacks in the range of 100 to 200 Gbps. If you have a low traffic site and outages are not a major concern for you, leverage the services of your infrastructure provider. For example, Rackspace, Amazon, CloudFlare and AT&T offer some DDoS protection. But when a large attack hits you, they will simply turn off your site in order to maintain network capacity for their other customers. If you can't afford long outages, your best bet is to subscribe to an anti-DDoS service provider that can rapidly shift bandwidth to absorb large attacks, such as Prolexic (Akamai), VeriSign[20], Neustar, or Defense.net[21] (F5).

I wish we had put in better DDoS prevention. If a company hasn't thought about how they will deal with that, having to address that for the first time over a weekend is not going to be a pleasant experience. The size of site that's a target is getting smaller and smaller. DDoS solutions can have implications on your network design as well. Addressing an attack is not something you want to do on the fly. – Peter Offringa, CTO Zoosk

[20] At one time I was Chairman and CFO of VeriSign, and BVP was an investor.
[21] I was on the board of Defense.net, and BVP was an investor.

Step 6. Secure Coding (Engineering)

Application software development is the most critical business function in the early days of most startups today. Naturally, there is a rush to hit product release goals, so they want "agile development" in order to hone in quickly on a compelling user experience. Developers do not want to be distracted with security concerns.

But agile development only works when coupled with DevOps, an approach toward the rapidly iterative deployment of software that empowers programmers to embed resilience into the application, so that quality assurance, performance, and security are addressed during development rather than as "after-market accessories" installed by a separate operations team. In the now prevailing DevOps approach to application software, the operations team works closely with – maybe even inside – the dev organization, and the advantages extend well beyond security to include scalability, flexibility, performance, and quality assurance. Hopefully you have already decided to build a DevOps team; if so, it is crucial that at least one person on that team is passionate and expert about cybersecurity.

Agile or not, every naked line of code will one day need armor. There are different kinds of armor, as you will read about in this chapter and the next, and if you try to add them later, you will find yourself re-writing much of your code anyway. Furthermore, it takes time to develop secure policies and sensitivities – if you don't start early, it will be difficult to change mindsets later. And if your engineers refuse to comply with security policies now, what makes you think they will comply later? The CTO's I interviewed wish more than anything that their companies had embedded security into software development from day one.

The most important feature of secure development is written and periodic in-person training by your senior developers or outside experts (this can be done online). Your coders should know, for example, to check the size of user inputs, perform and document explicit error checking on all input, filter input streams for malicious characters or sequences, manage memory, sanitize output, initialize and clear variables, and issue all SQL commands through stored procedures or pre-compiled PREPAREDSTATEMENTs.

The second basic feature of secure development is source code analysis – the automated discovery of vulnerabilities. Fortify uncovers bugs in your un-compiled code, and Veracode does it with binaries. These are complementary tools that usually uncover different problems.

In addition, you should execute dynamic testing from AppScan or Tinfoil, which scan for vulnerabilities in your applications before you launch them – all they need is a URL to test. These are all easy tools to incorporate into your continuous integration process.

Very few coders are well versed in security, which is why you should take advantage of third party libraries that manage the intricacies of encryption and authentication. It is tempting to simply create a user table for every new application, but eventually you will have to address the issues of validating password strength, prompting password changes, hashing and salting the passwords, encrypting the user data, restoring forgotten passwords, supporting multi-factor authentication, integrating with web-based authentication like Facebook Connect or OAuth, and integrating with your or your customers' enterprise directories like Microsoft Active Directory. Take advantage of the APIs from vendors like StormPath, ForgeRock, Virgil Security and Auth0,[22] since all those companies do is worry about facilitating and securing logins. They will keep up with the latest developments – for example, migrating to SHA256 hashes now that MD5 has weakened. The costs of these services is nothing compared with the resources it will take you to reproduce their secure software and facilities.

Finally, you need to think through access controls as you build apps. It is tempting to just give every component full access to the database, but it leads to vulnerabilities. It's tempting to give admins full control of everything, but at some point it will be necessary for information to be properly compartmentalized and obfuscated from admins, and all admin activities need to be monitored and audited from Day One. Getting access right is one of the trickiest parts of architecting a scalable application, and cannot be simply bolted on in a new release. Third party libraries like ForgeRock can help developers manage access controls.

[22] BVP is an investor in Auth0.

