unbank
ventures

Cyber Security

Develop Your Fintech Strategy

2018

Unbank.Ventures

Unbank.Ventures is an education company focused on incubation and accelerator services in the financial industry. We are building a global platform to provide education, advisory and investor connections to startups, financial institutions & service providers.

Our flagship programs are:

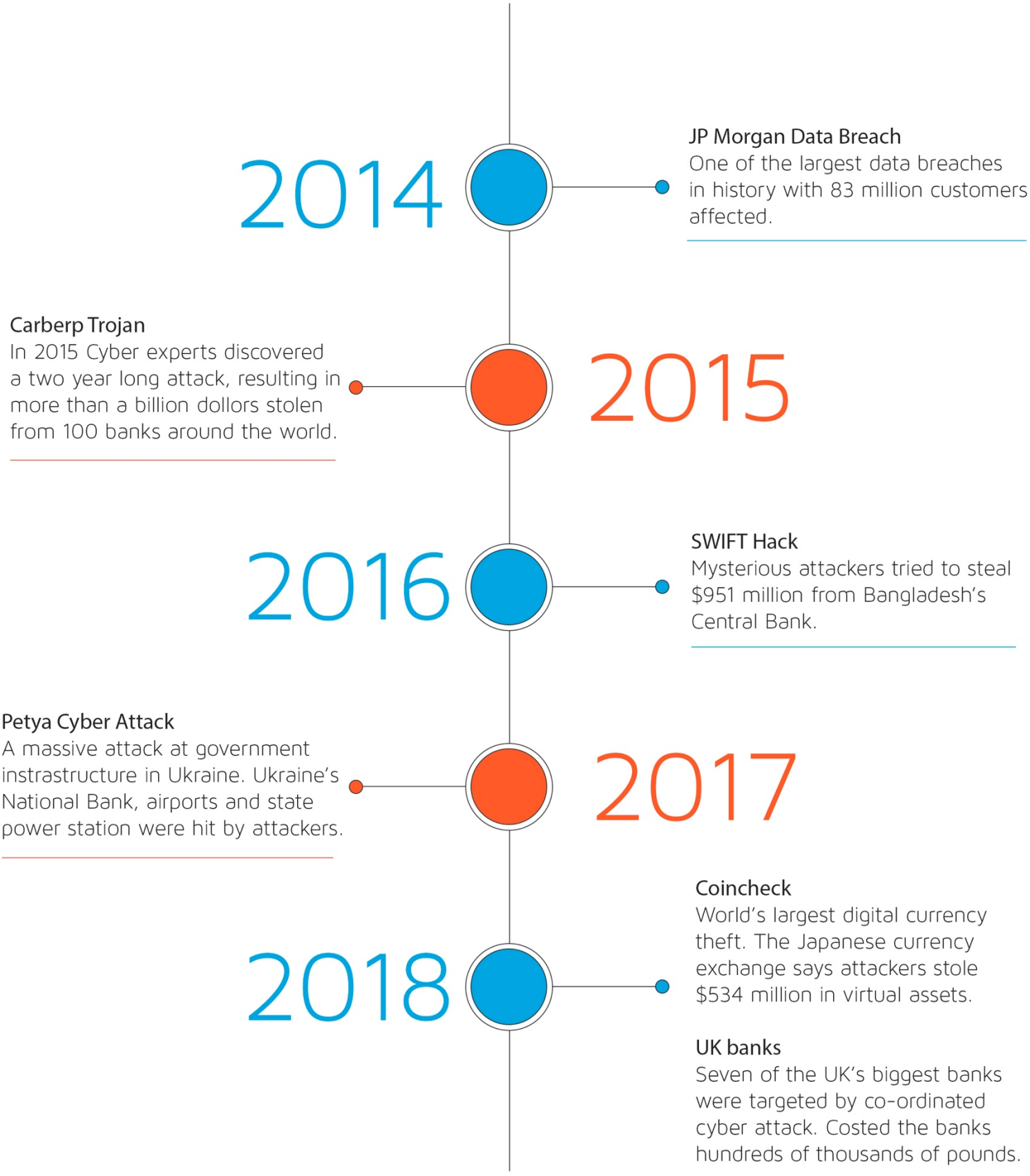
Unbank.Incubate

Unbank.Accelerator

Unchain.Ventures

Part 5

What is the current state of cyber security in the financial industry?


