Hewlett Packard Enterprise

Business white paper

The Business of Hacking

Business innovation meets the business of hacking

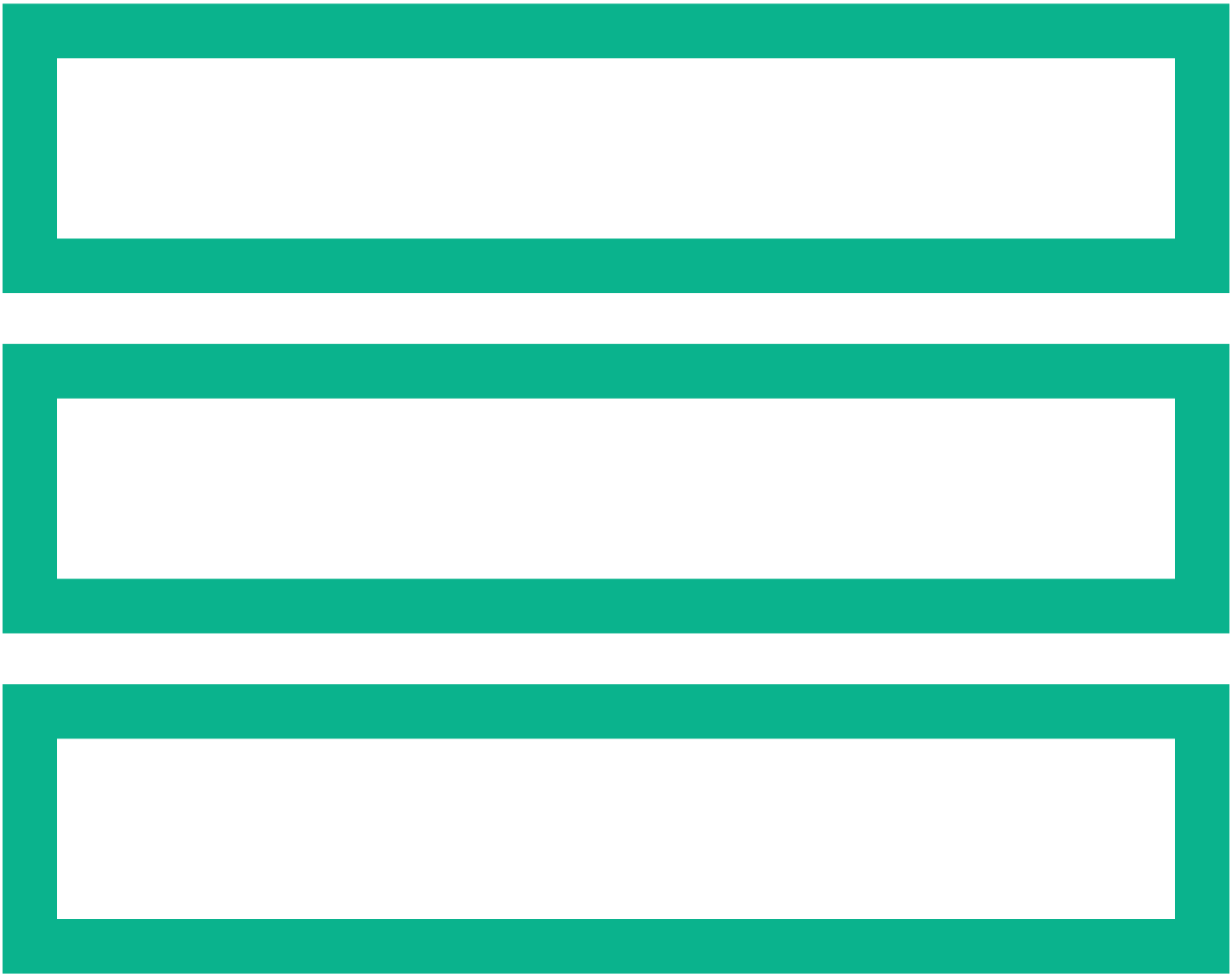


Table of contents

3 **Introduction**

4 **Business types and motivations**

8 **Guiding principles and culture**

9 **Value chain**
10 Human resource management
11 Operations
12 Technical development
13 Marketing and sales
13 Outbound logistics—distribution channels

14 **Disrupting the business of hacking**

19 **Summary**



The will to earn higher profit drives any business.

Introduction

Attackers are sophisticated. They are organized. We hear these statements a lot but what do they mean to us? What does it mean to our businesses? When we dig deeper into the "business of hacking," we see that the attackers have become almost corporate in their behavior. Their business looks a lot like ours. Cyber criminals look to maximize their profits and minimize risk. They have to compete on quality, customer service, price, reputation, and innovation. The suppliers specialize in their market offerings. They have software development lifecycles and are rapidly moving to Software as a Service (SaaS) offerings. Our businesses overlap in so many ways that we should start to look at these attackers as competitors.

This paper will explore the business of hacking: the different ways people make money by hacking, the motivations, the organization. It will break down the businesses' profitability and risk levels, and provide an overall SWOT analysis. From this, opportunities for disruption will be discussed and a competitive approach for disrupting the business of hacking will be laid out.