Step 7. Control the Internal Network (IT)

Your internal network of clients and servers represents the primary target for cyber attack. If you let it grow naturally in an ad-hoc way, it will devolve into a swamp of bots and malware, and you will never have any idea who really controls your company's resources and information. From the earliest days of your startup, you need IT oversight to maintain visibility and control – this will obviously be the most expensive and difficult part of your cybersecurity plan. By the time your startup reaches a headcount of 40, you should be hiring a dedicated, full-time security engineer to oversee these and other activities.

Prevention

Control and visibility begin with an IT asset inventory system, which is much easier to deploy BEFORE you have accumulated many IT assets. It should track every device with an IP address, and the software installations on each device, as well as provide asset discovery on your network. It should also allow for wireless network access restriction using 802.1x controls. There is a wide choice of such inventory apps available, and you can even get one for free from Spiceworks.

For every computer and network device, define and document a secure configuration and be sure to deploy it to every new computing device. For example:

- Computers: Install anti-malware agents, disable Bluetooth connections, disabled file sharing, disable auto-execution of USB programs, and enable security options like automatic screen-lock, full disk encryption, host-based firewalls, port filtering, 3 month password expirations, process tracking logs and Address Space Randomization Layout.

- Network devices: Upload new firmware releases, disable old protocol support and unneeded service components, document all policies that open ports (reviewing and culling them twice a year), and require authenticated/encrypted sessions (with non-default passwords!) to manage them. Validate audit log settings and record entries in a standard format, using Network Time Protocol to synchronize the timestamps. Firewalls should deny access to known bad IP addresses and enable session tracking mechanisms to identify suspiciously long TCP connections or unauthorized use of encryption.

– Smartphones: Since it is difficult for endpoint products to filter out malware and detect unusual behavior on smartphones, equip all mobile devices with cloud-based security services such as Z-Scaler, Wandera[23], Netskope or Mojave[24].

Administrative accounts are a common vector for many types of attack. Give each administrator a separate account, auditing their use and limiting them to system administration activities (use access control lists to prevent them from accessing web or email). Administrative passwords should have at least 12 intermixed characters, numbers and special characters with no words that can be defeated by a dictionary attack, and repeatedly remind administrators to never re-use those passwords elsewhere. Administrator access, and all remote logins, should require multi-factor authentication, with lockouts for repeated failed attempts. “In this day and age, in a corporate environment, people are still picking easy passwords. This is the number-one thing that needs to be addressed in a corporate environment,” advised Karl Sigler, a Trustwave pen tester who recently cracked 560,000 just last month.[25]

Design and implement network perimeters so that all outgoing web, file transfer protocol (FTP), and secure shell traffic to the Internet must pass through at least one authenticated proxy on a DMZ network. The proxy should support logging individual TCP sessions; blocking specific URLs, domain names, and IP addresses to implement a black list; applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites; and monitoring for sensitive information (documents, payment credentials, etc.). Barracuda is an excellent proxy-based firewall for startups.

Automate the patching of your systems (including network devices), except for your production servers, which should only be patched after your staging servers show no side effects.

[23] BVP is an investor in Wandera.

[24] BVP is an investor in Mojave.

[25] http://venturebeat.com/2014/08/14/white-hat-hackers-lifted-560000-corporate-passwords-in-31-days-were-all-screwed/

Detection

Your IT manager or DevOps security expert should use a Security Incident and Event Management (SIEM) tool to regularly review DHCP server logs, DNS hostname logs (to detect command-and-control requests), and all network device logs. Document all anomalies in the logs and retain them on dedicated logging servers for a long enough period of time to trace attacks. You can get free, open source SIEMs from LOGalyze or AlienVault.

Also run weekly vulnerability and port scans from a service such as Qualys[26] or Tenable. Provision a dedicated administrative account for the scanner to access your servers – the logs should always reflect the scan activity if both are working. If the vulnerability scans point to any needed patches that haven't automatically deployed, be sure to manually patch those systems.

Monitor all penetration testing, and disable accounts between tests. Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords. Zoosk's CTO Peter Offringa told me, "I wish we had started regular pen testing much sooner."

