Secure From The Start:

The Complete Guide For Entrepreneurs

Supporting growth, reducing risk, and managing costs, all in one.

hackerone

It's a common misconception among entrepreneurs that security can wait. "We can get by on the credentials of our suppliers for now," the thinking goes, "and when we close our B (C) round, we'll bring in a security leader."

More and more, this thinking simply isn't cutting it.

Cybercriminals are **more active than ever**, which in turn is leading many **VCs,** and **large companies you hope to sell to or partner with** to demand a proactive, robust approach to securing your applications from the start.

The trick is to be secure cost-effectively. Until recently, arming up on security was a lot like starting a tech company before the cloud, SaaS, and open source; then, you'd need racks of expensive hardware and proprietary software just to get started.

Today, **hacker-powered security** lets you consume security services with the same elasticity as cloud and SaaS - a fluid supply of expertise that matches your changing needs - and budget.

This report surveys the security landscape that every technology entrepreneur needs to understand and describes how hacker-powered security supports the unique needs of fast-growing businesses like yours.

What Tech Founders and CxOs Need to Understand about Security

Security is a big, rapidly-changing and high stakes topic.

It's true you could dedicate yourself to doing nothing other than reading the many excellent security reports, like the **OWASP Top 10**, or the **Carnegie Mellon Software Engineering Institute** publications, or any number of **government security resources**, and still have more to learn.

But of course this isn't practical, so we've summarized eight key security areas with which every founder and small business executive should be familiar.

1. Start with Security

Every business collects sensitive data and information from customers. You need to factor security into how you handle this data.

In the **Federal Trade Commission's Start with Security Guide**, they recommend three simple ways to protect customers and your business:

1. Don't collect personal information you don't need - cybercriminals can't steal what you don't have, so regularly review the places you collect customer data and ask "do we need that?"

2. Don't keep data you don't need. Delete financial or other unneeded data once a transaction is complete.

3. Don't use personal information if it's not necessary. Don't expose customer or employee data where sample data would do. And don't allow employees or contractors to access data they don't need.

This mentality needs to be applied to all your new products, as well. Train developers in secure coding. Explain to your engineers that they need to keep security at the forefront of their development efforts, and to regularly test and verify that privacy and security features work.

PRO TIP:

GDPR has elevated data privacy to a new level. This great **GDPR checklist** for startups makes a handy reference.

2. Manage Access Control

If you're going to keep sensitive customer data, then it's your responsibility to keep it secure.

Keeping outsiders out is obviously critical, but also consider those on the inside. All data shouldn't be accessible to every employee. Ask who needs to access this data, and as you grow your team, be sure this question is part of onboarding.

FROM THE FTC'S CASE FILES:

Goal Financial failed to restrict employee access to consumer data, resulting in the unauthorized transfer of more than 7,000 files to third parties. The FTC alleged that the company simply failed to implement the proper access controls.

3. Use Smart Password and Authentication Policies

Strong authentication is an easy deterrent to would-be criminals, as is sensible password hygiene. Two-factor authentication and other strong techniques should be used if data is at risk. Follow these recommended steps:

- Create and enforce password standards. Don't allow easy-to-guess or repeated passwords.
- Store passwords securely. Never in plain text or with methods that have been shown to be insecure.
- Guard against brute force attacks. Criminals use automated methods to endlessly guess at passwords. Limiting failed access attempts is an easy way to combat these automated tools.
- Implore admins (and employees) to change default passwords. The Equifax breach involved the **discovery of "admin/admin" credentials** on web accounts, along with researchers guessing easy passwords to eventually access sensitive employee information.
- Protect against authentication bypass. Secure every door to your networks and sensitive data. That means remedying known exploits and frequently performing security tests.

FROM THE FTC'S CASE FILES:

Lookout Services, Twitter, Reed Elsevier all failed to restrict the number of unsuccessful login attempts, which placed their networks at risk.

4. Secure and Protect Data, in Storage and Transmission

There are many ways to ensure strong encryption, but even the strongest is only as good as its implementation. Take Fandango and Credit Karma, both of whom used SSL encryption in mobile apps but turned off certificate validation. This made their apps vulnerable to man-in-the-middle attacks, and the risk could have been avoided by properly configuring SSL.

5. Network Security

In 2017, researchers found that one of the more common encryption standards, WPA2, exposes data and allows it to be read or changed while being transmitted. Unfortunately, a new 2019 report reveals that its replacement, WPA3, suffers from vulnerabilities that leave users at risk of exploits similar to WPA2.

You'll likely have a mix of networking as you grow, with a small internal network connecting your computers to each other and to the Internet, and most of your applications relying on your SaaS or cloud provider for networking.