The information in this paper draws on data and observations from HPE Security teams, open source intelligence, and other industry reports as noted.

Whether building in enterprise security or applying security intelligence and advanced analytics, we can use our understanding of the business of hacking and the threats to our specific businesses to ensure that we are investing in the most effective security strategy.



Business types and motivations

There are a few broad categories for attacker groups: organized crime, corporate espionage, hacktivism, cyber warfare/terrorism, and those just looking for pure monetary gain. We can compare the different lines of business within the hacking industry and see how financially lucrative each business is. Cyber warfare and hacktivism are not top of our list due to the non-financial nature of the motivation and culture. This paper focuses more heavily on monetizable criminal enterprise.

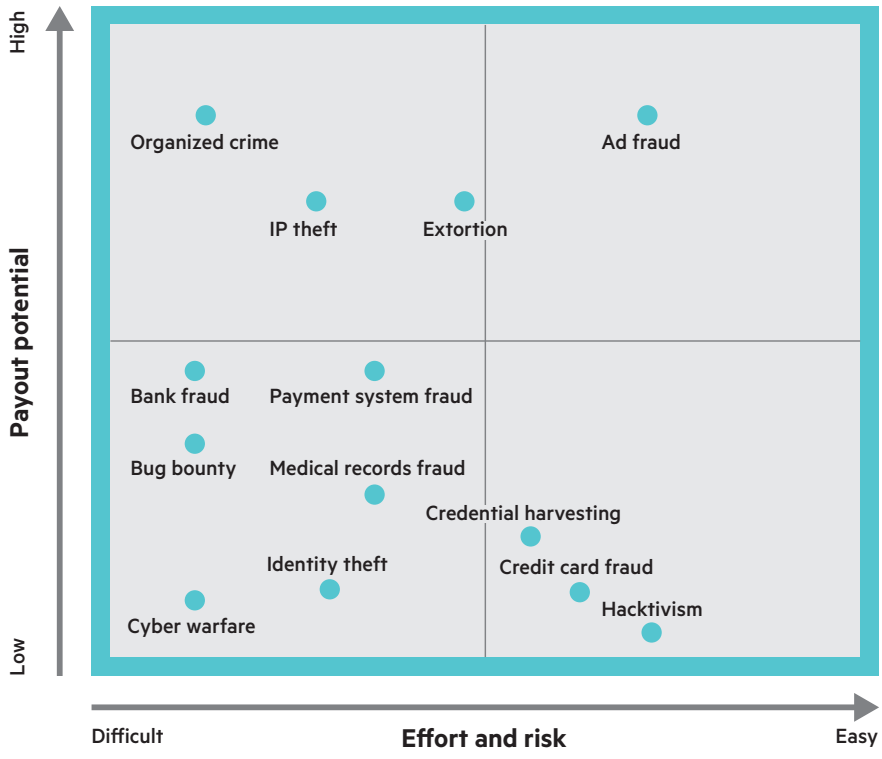


Figure 1: Attractiveness of hacking based on financial gain and effort



Attackers, as well as any other business, prefer to make the most amount of money by doing the least amount of work with minimal risk. Items in the upper right quadrant provide the highest profits with the least amount of effort and risk.

Monetary gain

Businesses designed for pure monetary gain typically involve some form of fraud. These are the big breaches reported in the news and can be very profitable:

- **Ad fraud:** Ad fraud is deliberately attempting to serve ads that have no potential to be viewed by a human user. Attackers set up a page of ads and have bots visit to generate fake traffic. Since it looks like the ads were viewed, the advertising network still gets paid.
- **Credit card fraud:** One of the largest headline-grabbing types of internet-based underground crime is credit card fraud. It involves either skimming bankcard numbers and PINs from Point-of-Sale (POS) and automated teller machine (ATM) systems, or stealing data from back-end systems. Attackers make money selling the bankcard information. They can also make money creating physical cards from the stolen information. These enable "card present" and "card not present (CNP)" fraudulent purchases. These purchases are usually made for easily sellable assets that can be used as "underground currency."
- **Payment system fraud/Bitcoin mining:** Relatively new to the industry, this type of business involves stealing money through alternative payment systems including PayPal, Apple Pay, and Bitcoin. Attackers make money here by stealing money directly or laundering the money once it has been taken.
- **Bank fraud:** This older business involves hacking into online banking systems and transferring money from one valid account to another account owned by the attacker. Money can be made here through direct funds transfer and commonly via wire transfers, or by selling network and vulnerability information about the bank system. These types of businesses often incorporate in specific regions of the world, to inhibit or elude investigation and interdiction.
- **Medical records fraud:** This usually involves stealing personal identifiable information (PII) from electronic medical records, health information exchanges, and other health systems. This data is then sold for insurance fraud or identity theft purposes. Since this type of attack is newly emerging and some international attacks have been reported, it is likely that new forms of fraud will occur over time.[1]



Track data from credit cards can be sold from $1–80 USD depending on quality, country, and CVV type.

Sample credit card values:

USA: $20/$30/$35 USD; AmEx $40 USD; Disco $30 USD

EU, ASIA 201: $65/$80/$95 USD; AmEx $80 USD; Others $80 USD

EU, ASIA 101: $85/$110/$120 USD; AmEx $80 USD; Others $80 USD



Some PII can be sold for up to 10x the value of credit card data.