Remediation

The best pre-remediation measure for many cyber threats is a reliable backup regimen. Be sure to store master images and backup system files over days, weeks and months for easy restoration in case hackers, malware, bad patches, or human errors corrupt your systems. Encrypt the backup files, and test the restoration process at least twice a year. And never co-locate your backup systems with production systems – Code Spaces is a startup that shutdown because a cyber attacker deleted their primary AND backup data, which were both stored in AWS.

There are many other precautions you can take, although some, like account monitoring, are less relevant to startups where insider attacks are less likely. More detailed recommendations for network security, as well as a vendor directory, can be found on the SANS Institute web site, at http://www.sans.org/critical-security-controls/controls .

[26] I served on the Board of Qualys, and BVP was at one time an investor in the company.

Step 8. Physical Security (CFO, HR)

Restricting physical access to your office is a good idea for many reasons. In addition to protecting your employees' physical safety, a secure "meatspace" mitigates the threats of computer theft, data theft, and targeted malware attacks.

For startups, here are five simple, affordable measures worth taking:

1. Lock your front door, so guests have to buzz in. This restricts access to current employees and invited guests. If you don't have a full-time receptionist manning the front door, consider installing the August smart lock for $200 so you can text entry codes to your guests, journal the entry times of your guests and employees, and easily de-provision employee access without having to change your locks every time.[27]

2. Sign guests into the office. This provides you with a record of who has entered and when. (If you have an August smart lock, there is no need for explicit sign-ins.)

3. Print distinct badges for your guests – this alerts employees – and reminds the guests themselves – of limitations as to what guests should see and hear. It also makes it easier to spot uninvited guests who may have bypassed the lock or sign-in ledger – guests should be accompanied at all times, without exception (which makes it easy to enforce without insulting your guests). Even without an office manager or receptionist, the sign-in and badging process can be managed by any one of the many tablet-based visitor management apps from Pingboard, TextUs.biz, HID, VisitorPass, ProxyClick, Analog Twelve and others.

4. Install video surveillance in entries, exits and common areas of the office. Dropcam[28] is an inexpensive and simple way to deploy highly advanced cloud-based surveillance features like motion detection, high res color, audio, and night vision. It will cost only $200 / camera plus $10 a month, and you can set up all the software and hardware in less than an hour.

5. Don't ask the janitorial crew to clean your server rooms; do it yourself.

[27] BVP is an investor in August.

[28] BVP is an investor in DropCam.

Step 9. Plan for Failure (CFO, IT)

In Step 1, I recommended compiling a Business Cyber Risk Analysis that includes a Defense Plan for preventing, detecting, and remediating cyber threats. Too often businesses deploy the first two types of measures and neglect the third, even though there is little cost in planning remediations.

Like any complex system, your cybersecurity plan will at times fail, even due to threats for which you have invested heavily in preventive defenses. So anticipate those failures and prepare for them. The alternative is to scramble after every incident, trying to think fast about how to respond, and starting from scratch each time seeking resources that have long lead times to procure. And the longer an incident goes without remediation, the more damage your startup incurs, as the attackers have more time to steal, defraud and disrupt.

For example, what happens if a DDoS attack successfully takes down your API, web site, or mobile app? Have you thought through how it will impact your operations and your customers? What can you do during such an outage to communicate with your customers and mitigate the impact on them? Do you perhaps need backup servers with different servers and IP addresses, or have a secondary DDoS protection service retained as a backup?

What about a data breach that exposes your employees or customers to identity theft? If you expect to collect any customer data, you should expect a data breach at some point in your future. These incidents are particularly challenging, and potentially fatal, so a remediation plan is crucial.

Consider the following pre-remediation measures – these are the ones you can actually take prior to any account data breach, just in case…

a) Work with your general counsel to determine your obligations under the law, industry regulations, accounting rules, customer contracts and data security certification requirements to notify law enforcement agencies, regulators, auditors, customers, and the impacted individuals in the event of a breach. Have the required forms ready at hand, filled out in advance as much as possible. CyberSponse, Syncurity and CO3 Systems are affordable services you can subscribe to that automate this notification process for you, as well as prepare you for other necessary workflows around remediating cyber crises.

b) Establish a relationship with a provider of identity theft protection services. (Don't bother with credit monitoring services – although they're cheap, your customers will figure out quickly that these services do little to actually protect them from cyber theft.) An ID theft protection contract should cost you nothing until such time as you activate the service. Lifelock[29] and Experian are the leaders in this market.