Many of the same best practices for data privacy and security also apply here, like using sound password policies and practices, being deliberate with privileged access, and applying all updates and patches.

The FTC also suggests you follow these best practices to harden your network and perimeter:

1. Segment your network. Not every computer needs to connect to every other computer on your network. Separating different systems by housing them on separate networks can help protect sensitive data.

2. Monitor activity on your network with Intrusion Detection tools.

3. Secure remote access to the network. Not everyone needs remote access, and not everyone who needs remote access needs to access everything. Limit access to only what people need to get their work done.

4. Ensure endpoint security. Your network security is only as strong as the weakest computer or smartphone at the other end. Think about every device that accesses your network when considering security.

PRO TIP:

Email remains one of the most common ways criminals steal data and gain access. CNET put out **this good piece** on how to spot a phishing email - make it, or something similar, part of your employee onboarding.

6. Partner and Provider Security

Business partnerships are essential to success as companies specialize more and more. But without keeping an eye on security, this can expose you to significant - and growing - risk. 59% of respondents in a **2017 survey** said their organization had experienced a data breach caused by one of their vendors, an increase of 7% from the previous year.

A few simple steps can mitigate this risk. Insist that appropriate security standards are part of your contracts, and build oversight into the process so you don't have to take your partner or supplier's word for it. **This blog** offers more detail and links to a third party risk checklist you can download.

7. Put Procedures in Place to Keep Your Security Current and Address Vulnerabilities that May Arise

Security is an ongoing process that requires you to keep your guard up. Apply updates for all third-party software you use as they are issued. If you develop your own software, implement a vulnerability disclosure policy so people have a direct way to let you know about bugs. If you use open source components, be sure to **track their security as well.**

When vulnerabilities come to your attention, listen carefully and then take action.

8. Secure Paper, Physical Media, and Devices

Many of these same common sense security lessons apply to paperwork and physical media, like hard drives, laptops, flash drives, and disks. Always consider the security of information that resides on these devices.

FROM THE FTC'S CASE FILES:

A Goal Financial employee sold surplus hard drives that contained the sensitive personal information of approximately 34,000 customers in clear text. The company could have prevented the risk to consumers' personal information by using available technology to wipe devices that aren't in use.

No matter how tech savvy you are, businesses of all sizes are at risk. Review the **FTC's Small Business Computer Security Basics** to protect yourself against scammers. And, check the **FTC's Business Center** for an up-to-date listing of relevant cases and other free resources.

Following this advice will establish a solid security foundation. To stay secure as the threat landscape continuously evolves, you need ongoing, proactive testing of your applications.

The remainder of this paper explores how hacker-powered security meets the unique AppSec needs of fast-growing companies like yours.

Hacker-powered Security Can Help You Expand Coverage, Reduce Risk and Save Money

Hacker-powered security lets startups address a wide spectrum of threats and do so flexibly and cost-effectively.

Hacker-powered Security Defined

Hacker-powered security is any technique that utilizes the external hacker community to find unknown security vulnerabilities and reduce cyber risk. Common examples include bug bounty programs (such as **HackerOne Bounty**), hacker-powered penetration tests (**HackerOne Challenge**), and vulnerability disclosure policies (**HackerOne Response**).

With hacker-powered security testing, companies get the skills, experience, and nonstop coverage of white-hat hackers and researchers to help identify vulnerabilities before they can be exploited by criminals. It's a fast, structured, and proven model for crowdsourcing the right expertise, applying it when and where you need it, and paying only for results.

Think of hacker-powered security as an extension of your internal engineering and QA teams, but with nearly limitless capabilities and an elastic, on-demand usage model. Three of the key advantages for high-growth companies like yours are flexibility, coverage, and savin

> "The first week we launched HackerOne (hackers) found several high priority bugs we fixed immediately. Huge value at the fraction of the costs."
>
> **AMOS ELLISTON, CHIEF TECHNOLOGY OFFICER AT FLEXPORT**

Flexibility

HackerOne has launched more hacker-powered security programs than any other vendor, and we bring this experience to every new client. One best practice is to start small and grow gradually.

Typically, the first thing to do is publish a Vulnerability Disclosure Policy so external researchers know they can submit reports safely.

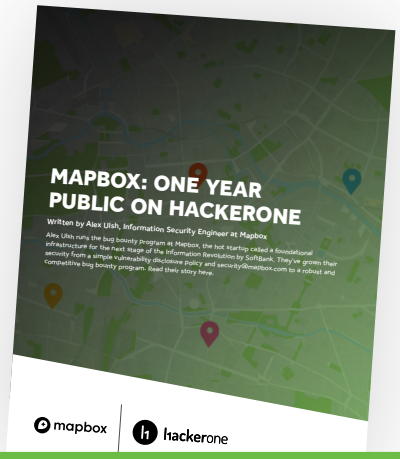
HackerOne Response is our VDP product that provides the proven process and hosted platform to efficiently collect vulnerabilities from the outside world into a single workflow so they can be remediated safely. This is where every business should start.