[1] bits.blogs.nytimes.com/2014/08/18/hack-of-community-health-systems-affects-4-5-million-patients/?_r=1





Everyday retailers put their Point-of-Sale (POS) systems online with the default password. Attackers only have to scan for Remote Desktop Protocol (RDP) that accept username: pos and password: pos to find these vulnerable systems.



One ransomeware technology, CryptoWall, has been tied to at least $325 million USD in criminal proceeds.

- **Identity theft:** This well-known business involves stealing information about individual's identities. Attackers make money by selling this information, including addresses, social security numbers, and credit information. This stolen information can be used to open lines of credit or to create other identities for use in other businesses listed above or simply as currency for the underground marketplace.
- **Credential harvesting:** This business involves stealing user names and passwords, often via phishing emails containing links that serve a fake but seemingly legitimate webpage and capture user credentials for banking sites, etc. This information can then be sold to those involved in the businesses listed above. More often, these credentials are stolen in database thefts and then the dumps are sold in the underground.
- **Bug bounty:** Identifying application vulnerabilities has become a lucrative business with its own marketplace and players. Vendor and third-party programs (the ZDI, Bugcrowd, Microsoft®, United Airlines, etc.) operate in the white market to remediate vulnerabilities before they are exploited in the wild. Gray and black markets purchase vulnerabilities and full exploits for private use, often weaponization (black) or to spy on private citizens suspected of crimes (gray).[2]
- **Extortion:** Extortion often targets higher-level employees or systems and datastores. Ransomware, installed on a system, prevents users from accessing their systems by either locking the computer screen or encrypting files with a password. The attacker demands a ransom in order to release the files. The ransom values may vary, ranging from $500 to $50,000 USD or even higher.
- **IP theft:** This business involves stealing intellectual property from a target. Such activity has been seen in the electronics industry (cell phones, tablets, etc.), as well as in the defense industry (war planes, weapons, etc.). It has even been seen in the entertainment industry (movies, software, etc.). Attackers make money by either being "employed" to infiltrate the organization in order to obtain access to the targeted IP and sell it to the target's competitors.

[2] **HPE 2016 Cyber Risk Report**, see pages 8–11

Organized crime

Organized crime businesses are some of the least publicized. Traditional organized crime has moved online for the purposes of money laundering, weapons distribution, drug trafficking, assassination services, and human trafficking. One of the key characteristics of online organized crime is that they often are the middlemen even to the other businesses in this list.

Hacktivism

Hacktivism involves loosely organized groups who hack for political or ideological purposes. Much of the hacktivists' business targets organizations they feel have done wrong. They are online activists who perform online protest. There are three main types of hacktivism:

- **Nuisance:** These types of activities include Web defacement and Twitter handle takeovers.
- **Disruptive:** Botnets, spammers, and DDoS are more focused on disrupting a target organization's function.
- **Destructive:** Destructive hacktivism actually destroys data or renders systems of a target organization useless.

A DDoS attack service can be rented for as little as $38 USD a month and can cost an organization an average of $40,000 USD an hour.[3]

Cyber warfare, nation-states, and terrorism

This category of business combines all of the businesses described in the preceding sections. It is an attack on a country's electronic systems, designed to cause harm or steal information. This business will not be addressed in depth in this paper.



Figure 2: Attacker personas and motivations

[3] cmswire.com/information-management/you-can-bring-down-a-website-for-38/

Guiding principles and culture

Just as with traditional enterprises, those operating in the underground market are driven by supply and demand. The more obscure a tool or information is, the more it is worth. Conversely, when the market is flooded with goods (i.e., credit cards) then the price per unit goes down.



Some cybercrime "businesses" have been found to operate on a 9 a.m. to 4 p.m. schedule, Monday through Friday with Monday mornings being the busiest time of the week, presumably to catch up from the weekend.[4]

These businesses do not operate in a hierarchy like a traditional enterprise but function more like a market-driven fair economy of buyers and sellers, each of which works as an independent contractor providing value to the community. These contractors can choose their working hours and often work a separate job to supplement their activities.

The underground cybercrime community is built on anonymity, and this anonymity can actually provide a radically free market system. The actors are only known by their handles and their true identities remain hidden. This breeds a strong paranoia throughout the business. Trust and a good reputation are key to the industry. If you are not trusted, it is very difficult to make money in the system. Trust is built by demonstrating your hacking skills, having other members of the community vouch for you, and providing valuable goods to the community. Groups often form around a shared common language (Russian, Chinese, etc.) or through gaming connections.

Hacking marketplaces have operating guidelines and forum rules. White hats abide by a hackers code of ethics. However, the criminal has always operated outside of ethical norms.

Steven Levy's Hacker Ethic:[5]

1	Access to computers—and anything that might teach you something about the way the world works—should be unlimited and total. Always yield to the Hands-on Imperative!
2	All information should be free.
3	Mistrust authority—promote decentralization.
4	Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
5	You can create art and beauty on a computer.
6	Computers can change your life for the better.