2014
JP Morgan Data Breach
One of the largest data breaches in history with 83 million customers affected.
Carberp Trojan
In 2015 Cyber experts discovered a two year long attack, resulting in more than a billion dollors stolen from 100 banks around the world.
2015
2016
SWIFT Hack
Mysterious attackers tried to steal $951 million from Bangladesh's Central Bank.
Petya Cyber Attack
A massive attack at government instrastructure in Ukraine. Ukraine's National Bank, airports and state power station were hit by attackers.
2017
2018
Coincheck
World's largest digital currency theft. The Japanese currency exchange says attackers stole $534 million in virtual assets.
UK banks
Seven of the UK's biggest banks were targeted by co-ordinated cyber attack. Costed the banks hundreds of thousands of pounds.

1 Background and Motivation

Unbank.Ventures provides this paper, a guide into the world of Fintech. As an education company in the financial industry, we work with Fintech startups and financial institutions all over the world and experience the huge potential that the intersection between technology and financial services creates.

We believe new technologies can give your customers increased value, through simplifications and smarter solutions. In addition, technological innovations can reduce costs. Better services at lower costs will attract new customers and help your company grow.

In this paper we will focus on Cyber Security in the financial industry. As the timeline on the previous page shows, there has been some major data breaches and cyber attacks in the industry the last few years. Millions of people have been affected and enormous amounts of money has been stolen. Even though most attacks are financial motivated, some are categorized as cyberterrorism, undertaken in order to create chaos and fear. The series of powerful attacks on Ukraine's infrastructure in 2017 is an example of the latter. Cyber attacks with substantial outcome are attracting media's attention, but most attacks have less public interest and are absent in traditional media. That doesn't mean they do no harm to businesses. They still pose a significant risk and innovative challenge for businesses.

As we have pointed out in the previous parts of our series ***Develop Your Fintech Strategy***, Fintech is in great growth. New technologies are being adopted by financial institutions and processes and systems become more accurate and efficient. There are a bunch of positive aspects with technology adoption, but everything has its drawbacks and technology is no exception. Implementation of digital solutions opens up for new possible cyber threats and give hackers more ways to perform a data breach.

Financial institutions are attractive targets for cyber attack. Hence, Cyber Security should be kept in mind when you establish your Fintech strategy.

This is the fifth publication in our Fintech series ***Develop Your Fintech Strategy.*** Last time, we focused on regulatory technologies (RegTech) and discussed how financial institutions can benefit from it.
For part 4, click here.

unbank ventures

Part 5

Why should financial institutions increase their focus on Cyber Security?

What are today's security trends in terms of Cyber?

What are the most serious cyber threats for financial institutions?

2 What Is Cyber Security?

Cyber Security is all about keeping your data, software and hardware safe from theft or damage. A data breach can result in loss of reputation, assets, and information, which can have huge negative impact on your business. Hence, protection of vital information about customers, employees, operations, products, and systems is highly important in today's competitive world. The field of cyber security aims to provide reasonable assurance when facing malicious actors.

In addition to security in the digital space, cyber security also include security in terms of physical access to hardware systems.

Cyber Security experts often discuss vulnerabilities and even more important, exploitable vulnerabilities. Vulnerabilities in a cyber perspective can be defined as weaknesses with a current digital system, and can be related to design, implementation, processes or control systems. If a particular vulnerability can be exploited by a hacker, we say it is an exploitable vulnerability.

2.1 Types of cyber attack

Hackers use multiple ways to attack their targets and their methods vary in complexity and sophistication. A brief description of some of the most common types of cyber attack in the financial industry follows.

Backdoor attacks are cyber attacks where attackers find a backdoor into the computer system, and manage to avoid the normal authentication and security processes. These attacks usually come as a consequence of weaknesses in the design and configuration.

Denial-of-service attacks (DoS) are attacks designed to prevent the rightful user to get access to the system. Common ways to execute DoS attacks are either to enter wrong password for an individual user enough times to lock the account, or the attacker can overload the machine capacity resulting in unavailable login for all users.

When an unauthorized user gains access to a data system, we call it **direct-access attacks**. An attacker can obtain access through physical access to the hardware, or by making operating software modifications using viruses and bugs like worms, keyloggers and covert listening devices. As soon as attackers have access they are likely to copy information or modify computer systems.

