Udipto Chowdhury
Prof. Kennedy
FCM 761
05/22/2023

Trenton Stanford Agenda

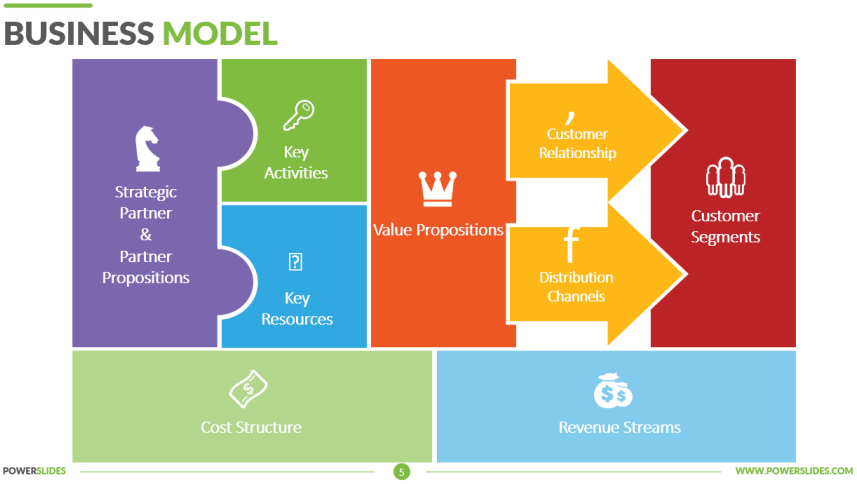
Version	Updated By	Title	Date	Notes
1.0	Udipto Chowdhury	CEO	05/22/2023	*none*

Table of Contents

Background

Trenton Stanford is a cybersecurity firm that resolves many issues dealing with cybersecurity, data leakage, or any issues. In addition, the company deals with threat mitigation, unexpected data exposure, threat protection, security monitoring, and data recovery. Since the company and myself are partners with McAfee and the Federal Bureau of Investigation, we make sure that at most 25,000 employees work over there with 10 different locations (New York City, San Francisco, Melbourne, Tokyo, Shanghai, Mumbai, London, Berlin, Cape Town, and Toronto) worldwide, altogether. Despite being a start-up company, my company will ensure what is best for the people, the business, and its reputation. In addition, there are external sources that will be willing to contribute to the projects that need to be completed by any means. In a nutshell, my company wants to ensure that the clients are to be protected from cyberterrorism, cybercrime, and any other complications that deal with network espionage. Because your safety matters and we want to ensure that no one deserves the right to damage people's network privacy and technological well-being.

Business Model



★

★ Strategic Partner & Partner Propositions: Client(s) gives us the offer and we make sure that their wants and needs are delivered as well as ensuring their protection from us.

★ Key Activities: Understanding client's/clients' situation(s), Planning to tackle the conflict(s) and problem(s), NIST Framework.

★ Essential Resources: McAfee Security, VPNs, and Traceback(s) to find the root cause of their problem(s).

★ Value Propositions: Communicating with the client(s) is/are the key to gaining a reputation, and making sure that their expectations are delivered successfully.

★ Customer Relationship: If the customer loves our work ethic, then we gain more customers for their favors as well as our revenue increases with reputation.

★ Distribution Channels: Advertisements, Word of Mouth

★ Customer Segments: Same with 'Distribution Channels' but clients will recommend our company if we maintain our work ethic and etiquette.

★ Cost Structure: Expenditures on applications, devices, paycheck distributions, and business infrastructures (around $200 million) - Supply

★ Revenue Streams: Profits for our services and shares (Projected target for $500-$750 million) - Demand

Purpose

The purpose of this document is to illustrate our company. It is like a brochure except it is focused on our company and our ambitions. Especially with our objectives and the blueprint for our company.

Scope

This program sums up what my company is about and it describes everything my cybersecurity firm has to offer from A-Z. As long as our employees do what they are supposed to do when it comes to their duties and responsibilities, employees can work however they want to as long as they follow these rules: No eating during work, do not talk about their work with anyone else except their co-employees, do not use computers for personal purposes (use the break room if you are bored), do not wear shorts or skirts (unless if you have my permission), and every Friday - employees would write their reflections regarding their work experience.