[4] **securityaffairs.co/wordpress/38086/cyber-crime/dyre-financial-trojan.html**

[5] Hackers—Heroes of the Computer Revolution, 1984, Steven Levy



Value chain

A value chain is a set of activities performed in order to deliver a valuable product or service to the market. These activities are carried out by subsystems that take an input, process it in some way to enhance value, and provide an output. All these activities together give the output more added value than the sum values of the individual activities. The effectiveness of the value chain determines the cost of the output and affects profits.

A virtual value chain describes a value chain in the cyber-marketplace.



The series of activities in the value chain of the business of hacking are not under an organizational umbrella like a corporate enterprise. However, they are all pieces that contribute to the end product. This is a deeper look into the primary and support activities involved in "the business." Some black hats carry out multiple activities while others are highly specialized, which may lower their risk of being digitally identifiable (lessen your footprint). Specializing in a small number of activities lowers the hacker's footprint but can make them rise above the crowd and increase the risk of catching the attention of law enforcement officers (LEOs).



- **"Spiders" are black hats for hire**
- **"Masterminds" are organizers of a hacking group for a target output**
- **"Mules" are workers for the group mastermind. These folks may not even know they are participating in criminal activities, but just want to "work from home, for $3000 USD a month."**

Human resource management

Job functions

The businesses are profitable as a whole, but each job in the business can be profitable on its own. Most jobs are on a contract basis, with some attackers performing multiple jobs. All roles within the value chain add value to the final product. Some add more value than others, and demand higher compensation. Not all jobs require IT skills; some have a very low barrier to entry. The following are examples of available jobs in the hacking business:

- Tool development
- Guarantor services/background checks
- Escrow services
- Recruiting
- Cyber laundering
- Sales and marketing
- Legal

Education and skills

Very little education and skills are required to get started in the hacking business. Some roles do not require any special computer skills or networking knowledge—just business acumen. Other jobs require various skills such as programming languages, networking, verbal language (Russian, Chinese, etc.), and social engineering. These skills can be gained through online forums, in Internet relay chat (IRC) rooms, or even via YouTube videos. Learning on-the-job is the tactic employed by most attackers along with finding a mentor to guide new recruits through their entry into the business.

Recruiting and vetting

Trust is the most important piece of the business of hacking. Attackers will use online forums they trust to buy services or tools from others in the business. There are different levels of forums with the more reliable ones being exclusive to well-vetted users and often require a fee to join. Vetting services for participants are offered by guarantors, where a user's background, contributions, and trustworthiness are evaluated and guaranteed. Good guarantors can quickly identify bad apples. Cheats and swindlers are rampant at the lower, less-sophisticated levels of the business. Some forums also include functionality that allows users to rate other users—much like the rating system for sellers on eBay.

Some posts recruit for custom services or for tools such as malware or zero-day vulnerabilities. These can also be validated by a guarantor before payment is made to the seller.



Figure 3: Actual post from online forum

Operations

The goal of any operations business is to reduce costs, increase profits, and accelerate gains. This is also true of the business of hacking.

Location

One consideration for business operations is the region in which a hacking business operates. Hacking takes place online in cyberspace, but the physical location of the criminal actor is important. More lenient cybercrime laws or the lack of enforcement of those laws makes some countries ideal locations for an underground operation. Additionally, local social and cultural patterns have a great influence on these threat actors. On the flip side, some regions produce higher profits, rendering them better targets.

Some laws make it harder for white hats, turning much of their work "illegal" while trying to protect global citizens from terrorists. The unintended consequence is that black hats flourish as they do not care about boundaries or laws.[7]

The Budapest Convention on Cybercrime in 2001 resulted in the first international treaty on crimes committed via the Internet and other computer networks. Some nations, India for example, have resisted signing the treaty but have enacted laws that follow what is outlined in the treaty.

Support

Support also falls under operations. Closed-source hacking tools often come with a warranty and support plan that can include bug fixes and upgrades for a year or other specified timeframe. Open source tools require community involvement for support and upgrades. The upkeep and support of the community forums falls within business operations.

Disaster recovery

Disaster recovery (DR) and resiliency is another aspect of business operations. While there are no formal DR plans within the hacking community, there are features of the industry that allow it to bounce back from takedown by police or fellow attackers. In true Darwinian fashion, early spambot takedowns taught the underground economy the value of DR. The open source principles of the community largely enable this DR capability. When one actor is taken down, another pops up swiftly in its place, similar to a hydra, utilizing the same code.

The Silk Road marketplace was taken down by authorities in November of 2013 and Silk Road 2.0 was up and running within weeks. Additionally, Agora marketplace was brought up in 2013 and had already surpassed Silk Road 2.0 in popularity by the time Operation Onymous took down Silk Road 2.0 and other competing contraband sites.[6]

Cash flow and cyber laundering

Cash flow systems allow attackers to transfer money for services and products outside of a normal (traceable) online business. Cyber money laundering is a process to make "dirty money" "clean" by transferring it through systems until the source can no longer be identified. One way to do this is by first converting e-currency to bitcoins, then to localbitcoins.com, then to blockchain wallet, and on to btc-e.com. A hacker will create a few fake online businesses that only accept PayPal. They will then buy products from them (like servers), create fake orders, and then pull the money out of PayPal. Another method is to sell your bitcoins at localbitcoins.com and transfer the funds directly into your PayPal account. Then go to payoneer.com and order a credit card that links to your PayPal account. They can then withdraw money from any ATM. Leveraging a site like localbitcoins.com methods is a way to lose law enforcement that may be monitoring this activity.

