Security scorecard organisation analysis

Background:

Sam Kassoumeh and Dr. Aleksandr Yampolskiy started the Security Scorecard in in 2013. They were two earlier leaders of security, CISO, gift group and involved in a huge e-commerce business. Cryptography PhD holder Dr. Yampolskiy was also BlogTalkRadio/Cinchcast Chief Technology. He has also organized security roles and lead technology at companies like Microsoft, Oracle and Goldman Sachs. Kassoumeh has more than ten years of experience in cyber security, he is also Federal-Mogul lead Global Security. https://securityscorecard. com/company/March 4, 2017

Security Scorecard is a third party security system that helps to predict insights risks. It is very important for the organization or in person to protect their data from the computer database.

Security Scorecard is used to discover posture of security for any third party business partners or a single vendor. It penetrates test prioritizing onsite visits for a surveys on vendor security. It also gives an immediate alert when any new risk occurs in ecosystem of the vendor. Moreover it collaborate with the vendors to track their security issues. https://securityscorecard. com/March 12, 2017

Objectives:

Web Application Security

Web application security is a web based security system for web page, web application, website and web services. Security Scorecard one of the major objective is to protect the system from web threads. It governs the risks that

may come with the web applications route and checks any current threads in a company’s websites. It uses active defacements, outdated version or vulnerable applications to analyze the general grade.

https://securityscorecard. com/platform/how-it-works/March 12, 2017

Strength	Weaknesses
• Can secure application through the web portal. • Don’t need to be physically in the client system. • Since it is web based don’t have to worry about the system compatible.	• Needs someone to monitor the security system 24/7. • Can take time to filter each and every links. • Needs a server system which increases cost. • Since there are multiple web

- One patch file can help many organizations using same platform.
- application in same destination one loophole can cause harm to all.

Opportunities Threats

- Can upgrade easily once the new version is introduced
- Cloud storage could give opportunities to the small organizations.
- Since the service
- Since it is on the server side small pot hole can infect all application.
- Some client might find costly to implement in their system.
- Failure to find patch required for

provider is monitoring constantly client don’t need to worry about updates.

- Can improve security system of the application without having to hire personal employee.

the vulnerabilities.

- Increasing cloud computing could demand more web application security and unable to move with the growing demand could affect the business.

Network Security

Network Security is the security of the system hardware and software’s from illegal access, malwares and any kind of access without the knowledge of the owner. Security Scorecard identifies vulnerabilities on the server-side which may harm the users system attacking through network port along with

matching the unprotected network services weaknesses. .

https://securityscorecard. com/platform/how-it-works/March 12, 2017

https://www. messageops. com/wp-content/uploads/2016/01/SWOT_Analysis. pdf

Strength	Weaknesses
• WPA2 security can be its major strength for wireless access. • Server room will have well-labeled devices. • Proper tracking for the vulnerabilities. • Proper awareness to the clients.	• Productivity loss when monitoring is lack. • Can lead to legal concern in lacking mobile device policies. • Moisture problems are another weakness which could be

caused due to lack in humidity control.

- There might be time waste skipping the spam messages.

Opportunities	Threats
• Updated version VoIP technology can make savings and increase functionality .	• Giving permissions to users may create threats in the system.
• “ MDM of BYOD devices will mitigate	• Lack of updates could cause

	legal and management concerns.” (messageops, 2017)	security issues.
	• Can implement cable management to prevent outage producing errors	• Upgrading the software completely might not be practical in the older systems.
	• Efficient outcome can be done by refreshing hardware.	• Can be costly to the customers if they need to upgrade their systems frequently.

Stakeholders:

1. Immersive
2. Brinqa
3. Optiv

4. Venminder
5. Sycomp
6. En Polinte Technologies
7. Gothem Technology Group, LLC
8. Refister a Deal
9. Guide Point Security
10. Truvantis

Financials

According to Security Scorecard announcement in March 2015 they funded $12. 5 which was controlled by Sequoia Capital and existing stockholder sharing in the Series A round. Company has grown swiftly since it began sincerely in early 2014 and has more than 100 highly skilled employees working in front end and back end worldwide. https://securityscorecard. com/company/(March 16, 2017)

Risks:

Tangible Risks:

1. Spy workers: Spy workers are one of the main risks for the company. They can take our secrets to other companies for their profit. This will hamper the business.
2. Cable error: Since the company is about online security failure of the network cable might affect the company to give proper services to the clients.

3. Update delay: I the company fails to update the product on time then there are many new updated vulnerabilities which can enter the system and crash the whole system.
4. Unskilled manpower: Unskilled manpower or not enough experience in the field will cause errors in performing some major tasks. So, they should be working under the experienced workers.
5. Competitors: Competitors are the most dangerous risks for the business because if we cannot match up with the competitors then they may be introducing more advance products than ours which will eventually leads to loss in clients.

Intangible Risks:

1. Power cut off: Power cut off is one of the major issues for the developing countries. There might not be any power cut off in developed countries but in under-developed or developing country it is still a major issue that will hamper the business.
2. Connection loss: Connection loss in the network is one of the biggest issue. Since, connection is a technical issue it can happen any time without the prior notice. We can’t even be prepared for this kinds of issues. We have to deal with it once it occurs and must be able to solve it as soon as possible.
3. Natural calamities: Natural calamities is a disaster which we never know when it happens. Since it is cause due to nature disasters we can’t even think of what damages will it brings to the company.
4. Server down: Server is the main storage of all the data. Even after taking all the precautions we might face this problems unknowingly.

We can only take precautions like taking backups, cloning servers or making different servers for different tasks.

5. Software crash: Security Scorecard is a web application that provides the security to the client’s computer devices. If the application crashes it will fail to give security and threats might find its port to enter the system of the clients. So, we must be very aware about it.