Malware attacks involves special designed software that aims to steal or destroy data. Viruses, worms, Trojan horses, ransomware, spyware and adware are examples of malware.

Man in the middle (MITM) is a cyber attack where an attacker insert itself in the middle of a conversation between to parties, and manipulate the conversation in order to obtain sensitive information. The two users still think they are communicating with each

other, but they are actually communicating with the middle man.

Since passwords still are the most used method to authenticate users, **password attacks** are a common strategy for attackers. There are mainly two methods used for password attack, Brute-force and dictionary attack. The first method involves using a software to randomly guessing different combinations of letters, numbers and commonly used passwords in order to crack the password. Dictionary attacks use combination of words from a dictionary in order to log in.

Phishing is a method where the attacker tries to acquire sensitive information from users by using emails and websites. The attacker aims to trick the target to send information such as usernames, passwords, credit card details etc. These attacks have shown to be pretty sophisticated. The attacker pretend to be a trusted entity, like an employee, friend or another plausible person, and it can be difficult to actually understand it is an attack without talking to the real person.

Eavesdropping involves surreptitiously listening to a private conversation. This form of attack can be done over phone, email and chat.

Jackpotting involves an attack at an ATM, where the attacker installing a malicious software and hardware onto an ATM. The malware give them control over the ATM and the attacker can then force the machine to dispense cash quickly.

3 Why Should Financial Institutions increase their focus on Cyber Security?

We live in a digital world, surrounded by digital products, platforms and solutions. Businesses today rapidly adapt new technologies in order to achieve a competitive advantage in a highly competitive environment. Fast development and adoption of new technologies can potentially lead to increasing number of security vulnerabilities and flaws. The risk of cyber attacks cannot longer only be a job for the IT department. It must be a part of the organizational culture and rooted in the strategy.

Beside the increasing number of potential security flaws, there are indications of increasing security threats. First of all, we experience an increasing complexity in the global environment, with great powers trying to strengthen their position through intelligence operations and sabotage in the digital space. Many attacks come from Russia and China, but also North Korea has their own cyber–army, which has become a big cyber threat for western governments and financial institutions.

Another potential threat is the increasing number of internet users. Today more than 4 billion are connected to the internet, which means nearly half of the world's population

still live unconnected. The growth rate in internet users are high, and as the number of users increase we can expect increasing number of attacks in the digital space.

Increasing threats and rapid development in technologies makes cyber security to a field every financial institution should focus on in the upcoming time. KPMG's 2018 U.S. CEO Outlook pointing at Cyber Risk as the top risk for today's businesses, no matter industry. And as much as 68% of CEOs believe it is a matter of when and not if. For financial institutions, which are attractive targets for hackers, there is no doubt Cyber Security should be a priority, and kept in mind when new technologies are being considered.

4 Cyber Security Trends In The Financial Industry

The technology sector has been growing rapidly. New advanced technologies have entered the market and the field of Fintech has increasing importance in the financial industry. As new technologies are adopted, the field of Cyber Security must adapt to new vulnerabilities and attacks. Hence, the rapid growth in technology, is a driving force for the massive growth in the field of Cyber Security. New trends come and go, and the next paragraphs will point out some of the trends we see in the field today.

4.1 Proactivity

As a result of the major ransomware attacks we have experienced lately, businesses in all industries have opened their eyes for the catastrophic consequences of an attack. Wannacry in 2017 and Petya in 2016 hit thousands of computers and resulted in damages worth billions of dollars. The need for backup routines and regularly updates came into people's mind and forced organizations to go over their routines in terms of cyber preparedness.

4.2 Adoption of more advanced technologies

We have earlier discussed the potential of groundbreaking technologies like Artificial Intelligence and Blockchain to financial institutions. In terms of Cyber Security, AI can be of great support for security professionals. Banks usually have a lot of data, and by applying machine learning algorithms, the data can be used to discover weak points and vulnerabilities before they are exploited. It can also be used to predict whether a transaction is genuine or not. There are a bunch of AI solutions for fraud detection and identity theft, and there will truly be even more as the technology becomes better and more intelligent.

Also Blockchain has a wide field of application, and it is secure by design. Blockchain is decentralized and distributed, which makes it nearly impossible to manipulate or destroy. It is highly likely that we will see more use of blockchain for transactions in the upcoming time.