[6] en.wikipedia.org/wiki/Silk_Road_(marketplace)

[7] **HPE 2016 Cyber Risk Report**, see pages 11–12



Attackers can use the "pick up in store" option on online stores to avoid any tracking via the shipping address. Most stores require an ID for in-store pickups but some only require the receipt. Alternatively, many items can be shipped to drops and mules can re-ship them on to other locations.



"Script-kiddies" are unsophisticated attackers that execute scripts written by others. The actors are typically hacktivists or unskilled beginners.



A "bot herder" is someone who controls a number of machines (botnet) and rents the botnet out to buyers at an hourly rate.

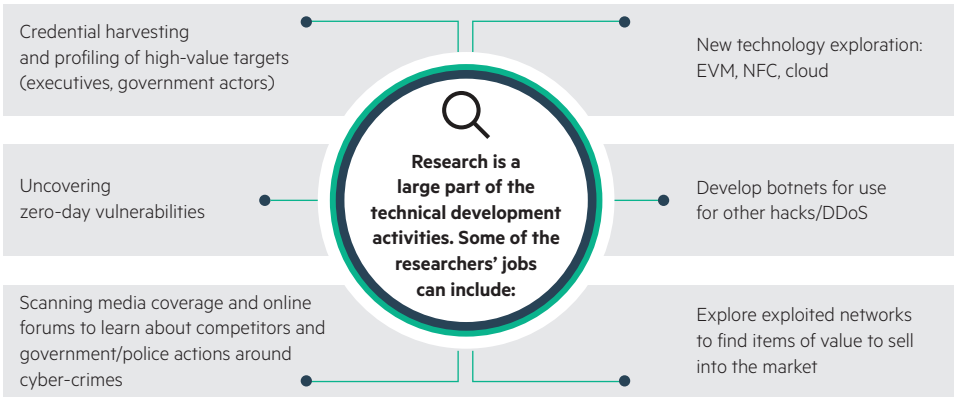
It is very common for criminal enterprises to have a legitimate "front business" in a completely different industry as a vehicle to launder profits from "overseas" operations. There is a complete legal field that establishes and then closes down front companies in various countries around the world. Often there are layers upon layers of fake businesses in multiple countries making it very difficult for investigators to determine what is real and what is not.

Escrow services

Escrow services are often offered as an intermediary to two parties involved in a transaction. If one hacker is buying an exploit from another then the funds for the exploit will go to an escrow service until the validity of the exploit can be verified. This business requires very little knowledge of computers and IT systems. The level of trust required for an escrow service is very high, and they take some time to become well established. The early users are very likely to be personally known to the escrow founder.

Technical development

Technical development is what most people think of when they think of attackers. This aspect of hacking requires computer-savvy actors performing development activities that include research to find zero-day vulnerabilities, development of exploits for these vulnerabilities, and tools to automate the different pieces of a hack (bot-nets, data exfiltration, etc.). The actors must be skilled in networks or applications, or both. Larger groups may have the expertise in-house to build tools, but smaller groups may have to outsource tool development. Expertise of the developers can range from script-kiddies to professional developers, basic system administrator skills to network architects. This activity in the value chain also includes quality assurance (QA) roles. Tools or exploits created can be subjected to QA and validation by a third party. This will increase the value of the end product.





Marketing and sales
The entire cyber market relies on reputation and credibility to make sales. Attackers must work continuously to build and maintain their status and trust in the marketplace. They also must constantly evaluate other actors they do business with. One false move or sub-par offering in the market can ruin a reputation.

Beyond brand and reputation management, attackers must also perform basic product marketing tasks including competitive analysis, pricing, and differentiation messaging. Competitive analysis involves knowing what competitors are offering to the market and at what price. It also includes evaluating the tools used to uncover any tracking features or exploit kits implanted in the tools by competitors to potentially harm their business.

A full market evaluation is used to determine pricing for goods and services. Because the market is based on supply and demand, if the market is flooded with credit card numbers, the price per number will go down. Typically newer market opportunities (e.g., mobile device and mobile payment systems) command a higher price. This is facilitated by the use of auction-style technologies to calibrate the price of a stolen asset as it declines after the breach has been detected and reported on.



Attackers can buy banner ads on underground sites to promote their products and services. They also steal customer databases from their competitors to market to them.

Tools can be priced on a per-use basis or bundled with a year of product support. Marketing tactics for lead generation for tools also include trial versions, freemium pricing on limited-functionality products and full-featured versions for a fee. The market is also moving towards “as-a-Service” tools where you can rent a tool for a defined timeframe or a specific number of uses.

Differentiation is used by attackers to drive demand for their products. Validation of the effectiveness of a tool, reputation for previous deals or quality of tools, innovation, and ease-of-use are all competitive differentiators.