Key Terms and Definitions

1. Workplace Communication: The process of exchanging information and ideas verbally and non-verbally between one person or group and another person or group within an organization.
2. Risk Management: Identifying, assessing, and controlling threats to an organization's capital and earnings. These risks stem from a variety of sources, including financial uncertainties, legal liabilities, technology issues, strategic management errors, accidents, and natural disasters.
3. Data Protection: The process of protecting sensitive information from damage, loss, or corruption.
4. Cyber Risk Mitigation: the application of policies, technologies, and procedures to reduce the overall impact and risk of a cyber threat. It is a critical practice to help guide decision-making around risk control and mitigation and allow your organization to stay protected and achieve its business goals.
5. Authentication: The process of identifying someone's or something's identity, making sure that something is true, genuine, or valid. This can be carried out either by a PIN or password, retina scan, biometric scan and sometimes even a combination of these things.

6. Social Engineering: This technique includes psychologically manipulating human minds and breaking standard security procedures and best practices to gain unauthorized access to systems, networks, or physical locations or for financial gain.
7. Digital Signature: A method used for the encrypted, electronic stamp of authentication on digital information such as documents, emails, macros, or digital content. A digital signature assures that the information or data originating from the signer has not been altered.
8. Agile Project Management: An iterative approach to managing software development projects focusing on continuous releases and incorporating customer feedback with every iteration.
9. Intrusion Detection System: A monitoring system that detects suspicious activities and generates alerts when they are detected.

Governance

This program has been authorized under CEO and Board since my company's grand opening. The CEO (which is me) will delegate the authority to anyone internally as long as any employee/employer is not putting in the effort to uphold the company's reputation. Every Friday, all the employees will have a meeting with the employers and in turn, all the employers will have a meeting with us executives. If the stakeholders are involved, my executives and I will make sure their demands are met and they receive their cut depending on the project or their favors. I will ratify the changes to make sure my executives and the stakeholders agree to their terms. Security guards and employers will enforce my company regarding security and ensure that this company is not infiltrated. Therefore, these are the roles that serve its importance when it comes to upholding the company's reputation.

Department	Personnel	Title	Function
Executives	CEO, VP, Treasurer, Director of Communications	VIPS	Looking after the company and ensuring the company upholds its reputation.
Employers	Generalized	Mr./Ms./Mrs.	Recruiting employees, making sure the employees are doing what they are supposed to.
Employees	Generalized	Mr/Ms./Mrs.	Do the assignments, Learn the tricks and trades, and make sure that the company's reputation has been upheld.

Regulatory Landscape

When it comes to establishing a regulatory landscape: technological infrastructure, employment diversity, and company establishment are the essentials when it comes to creating a regulatory landscape. Treasurer plays the role of analyzing the revenue and costs of the infrastructures, Employees play the role of reporting their checklist and tasks they have finished, and I play the role of making sure everything is running smoothly and assisting the employees and the executives when it comes to marketing and distribution. Our primary regulation is to make sure everything is accomplished in a fashionable and punctual matter. Be it company maintenance, revenue, and sales, or ensuring the employees are to be treated with respect no matter their positions.

Privacy Programs

When it comes to Privacy Programs: Employee Training, VPN, and Virtual Monitoring are the keys to establishing employees' privacy and preventing data leakage. When it comes to

core fundamentals for data privacy, unique passkeys (RSA tokens, Two Factors) are the key to ensuring this person is trustworthy when it comes to exchanging confidential pieces of information.

Data Governance

When it comes to protecting any kind of data, the employees, the IT Specialists (ensuring every single electronic device work properly), and I will make sure the data are not exposed and are impossible to hack through with the SHA-256 algorithm and creating extra layers of protection through VPN and two-factor authentication.

Training and Awareness of the Program

The Training and Awareness Program is crucial to us when it comes to working with Trenton Stanford. Soon-to-be employees are to be given brochures regarding our company's motto, what the executives and I are to be expected of, and employers' wants and needs. As long as my company works like a well-tuned engine, there is nothing to be worried about. In-person orientation, Zoom meetings, and In-person tours of the whole building are the key elements when it comes to illustrating what and where the future employees are going to be working at.

Risk Management

When it comes to Risk Management, NIST's CS Framework is the way to go since it gives the company motivation on what to do and what not to do. Because it was created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure, which in turn helps the companies to be prioritized, a flexible, repeatable, and cost-effective approach to the Framework. Which in turn helps us to manage cybersecurity-related risk. Since a goal-based approach determine the actual outcome of a project when compared to the goals of the original plan. This helps the position of the evaluation that was taken to understand the position as well as knowing the do's and don'ts when it comes to improving the employers' and employees' awareness when it comes to dealing with cybersecurity infrastructure. In a nutshell, risks are to be carefully analyzed and follow the NIST CSF guidelines.