Once you know you can efficiently manage the vulnerabilities that come in, the next step is to move into a private HackerOne Bounty program to start paying hackers to hunt for vulnerabilities in your applications. About 80% of all HackerOne Bounty programs are private. A private program allows you to begin with a small number of assets in scope and a small number of invited hackers. This will ensure you ease into the program with a manageable number of bug reports, and therefore a manageable budget.

As your efficiency working with hackers and remediating bugs increases, and as the size and complexity of your applications grow, you can gradually increase the number of hackers and expand the scope. Down the road, it may even make sense to make your Bounty program public to ensure the most eyes possible are scouring for any potential opening.

"The first week we launched HackerOne (hackers) found several high priority bugs we fixed immediately. Huge value at the fraction of the costs."

ALEX ULSH, INFORMATION SECURITY ENGINEER AT MAPBOX



READ THE FULL STORY NOW

mapbox

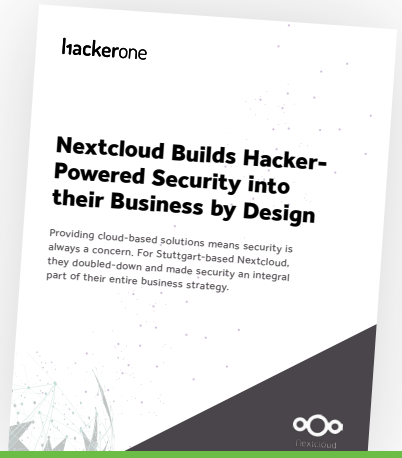
Coverage

There are over 300,000 hackers and counting in the HackerOne community, with a diversity of skills that's unmatched anywhere. In a private Bounty program, you can invite the hackers with the precise skills you need to complement your own team and ensure you are covering all your bases.

Importantly, you can also steer hackers towards the applications and vulnerability types you care about most. This is achieved through the security page and the bounty table, which you can think of as the billboard for hackers.

"We obviously can't hire enough engineers to protect against every possible vulnerability, but we can use our bug bounty program to add on-demand expertise where we need it and continuous coverage nearly everywhere else."

FRANK KARLITSCHEK NEXTCLOUD FOUNDER AND MANAGING DIRECTOR



READ THE FULL STORY NOW

Nextcloud

Savings

Because you control every aspect of your Bounty program, you always know what the maximum costs will be, and you only pay for valid bug reports. Most HackerOne customers spend a fraction of a security engineer's salary on their Bounty programs. And while it's far from a start-up, the US Secretary of Defense announced saving over $1 million dollars in their first hacker-powered program.

Compared with traditional penetration testing, HackerOne Challenge customers also discover many more vulnerabilities. In one comparison of a traditional pen test to a hacker-powered pen test, the traditional firm found three vulnerabilities in the client organization. The hacker-powered pen test found those three and 60 others.

Sumo Logic, for instance, turned to HackerOne when their traditional pen test reports kept coming back clean. They knew their software wasn't perfect, but instead, the testers were looking in the same places.

"The diverse perspectives and creativity of the participating hackers was astounding. We were so impressed, we couldn't wait to do another (HackerOne) Challenge. Some of these vulnerabilities would never have been found otherwise. The community and HackerOne's team served as a complement to and extension of our internal security team, allowing us to scale on a moment's notice, and exceed compliance standards."

GEORGE GERCHOW, CHIEF SECURITY OFFICER, SUMO LOGIC

READ THE FULL STORY NOW

sumologic

What's Next?

Adopting a comprehensive security approach can't wait, and the terrain is vast and quickly changing. Hacker-powered security can put your venture in a proactive posture from day one, keeping you a few steps ahead of the bad guys.

Whether your key driver is flexibility, maximum coverage, savings, or all of the above, HackerOne can tailor a program to meet your needs today and scale up as you grow.

Join 1,300 other organizations that trust HackerOne.

Learn more to get started >

hackerone

ABOUT US

HackerOne is the #1 **hacker-powered security platform**, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. The U.S. Department of Defense, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Microsoft, MINDEF Singapore, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, the CERT Coordination Center and over 1,300 other organizations have partnered with HackerOne to find over 120,000 vulnerabilities and award over $51M in **bug bounties**. HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, and Singapore.

Contact us to get started.