Outbound logistics—distribution channels
Outbound logistics are how a product is delivered to the buyer. Attackers will use sales boards in IRC and online forums to sell their goods and arrange for delivery of the product. The actors’ real identities remain hidden, but they have virtual personas enabling deals in trusted marketplaces. More trusted marketplaces usually require a higher level of vetting for participants, and products demand higher prices. Plus, buyers and sellers often have to pay to join these marketplaces.

Disrupting the business of hacking

By understanding the business aspects and drivers of hacking, we can begin to disrupt the players and the marketplace. The goal is to make it more expensive for these businesses to operate and/or increase the risk beyond acceptable levels for the attackers. Typically, enterprises have achieved this by introducing new security technologies into their environment.[8] These products do not stop attacks altogether, but they do slow attacks down and increase the cost of carrying out an attack, thereby reducing the scope for attack.

SWOT analysis

A Strengths, weaknesses, opportunities, and threats (SWOT) analysis of the business of hacking uncovers strengths that can be attacked and weaknesses that can be exploited.

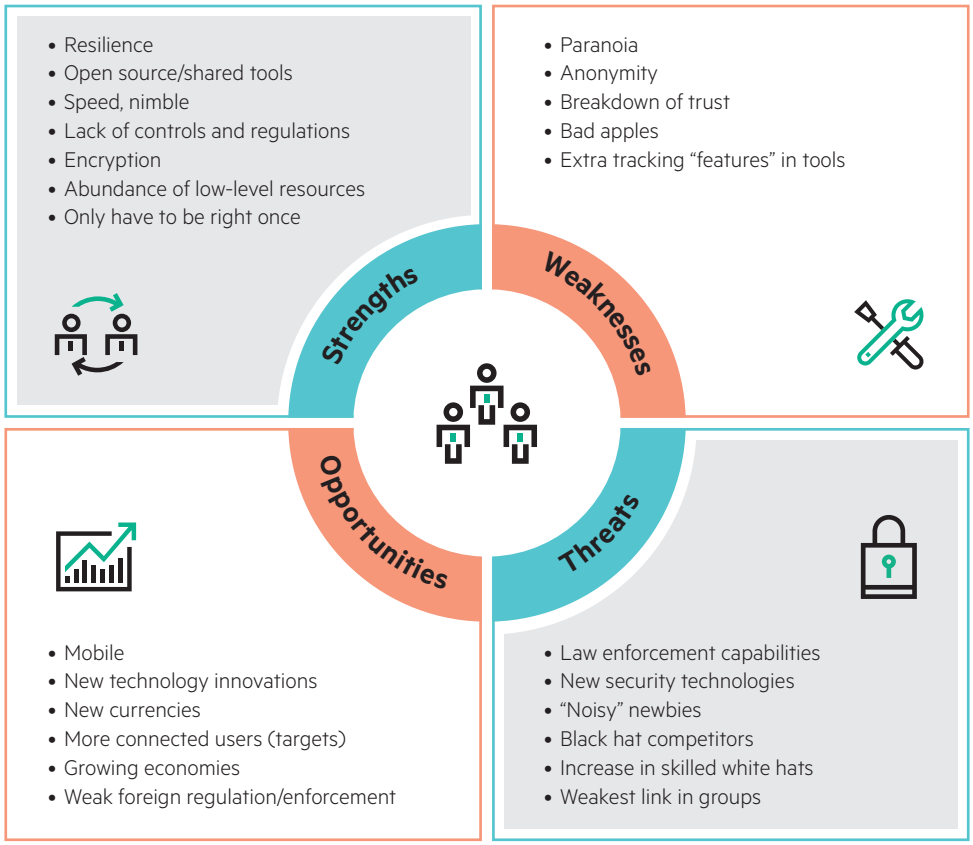


Figure 4: SWOT analysis of the business of hacking

[8] Learn more about vulnerability-specific mitigations:
HPE 2016 Cyber Risk Report, see pages 26–30



Strengths

One of the strengths of the business of hacking is that it is widely an open source community. Tools are shared, allowing for speed in gaining access to victims and in developing new exploits. It also results in a highly resilient marketplace. If authorities shut down an underground site, another one will take its place. This speed is often something our organizations cannot match. Legitimate enterprises must also abide with regulations while attackers do not. Moreover, while most countries now have cyber security laws, many of them lack proper enforcement. For these reasons, hacking businesses benefit from a large talent pool and enjoy an even larger target pool.

Weaknesses

Hacking businesses are full of weaknesses such as, a natural lack of trust and paranoia fostered by the code of anonymity amongst attackers. No one knows who anyone else is and no one truly trusts anyone else. This paranoia is the largest opportunity for offensive attacks from those looking to disrupt the business of hacking. Seeding mistrust could disrupt sales and operations. Attackers are human, making the same mistakes other organizations do. They use default passwords, are susceptible to social engineering, and install tools with hidden malware. Their business is built on reputation. Tarnish that handle's reputation and they must start over, building a new persona, costing them valuable time, effort, and money for guarantor fees, higher-level forums access, etc.