Read more about AI and Blockchain here:
Part 2: Blockchain in Trade Finance
Part 3: AI in Finance

4.3 More advanced attacks

Unfortunately, advances in technology also lead to more advanced attacks. Usually hackers are forward leaning and ready to make use of new technologies pretty fast. They always aim to stay one step in front of researchers and Cyber experts, which can be frightening in a security perspective.

We have already seen examples of hackers using AI in cyber attacks. Data scientists from security firm ZeroFox, studied how AI can be used in order to create phishing tweets, and they figured out artificial hackers based on machine learning was better at creating posts with malicious links.

There are several ways attackers can take advantage of rapid developments in AI, and password attacks, phishing, and malware creating is just some of them.

In terms of malware, hackers have started to use more innovative macro tactics, to attack banks. Last year researchers observed a bank Trojan that used malware macros to evade Sandbox detection.

There is also a potential cyber risk in Internet of Things (IoT). IoT uses sensors to collect data, communicate, analyze and act on information. IoT devices can be commanded to undertake a coordinated attack at vulnerable systems. This can possibly lead to very dangerous situations. In the financial industry IoT is still in a very early stage, but the technology can be used for payments, in blockchain smart contracts, for authentication, and for banking at home.

The use of AI Assistants creates another potential vulnerability. Recently, it was discovered that Amazon Echo, which uses "Alexa" software, had recorded and sent a private conversation. This is problematic in a security perspective, since it opens up for a potential eavesdropping attack. Several banks are looking into AI Assistant banking services, and making a hundred percent secure service will be essential.

4.4 Multi-factor authentication

Password attacks are common, and AI can make it a lot easier for attackers to crack your password. Therefore, it is important to use multi-factor authentication. AI powered biometric authentication can use voice, fingerprint, retina and face scans, instead or in addition to normal passwords.
I believe we will see increasing use of more advanced authentication systems in the financial industry in the upcoming time.

4.5 Regulations

New cyber security regulations are being rolled out all over the world and some of them also affect financial institutions in the US.

Last year (2017) China's Cybersecurity law was put into effect, and the Cyber Security Agency in Singapore proposed their Cybersecurity Bill a month later. General Data Protection Regulation (GDPR) was put into effect in 2018 and gives consumers more rights and ownership over their data. Every

organization that store data about European citizens must follow to the new regulations. Many will truly fail to comply with GDPR, which will be very costly.

4.6 Competence shortage

There is shortage on competence in the cyber security industry. As businesses understand the real importance of cyber security and the massive consequences an attack can result in, financial institutions will experience challenges filling their new security positions, due to the relatively high demand.

We experience an increasing interest for Cyber Security among consulting firms. They are collecting highly professional expertise for their advisory services, and educate talent themselves. Due to the shortage of experts in the industry and the increasing priority among consulting businesses, we expect more outsourcing of Cyber Security in the upcoming time.

5 Cyber Threats To The Financial Industry

As we already have pointed out, most cyber attacks are financial motivated. The more sensitive data and valuable assets a business holds, the more likely it is to be attacked. Banks and other financial institutions have both sensitive information and money, and they are consequently a major target for financial motivated attackers. Banks are also a naturally target for cyberterrorism, since a successful attack can create chaos and decreasing trust. There is no doubt financial institutions face many threats in the digital space, but what is the biggest threats right now, and where are they coming from?

5.1 Changing landscape

Today's banks operate in highly complex environment with rapid changes. The risk landscape in 2018 is quit different then what it was only a few years ago. Attackers experiment with new methods and discover new vulnerabilities as soon as they occur.

Managers have to be up to date, and continuously following the developments in the field of cyber security. To be backward leaning in a constantly changing threat landscape, can be very dangerous and highly costly.

5.2 Third- and Fourth-Party Cybersecurity Risk

To monitor your vendors can be hard, especially for large financial institutions. In order to protect your data, you should have clear defined routines and control of who has access to your data.

Even though it is hard to monitor your vendors, it is even harder is monitoring fourth parties. Your vendor's third parties can pose a threat, and should, in line with your own vendors, be monitored. If a fourth party is out of play, due to a cyber attack, how will it affect your third party, and further how will it affect your own business?

A well developed vendor management plan can help you manage these threats.