Risk Register

- ★ Please refer to the '.xlsx' file for Risk Register.
- ★ In addition, because 'Identify' and 'Recover' used to be this company's weakest link, these two categories are on the better side with a 3.5/5 rating.

Physical Security

- ★ Security Guards will scan you every time you enter the company.
- ★ Biometrics will tell if you are an authorized employee.
- ★ CCTVs are everywhere so be mindful of your actions.

Policies

- ★ Data Classification and Governance Policy
  - Must not be shared with others with the exception of co-employees and your subordinates.
- ★ Identify and Access Management Policy
  - Keep your RSA token with you whenever you enter the building.
  - Make sure that your Identification Card is not lost.
  - Failure to adhere to these regulations can be resolved with your supervisors or myself.
- ★ Data Retention and Destruction Policy
  - Do not under any circumstances share confidential information with any third-party candidates (that includes clients, stockbrokers, and stakeholders).
  - Make sure the confidential data are not to be spilled anywhere outside of the workplace.
  - Failure to adhere to these regulations means that your employment is being terminated in an immediate manner.

- ★ Website Privacy Policy and Terms of Use
    - Do not share any Confidential Information with the Third Party
    - Use the desktops at your own risk (This means no Youtube, no Social Media, no Lesuire Activities, and no NSFW activities)
    - You can use the desktops for personal/leisure uses only in the break room.
    - Failure to adhere to these rules will conduct a 96-hour individual surveillance and the user's web access to be suspended for a few days.
- ★ Mobile Device Policy
    - You can use your phone outside of the workplace and in the break room.
    - Under any circumstances, do not attempt to connect to the WiFi without authorization.
- ★ Acceptable Use Policy
    - Self-Explanatory
    - Use your electronic devices at your own risk

Procedures

- ★ Business Recovery Procedures
    - Create a backup once a week (every Friday)
- ★ Disaster Recovery Procedures
    - Create a backup once a week (every Friday)
    - Evacuate the building in case of fire or any other natural disasters
- ★ Incident Response Procedures
    - Respond to the Incident w/ solutions as soon as possible (Top Priority)
- ★ Identity and Access Management Procedures
    - Biometrics
    - Make sure that there are no impersonators
- ★ Third-Party / Supply Chain Due Diligence Procedures
    - Since Third-Party / Supply Chain Due Diligence is any person or organization that is connected to your supply chain or is executing business on your organization's behalf such as a supplier, distributor, agent, and/or partner can

potentially expose you to unknown third-party risk, the company and I will ensure that there are no infiltrations being occurred inside the building.

- ★ Software Development Lifecycle Procedures
  - Once a year, all the desktops will be updated to the latest updates
  - Defectives are to be discarded

Guidelines

- ★ Data Loss Prevention Guidelines
  - Create a backup once a week (every Friday)
- ★ Physical Security Guidelines
  - Pretty Self-Explanatory
  - Security Guards will know if that guest is a friend or an enemy
- ★ Inventory and Asset Management Guidelines
  - Self-Explanatory
  - Inventory and Assets are to be carefully inspected with precautions
- ★ Vulnerability Management
  - Devices will not be vulnerable as it is protected by McAfee and NordVPN
  - However, if it is then the device has to be reset to the original settings

Periodic Testing

- ★ Annual Risk Assessments
  - Once every Six Months
  - It is based on NIST's Guidelines

- ★ Annual Penetration Testing
  - Once every Three Months
  - The IT Specialists and I will assess the Penetration Testing.
- ★ Annual DR/BCP Testing

- Once every Six Months
- Since the BCP (Business Continuity Plan) consists of a business impact analysis, risk assessment, and an overall business continuity strategy; while the DR (Disaster Recovery) plan includes evaluating all backups and ensuring any redundant equipment critical to recovery is up-to-date and working.
  - BCP is to be analyzed through NIST's Framework as well as our expectations.

★ Periodic Phishing Testing
- Once a month
- IT Specialists will send spam emails at random times.