Opportunities
75% of mobile applications scanned were found to have at least one high- or critical-severity vulnerability.[9]

Opportunities

The opportunities for hacking businesses are very similar to the opportunities for legitimate organizations. The difference is that legitimate businesses are moving to mobile technologies, SaaS, and growing economies to grow our businesses. Attackers view these emerging technologies as opportunities for weaknesses in our organizations that they can exploit. Developing countries are adopting new technologies to pay bills and access the Internet. Unfortunately, these new technologies and developing infrastructures do not always employ the most advanced security making them an easy target for attackers.

Threats

The greatest threat to hacking businesses is new security technologies. These technologies such as DNS malware analytics slow attackers and increase their risk of getting caught, resulting in lower profits for them. They must also constantly watch their backs for competitors and noisy newbies whose actions can trigger security alerts and ruin their operation.

[9] **HPE 2016 Cyber Risk Report**, see page 56

Maturity curve

Each type of hacking business follows a typical maturity curve. There is an emerging phase where the cost of doing business is high, then a growth phase where automated tools flourish and profits increase. The mature phase follows where innovation slows, profits are steady, and typically, the market begins to be flooded. The final phase is a declining phase. This is caused by a saturated market or by new security technologies that make the hacking business no longer viable.

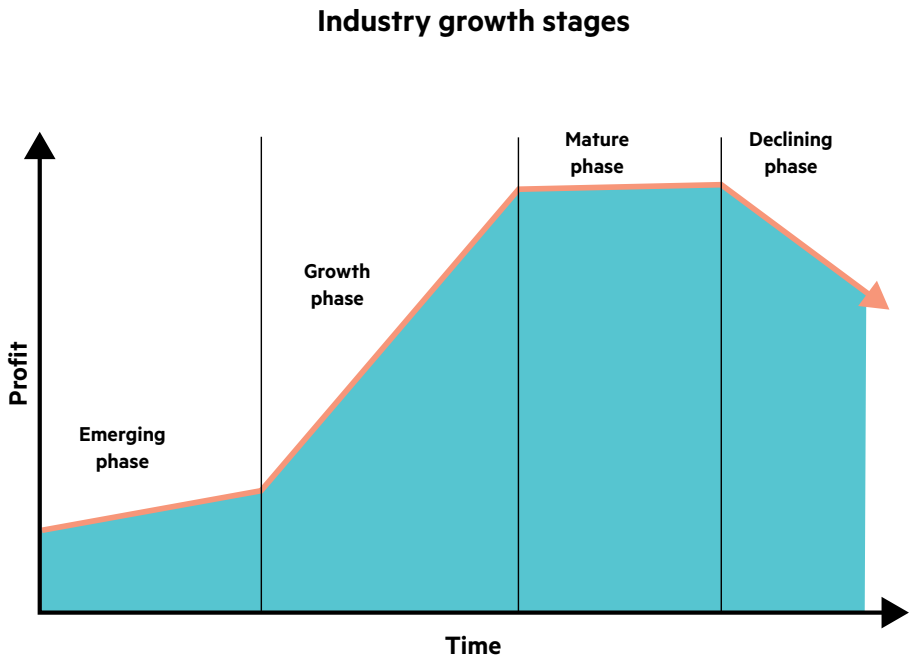


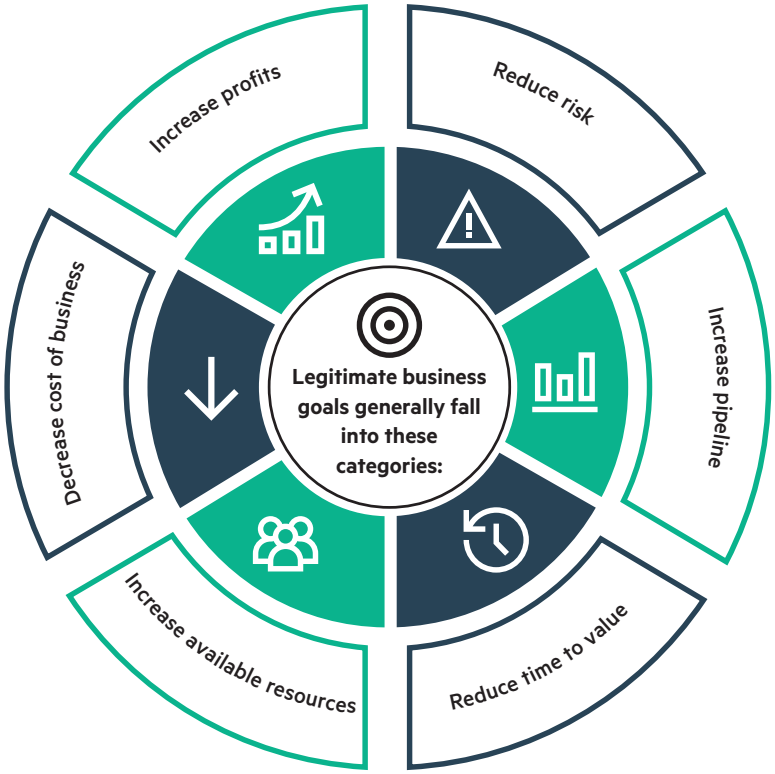
Figure 5: Industry maturity curve

The progression of credit card fraud provides a good example of this maturity curve. While there is still big money to be made in credit card fraud, the market is flooded and the business is in the declining phase. The introduction of EMV chip and pin cards in the United States will make it harder for attackers to make money on "card-present" transaction fraud. Even slowing them down a little will negatively affect their profits and we should do it more often. The maturity curve restarts when new technologies are introduced, such as mobile payments. This full curve can mature much faster in cyber businesses than in traditional business.