c) Draft the blog post that you will share with customers when a breach happens. Obviously you won't have all the details, but you can write enough of it that mostly you will be filling in the blanks when necessary. Start with the facts that you know, be open about what you still don't know. Explain which accounts are impacted and what data may be lost, and whether there is any evidence yet of identity theft using the stolen data. Explain what precautions can be taken (e.g. changing passwords on your site and others). Explain what you will be doing to provide them with identity theft protection. Offer up contact information in case they have questions. Give some timeline on when you expect things to return to normal, and assurances that you have outside help to repel the attack and restore secure operations.

d) Identify a forensics and remediation crisis firm to be on call, so you know help is quickly available. There are many excellent teams out there, including Mandiant (FireEye), CrowdStrike, Stroz Friedberg, Black Hill Security, Kroll, and K2 Intelligence.[30] Find one who can be on site within three hours.

At this point, your post-remediation plan is really just that – a plan. But it's crucial to write it down so everyone, including you, knows what to do…

a) As soon as you suspect a data breach, inform the CEO and General Counsel immediately, even if it is simply a suspicion that a data breach might have occurred. Document steps taken and who was informed and when.

b) Hire the forensics and remediation experts to help you understand what has happened and how to repel the attack. Internally, all hands should be on deck.

[29] I serve on the board of Lifelock, and BVP is an investor in the company.

[30] BVP is an investor in K2 Intelligence.

c) Conduct all internal communications regarding the crisis using alternative media and devices to the extent that you can. Consider that the attackers may have access to your email accounts and computer keyboard streams, and they will be watching what you do. So provision new email accounts and try to re-image your computers and smartphones among the crisis team members.

d) Ascertain what data have been compromised to the best of your ability, and which accounts have been impacted. Look for any evidence that ID thieves have already exploited the stolen data.

e) Alert whichever state, federal or industry regulators you need to, as advised by your attorney. Hopefully you are already prepared for this step in order to assure proper compliance and give you the time you need to focus on other remediation steps during the crisis.

f) With your attorney's approval, publish your blog post with the facts, and follow up immediately with an email to all your customers explaining the situation. It is tempting to suppress details of the crisis, but that would be a mistake. Data breaches happen all the time to the biggest companies and government agencies out there. No one today is judged harshly for experiencing a breach, but they *are* judged harshly for covering it up.

As you can see, the first three steps of this plan should be executed prior to any breach. The remaining steps should be put in place so that everyone knows what to do when a breach occurs. The up-front cost of the plan is minimal, but you will be glad to have it in the likely event that it is needed.

Prepare remediation plans for every significant cyber threat you face. If you would like expert assistance with this, I recommend Good Harbor Security Risk Management.

Step 10. Be Open With the Public (CEO)

> *There was a time when corporations could manage their public images through PR firms. But today, thanks to social media, there is far more transparency, so trying to cover up mistakes of any kind is a folly. Many CEOs fail to appreciate this new reality, continuing to patronize the public with a cocktail of silence and spin. Others embrace the new reality, recognizing that there is a lot of patience and forgiveness out there for people who openly and authentically own their mistakes.*

It is good business to protect IP, customer data, and other confidential business information, and a large part of cybersecurity is about securing these data. But it’s important to distinguish confidential data from simply unflattering or even embarrassing facts about management. Such facts can either fester and grow in the dark, or they can be exposed to sunlight and dry up. This is why great startup founders are usually also great bloggers. They know how to speak honestly and openly about their challenges.

An authentically honest posture is good for cybersecurity. For one thing, the open discussion of cybersecurity challenges invites helpful criticism and ideas, and it buys you good will when you do have a crisis to manage through. Also, an open, public posture dissipates any anger that your company may evoke among unhappy customers, disgruntled employees, or political hacktivists. When you or someone on your team ends up hurting a customer or employee, make it your priority to apologize and remediate, rather than obfuscate the error.

There’s simply no good business reason to unnecessarily provoke cyber attacks.

Epilogue: What Next?

If you have followed the 10 steps, you are reasonably prepared to conduct business as a startup in the wilds of cyberspace. As you grow you will encounter the need for additional investments in cybersecurity infrastructure, but you will be much better prepared for it. You will have visibility into your own network, know your own weaknesses, understand why you spend what you do, and have a team in place that culturally supports the business need for cybersecurity.