Configuration Standards

★ Mobile Device Configuration Standards (Mobile Device Management)
- Nord VPN

★ Desktop / Laptop Configuration Standards
- Nord VPN
- Teramind (Remote Desktop Surveillance)

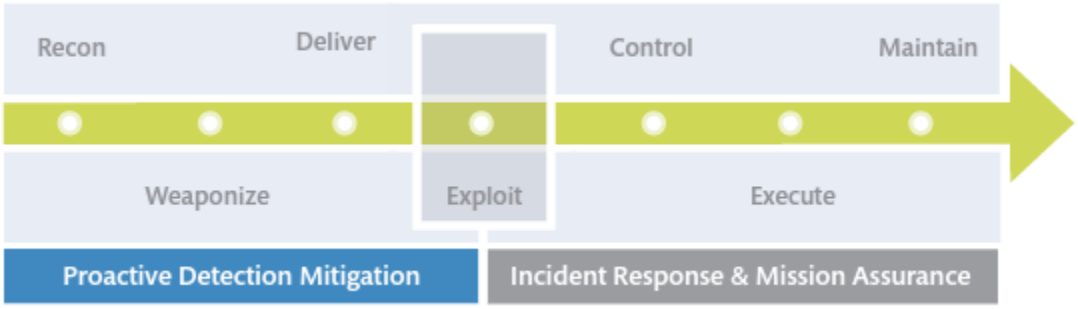
★ Network Device Configuration Standards
- Secured Network Protection

★ Network Security Standards
- Very Self-Explanatory
- As long as network security has a secured protocol, then there is nothing to be worried about.

★ Email Configuration Standards (incoming/outgoing/mail client)
- SMTP
- Encrypted Message Protocol through Gmail

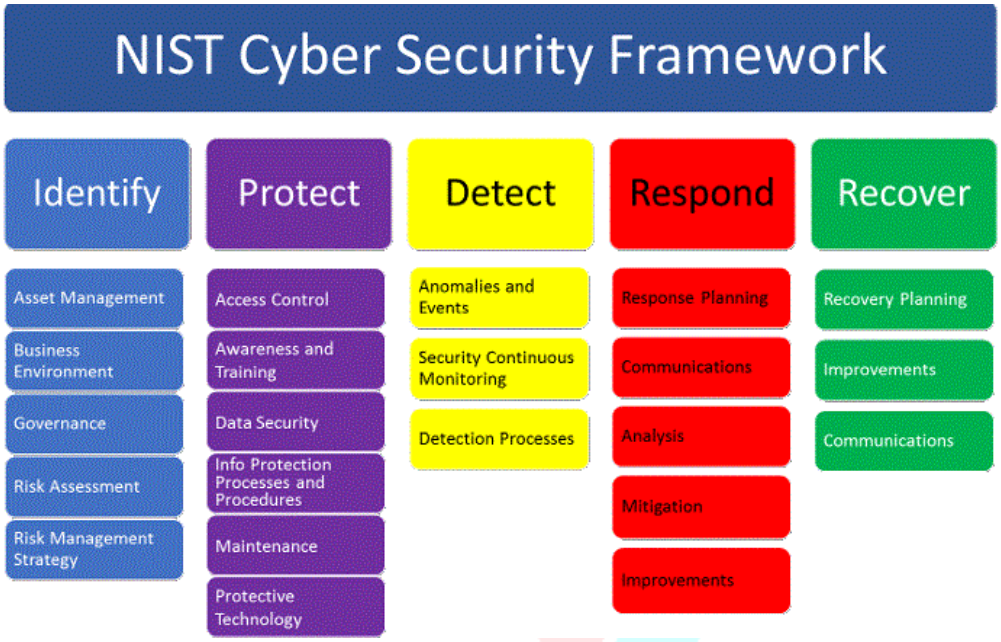
Cyber Defense Program

Outline your Cyber defense strategy. What are the core tenets? What are the baseline fundamentals of cyber defense?



- ★
- ★ Recon: Analyze open resources to provide indicators and warnings of intrusion attempts.
- ★ Weaponize: Analyze artifacts to create high-fidelity signatures to detect malicious activity.
- ★ Deliver: Understand adversaries' tools and techniques for delivering messages to intercept them as early as possible.
- ★ Exploit: There should be leverage for anti-exploitation and exploit detection techniques to find zero-day attempts.
- ★ Control: Employ robust intrusion detection signatures and tools to detect newly installed implants.
- ★ Execute: Create and configure internal networks to detect existing internal compromises.
- ★ Maintain: Deploy advanced host analysis to detect hidden implants and abnormal activity.