The maturity curve also lags in different regions of the world. Africa and South America are rapidly developing technology capabilities but are often behind in adopting the associated security controls. Attackers see this as a large opportunity and are exploiting it accordingly.

Ad fraud is currently in the growth phase. Profits are soaring for attackers. Corporations must begin to think, "Does this affect my business?" If it does, what can you do to disrupt it? There is no IDS signature for ad fraud or a rule you can put into a firewall to block it. Maybe the solution is to not pay for online advertisements through advertising networks. Or, perhaps the solution lies in holding your ad vendor accountable for fraudulent clicks. This is a non-technical solution to the problem, which will reduce wasted spend from your company and also decrease profits for the attackers.

Business goals



These are the same business goals of the hacking businesses. By knowing our competitors' business goals, strengths, and weaknesses we can arrive at ways to reduce their competitive advantage. If attackers want to increase their profits, it is our job as their competitor to reduce their profits. If they seek to reduce their risk, then we should attempt to increase their risk, and so on.

Here are some examples of disruptive techniques; some very basic, and some far-fetched. Their purpose is to open up the mindset of how we can disrupt the business of hacking and make our businesses less of a target.

Reduce their profits

A majority of attackers are in it for the money. As an enterprise, you can take steps to reduce the attacker's ability to profit from attacking you. If organizations encrypt their data wherever it lies, at-rest, in-motion or in use, with products such as **HPE Data Security** that data will be useless to attackers, thus restricting their ability to sell and reducing their profits. Additionally, storage is cheap. If an organization began to bulk-store fake data, then attackers who steal this data will experience quality issues, reducing its value and forcing the attacker to spend extra time validating data before selling it, which will increase the cost of their doing business.

Increase their risk

With more regulations and harsher punishments being established in many countries, the risk of getting caught hacking is increasing in those areas. The problem is one of enforcement. UN regulations have been adopted with varying degrees of enforcement from country to country. This is driving attackers to operate in these more lenient countries to reduce their risk. In the countries with strict enforcement, the ever-increasing police sophistication in the areas of cyber-security is effectively increasing the risk for attackers in those locales.



Many attacks occur through devices that were left with default usernames and passwords. What if every device manufacturer required authenticated access to their devices and refused to allow default passwords?

Reduce their target pool

The number of threat targets for attacking is huge and expanding rapidly with mobile devices and mobile payments. There are some simple data security tactics that can be employed to drastically reduce this vulnerable target pool. Encrypting data on mobile devices and enforcing password protection is a start. Additionally, application developers can use application security tools such as **HPE Security Fortify** to detect vulnerabilities in their applications before deploying them into production. Attackers prefer easy targets, so deploying any technologies to harden your assets will have dramatic results.

Increase time to value

Time is money. Attackers work to find vulnerabilities and exploit them as quickly as possible. They will then explore a network looking for items of value, exfiltrate, and sell them to make a profit. **DNS Malware identification** can be used to identify malware infected systems and remove them from the network before they are used as jump points into your network. This increases the time it takes for an attacker to explore your network and find valuable data.

Reduce their talent pool

As hacking is mostly anonymous, attackers use “nicks” or online personas to carry out their work. These personas are tied to reputations for quality, timeliness, and other attributes we value in our businesses. If a nick is burned or rendered useless it can take a significant amount of time to build up a new nick with a strong reputation. Squashing reputations is one way to reduce the number of viable attackers. No one wants to do business in the underground with someone linked to an FBI investigation.

Increase the cost of doing business

To truly disrupt the business of hacking is to increase the cost of the attacker's business, erode their profits, and increase the time it takes to successfully execute an attack and sale. Deception grids are gaining popularity amongst enterprises to not only disrupt the adversaries, but also to learn their techniques. Think of it as competitive analysis. Organizations set up realistic duplications of their networks to trap adversaries. The adversaries believe they are in the real network and continue to move laterally in this deceptive network. Enterprises can then learn more about the intended target (data, infrastructure, credentials, etc.) as well as observe the attacker's techniques. This allows organizations to take proper precautions in the real network to protect their true assets. **Deception grids** are complex but may represent the future of getting ahead of the attackers and disrupting them.

Summary

The business of hacking is a business just like ours. If we think of it like a business, like a competitor, then we can prioritize the most effective efforts to disrupt it.

All enterprise security technologies are intended to slow attackers in some way, with varying degrees of effectiveness. Some are effective at deterring opportunistic attackers (patching) but are ineffective at targeted attackers. Others are successful at reducing attacks of one type (EMV chip and pin credit cards), but lead attackers to move to alternate attack vectors (mobile payments). It is our duty as a legitimate enterprise to introduce these technologies to disrupt the business of hacking on a continuous basis. It is critical that an enterprise determine which technologies will be most effective at disrupting the adversaries targeting their unique business.

Learn more at
hpe.com/software/businessofhacking



Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

© Copyright 2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

4AA6-4760ENW, May 2016