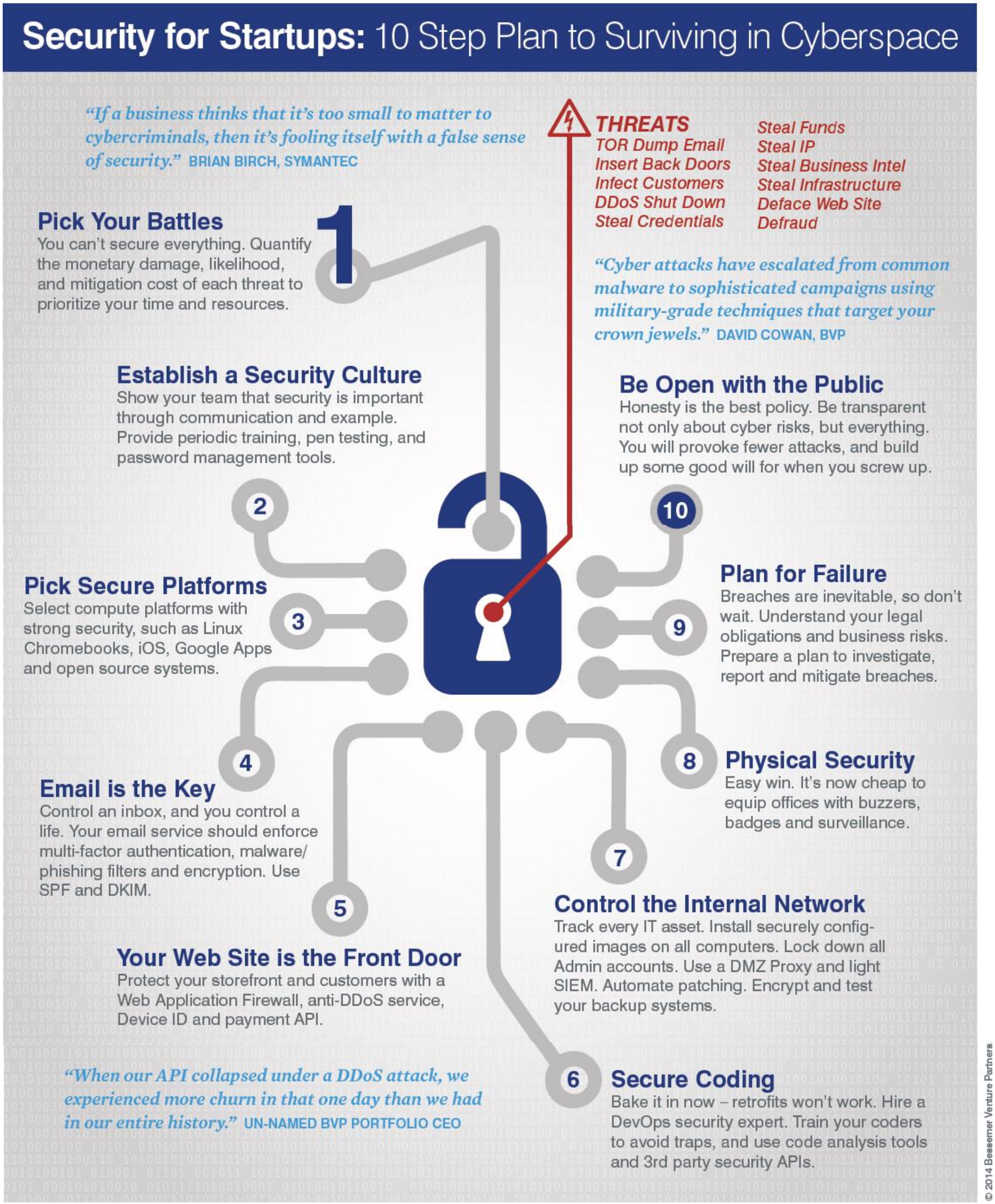
There are three additional cybersecurity milestones that startups typically encounter as they grow. The first is certification – a process led by third parties through which companies demonstrate compliance with the data security standards of SOC-2, HIPAA, PCI, etc. Certification and security are not the same thing! But if you have invested in the right security infrastructure and processes for your business, certifications will be relatively easy to get.