Additionally, NIST helps with establishing an action plan when it comes to Cyber Defense Program.



In fact, it is all about doing what is best for the company when it comes to protecting others from random cyberattacks, and based on the diagram below, the framework will ensure that again, the company runs like a well-oiled machine.

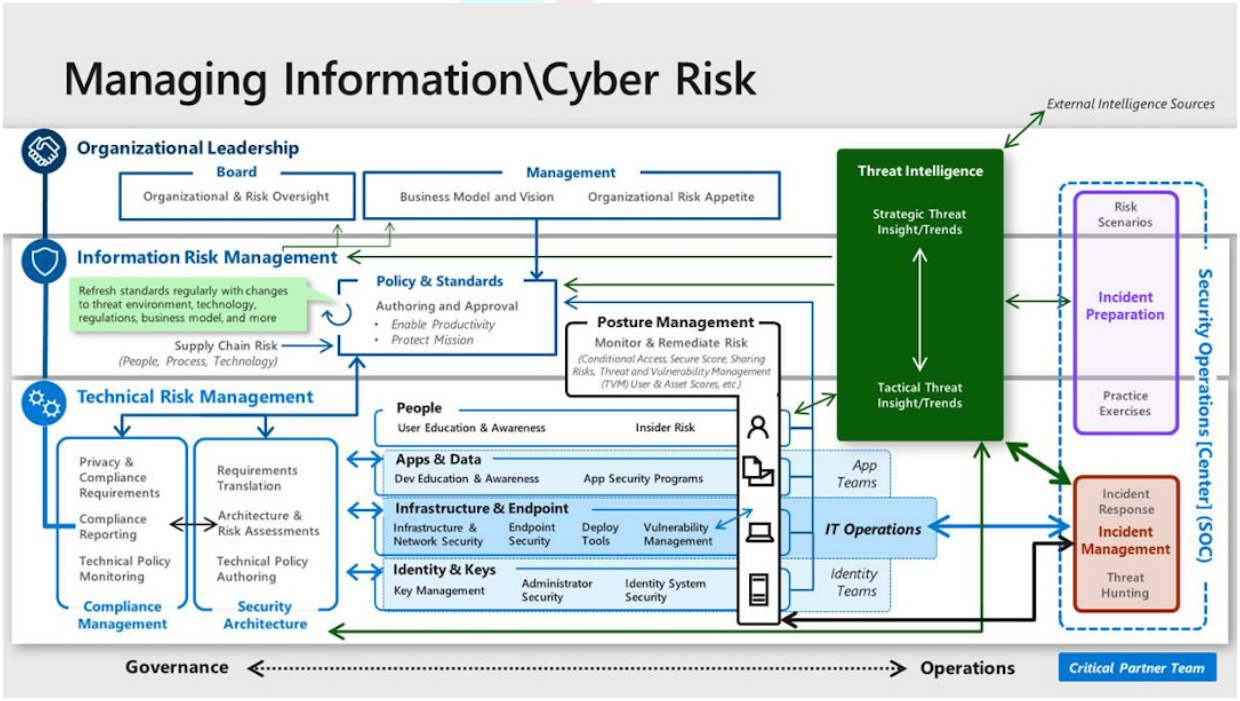
Defense in Depth: Which technical components of this strategy will you implement?

- Definitely, Protection when it comes to technical concepts. According to NIST, our company should develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services.

Zero Trust: Which Technical components of this strategy will you implement?

- Since Zero Trust is defined as a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. It should fall under the Identify category according to NIST since it helps us to identify if the employee's identity is genuine or artificial.

Team / Organization Structure: How is your Cyber team structured? What are the key roles and responsibilities? Agile approach? 3LOD approach? A blend of both?



- This illustrates how the cyber team should be structured and their key responsibilities are to ensure the data is protected and the network is not breached externally.
- In fact, if we combine agile methodology with three lines of defense. The combination will be unstoppable since the agile methodology is a way to manage a project by breaking

it up into several phases. It involves constant collaboration with stakeholders and continuous improvement at every stage. With the concept of Three Lines of Defense: The first line of defense owns and manages risks/risk owners/managers, the second line of defense oversees risks/risk control and compliance, and the third line of defense provides independent assurance/risk assurance. It is all about prioritizing our objectives.