5.3 DDoS Attacks

Initially, I presented denial-of-Service (Dos) attacks, which aim to disrupt services of a host connected to a network. Distributed denial-of-service (DDoS) attacks are increasing I popularity among hackers. It occurs when a portion of a network is targeted by incoming traffic from many different sources, usually resulting in very slow network or a completely crash and downtime.

Financial institutions can lose enormous amounts of money due to downtime. DDoS attacks are increasing in scale and pose a serious threat since it is relatively easy to execute. In April 2018 seven of the UK's largest banks were hit by a massive DDoS attack, resulted in reduced operations, downtime, and hundred of thousands of pounds in loss. The attackers used a software that could be rented for as little as 11 pounds. DDoS attacks are cheap, simple to carry out, and therefore a big threat for financial institutions also in the US.

5.4 AI

As described in paragraph 4.2, cyber attacks become more sophisticated with more advanced technologies, and there is no way to discuss potential threats without mentioning artificial intelligence. Fintech companies are working hard to come up with groundbreaking AI solutions for security proposes, and the industry fears that skilled hackers can get ahead in the AI technology race. If they do, they can use their AI to discover exploitable vulnerabilities before cyber security experts find them.

5.5 Jackpotting

Lately, cyber attackers have started to target ATMs. Earlier this year the first "jackpotting" attack was executed in the US. Criminals have figured out a way to exploit a vulnerability in banking, and just the first week they stole over $1 million dollars. This shows that cyber attacks are coming n new creative ways, which is problematic in a time were more services become digital.

5.6 State supported attacks

Intelligence services report increasing focus on cyber warfare. Cyber is both a cheaper and faster method of warfare, and many states have started to use cyber as a way to attack their enemies. Nation state attacks are not only targeting government infrastructure, they also attack businesses and organizations, in order to create chaos, gain sensitive information, and to finance their activities.

Russia is one of the most active actors in terms of state supported cyber attacks, but also North Korea, China and Iran have dedicated cyber armies that pose a threat for American financial institutions.

6 Conclusion

The fifth part of our series regarding development of Fintech strategy has focused on Cyber Security in financial services. Cyber is definitely one of the top risks for businesses today, and the consequences of a data breach can be enormous. Since the financial industry is a main target for attack, managers within the financial industry should be aware of the threats and keep up with the fast growing Cyber space.

Many financial institutions today aim to gain a competitive advantage through innovative technologies. Adaption of a new technology can improve business processes and platforms, but also potentially lead to new vulnerabilities, which in some cases are exploitable. Since the beginning of the digital revolution, hackers have detected exploitable vulnerabilities and carried out targeted attacks. As we have seen, millions of people have been affected and huge amounts of money has been stolen, due to successful cyber attacks.

Cyber Security is an ever changing field of expertise, and it can be hard to keep track with new trends. There is increased proactivity among managers and cyber experts are taking advantage of new groundbreaking technologies, like AI and Blockchain. Cyber security regulations are also being rolled out all over the world, and point out the importance of established routines in the digital space. Even though, the focus on cyber is increasing, there is also a competence shortage in the industry, and as more managers understand the importance of highly competent cyber specialists, we expect there will be more outsourcing of cyber security.

Financial institutions are facing a wide spectrum of cyber threats. One of the biggest threats involve the changing risk landscape. If companies do not keep track with new methods and techniques used by attackers, they will be a more attractive target.

Most businesses monitor their own processes and data flows, but are failing in monitoring third and fourth parties, which can be crucial. If a vendor is put out of play, as a result of a cyber attack, it can have impact on your daily operations. Other potential threats in 2018 are DDoS attacks, jackpotting, AI attacks and the increasing number of state supported attacks.

A cyber attack can be highly costly and end up in new investments, management replacement, public relation expenses, as well as huge marketing campaigns. Being proactive can be very valuable, and cyber security should therefore be taken into count when you develop your Fintech strategy.

Contact

To learn more, contact:

Brett R. Noyes
Managing Director at Unbank.Ventures
P 509-910-3496
E brnoyes@unbankventures.com
Skype noyeslimited

Author

Andreas Orset
Consulting Intern at Unbank.Ventures
P 0047 938 29 158
E andreas@unbankventures.com
Skype a.orset

Website
http://www.unbankventures.com/

Headquarters
San Francisco, California

Specialties
Fintech, accelerator, incubator, and venture capital

Year founded
2016

Company type
Partnership

Company size
2-10 employees