The second milestone will be the hiring of a Chief Information Security Officer – a truly empowered role reporting to the CEO with a budget to effect change in the company. This is usually a happy day for the CEO, who can now delegate further development of the Business Cyber Risk Analysis to a full time professional!

The third milestone is the commissioning of a Secure Operations Center. At some point, your startup will be so successful that you will have a vast network of IT assets to manage, and a budget to do so properly. That's when your CISO will convince you that equipping a team of full time analysts to process all the cybersecurity alerts is money well spent.

Unlike other technical problems, cybersecurity is one that you will never solve. But that does not mean you cannot make it a core competence of your business. To the extent that your startup depends upon online assets, your success depends upon the security of your data.

Appendix: Reference Chart



Security for Startups: 10 Step Plan to Surviving in Cyberspace

"If a business thinks that it's too small to matter to cybercriminals, then it's fooling itself with a false sense of security." BRIAN BIRCH, SYMANTEC

THREATS

TOR Dump Email	Steal Funds
Insert Back Doors	Steal IP
Infect Customers	Steal Business Intel
DDoS Shut Down	Steal Infrastructure
Steal Credentials	Deface Web Site
	Defraud

"Cyber attacks have escalated from common malware to sophisticated campaigns using military-grade techniques that target your crown jewels." DAVID COWAN, BVP

1 **Pick Your Battles**
You can't secure everything. Quantify the monetary damage, likelihood, and mitigation cost of each threat to prioritize your time and resources.

2 **Establish a Security Culture**
Show your team that security is important through communication and example. Provide periodic training, pen testing, and password management tools.

3 **Pick Secure Platforms**
Select compute platforms with strong security, such as Linux Chromebooks, iOS, Google Apps and open source systems.

4 **Email is the Key**
Control an inbox, and you control a life. Your email service should enforce multi-factor authentication, malware/phishing filters and encryption. Use SPF and DKIM.

5 **Your Web Site is the Front Door**
Protect your storefront and customers with a Web Application Firewall, anti-DDoS service, Device ID and payment API.

6 **Secure Coding**
Bake it in now – retrofits won't work. Hire a DevOps security expert. Train your coders to avoid traps, and use code analysis tools and 3rd party security APIs.

7 **Control the Internal Network**
Track every IT asset. Install securely configured images on all computers. Lock down all Admin accounts. Use a DMZ Proxy and light SIEM. Automate patching. Encrypt and test your backup systems.

8 **Physical Security**
Easy win. It's now cheap to equip offices with buzzers, badges and surveillance.

9 **Plan for Failure**
Breaches are inevitable, so don't wait. Understand your legal obligations and business risks. Prepare a plan to investigate, report and mitigate breaches.

10 **Be Open with the Public**
Honesty is the best policy. Be transparent not only about cyber risks, but everything. You will provoke fewer attacks, and build up some good will for when you screw up.

"When our API collapsed under a DDoS attack, we experienced more churn in that one day than we had in our entire history." UN-NAMED BVP PORTFOLIO CEO

Published January 2015.

About the Author

David Cowan (@davidcowan) co-founded cybersecurity companies Defense.net, Good Technology and VeriSign, and co-authored several cybersecurity patents. As a partner of Bessemer Venture Partners, he has also led the early venture capital rounds and served on the boards of Cyota, Postini, Qualys, Tripwire and over a dozen other cybersecurity startups. He is currently a director of Lifelock, Reputation, GetInsured, Rocket Lab, Smule, Zoosk, iSight and Endgame. With a track record of over 20 IPOs, Cowan currently ranks fourth on the Forbes Midas List Hall of Fame.

Cowan has degrees in computer science, mathematics and business administration from Harvard University. He sings a cappella with Voices in Harmony, and blogs about cybersecurity and startups at WhoHasTimeForThis.com.

About Bessemer Venture Partners

Security for Startups is published by the BVP-Funded Team of Bessemer Venture Partners (BVP). BVP is a global, $4 billion venture capital firm with offices in Silicon Valley, Cambridge MA, New York, Bangalore, Sao Paulo and Herzliya, Israel. For over 100 years, BVP has incubated and funded the early stages of durable businesses such as Skype, Staples, LinkedIn, Ciena, Yelp and Pinterest, and over 110 BVP startups have gone public.

Several of BVP's partners have run cybersecurity companies, and the firm has now funded over 30 cybersecurity companies. See bvp.com/cyber to learn more about our practice.