Ottawa's French School Cyber Attack 2021

By : Gursheen, Kavitha, Thasleema

(UPLIFT-YWCA : Advanced Information and Cyber-Security Leadership [Uottawa])

SITUATIONAL AWARENESS

Situation

Ottawa French public school board was the victim of a network security breach in October and it paid the hackers a ransom to secure the stolen data. Informations such as Bank details, Address, DOB about employees,students and parents had been stolen which is approximately 75 gigabytes worth of data.

We have analysed and recommended a set of frameworks, standards and practices to be established in school boards to avoid future attacks.

Mission

To analyse the attack using the context of the organization and using CAF framework and regulation like PIPEDA. Gap Analysis against CSF and best practices to prevent future attacks.

Execution

Analysis will be done using the existing frameworks and regulations against the available information regarding the attack and the school such as

- Assets breached
- Interested parties
- Policies and procedures
- Applicable frameworks
- Best practices

Controls

Regulation:

PIPEDA

Framework:

Context of the organisation

Cyber Attack Framework

Cyber Security Framework

Services

Internal:

SIEM

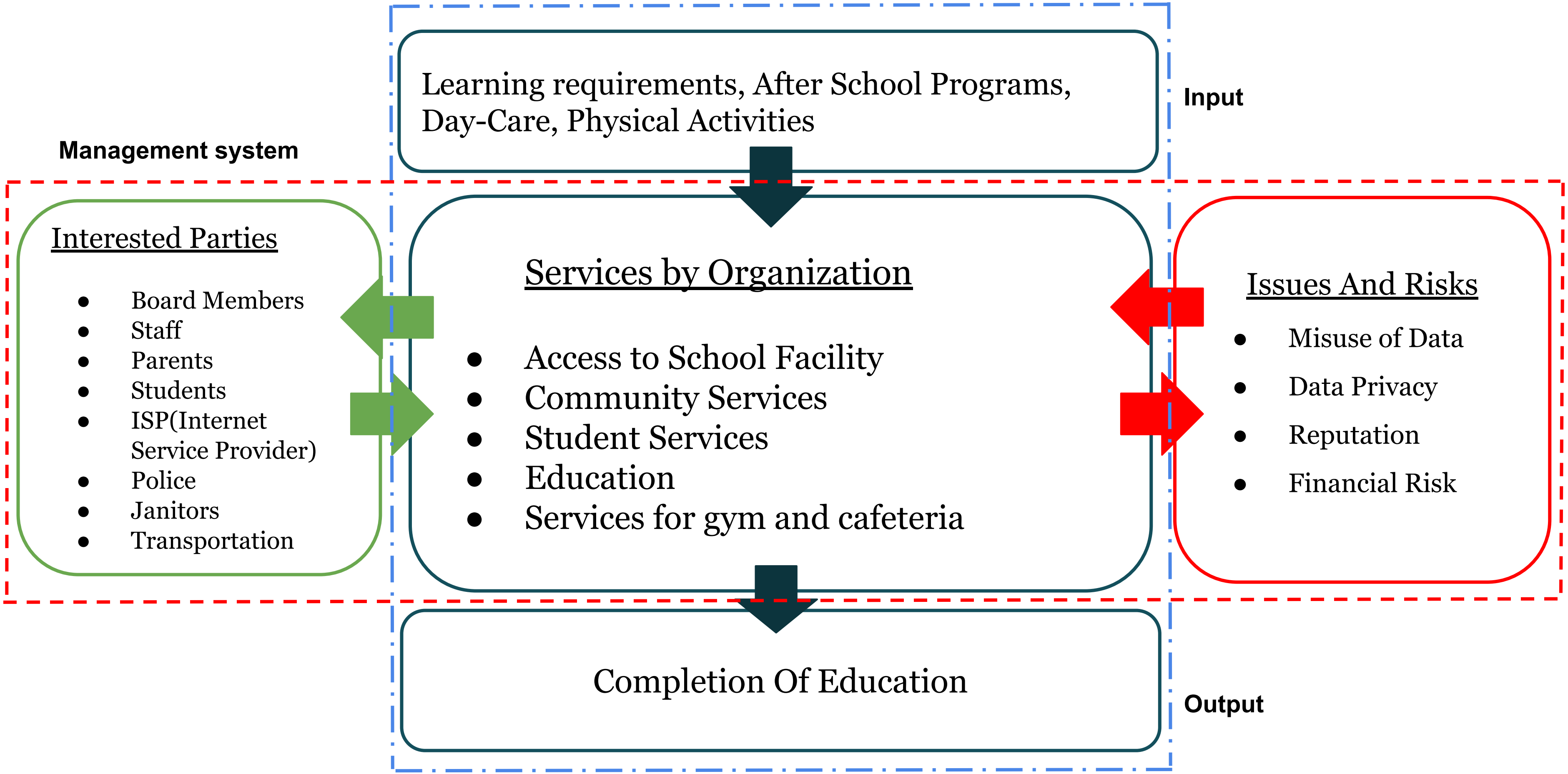
SIRT : Table-Top

Training to staff and students

External:

Third party auditing, ISO 27701

CONTEXT OF ORGANIZATION



Input

Learning requirements, After School Programs, Day-Care, Physical Activities

Management system

Interested Parties

- Board Members
- Staff
- Parents
- Students
- ISP(Internet Service Provider)
- Police
- Janitors
- Transportation

Services by Organization

- Access to School Facility
- Community Services
- Student Services
- Education
- Services for gym and cafeteria

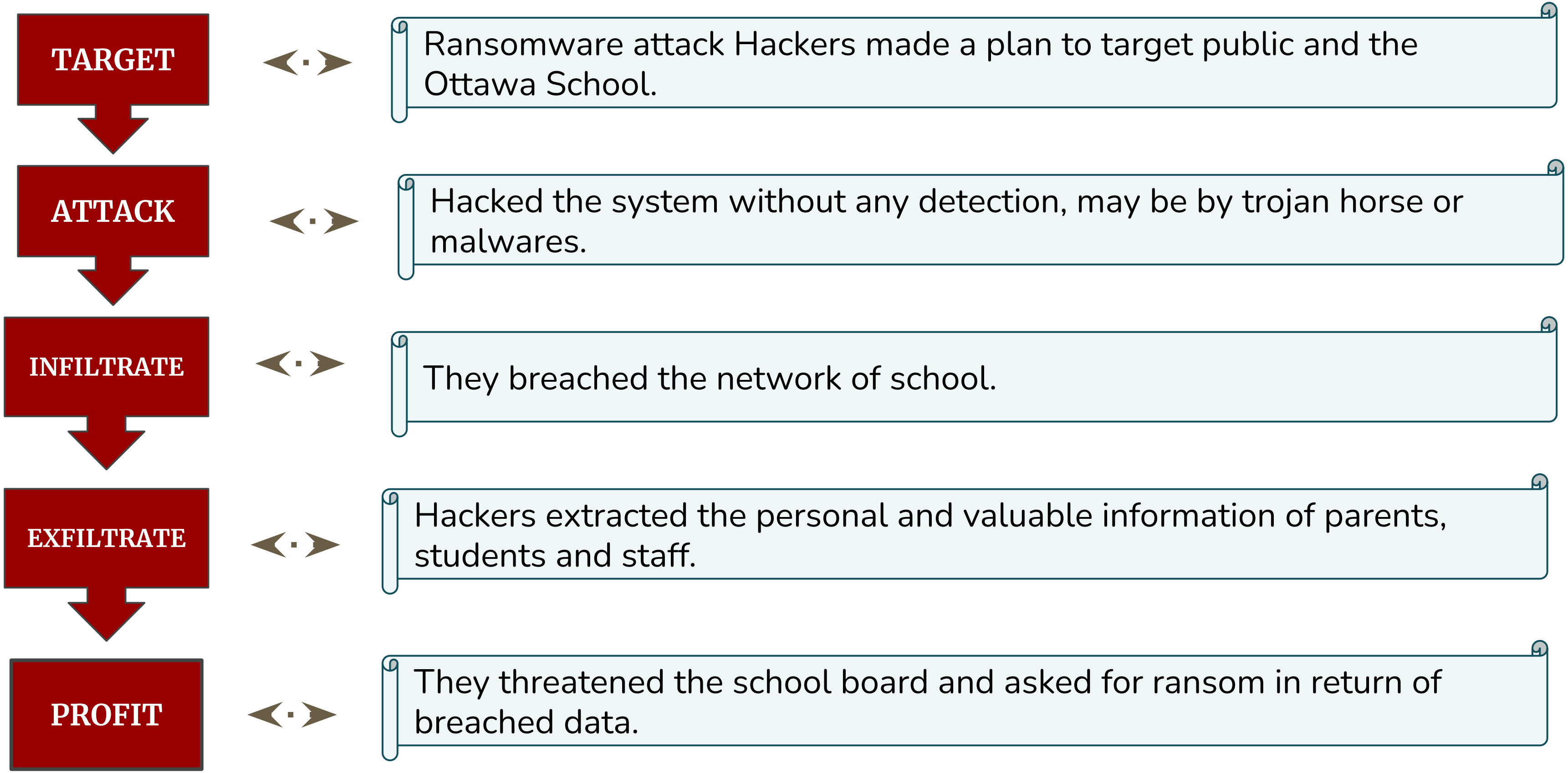
Issues And Risks

- Misuse of Data
- Data Privacy
- Reputation
- Financial Risk

Completion Of Education

Output

CYBER ATTACK FRAMEWORK



TARGET — Ransomware attack Hackers made a plan to target public and the Ottawa School.

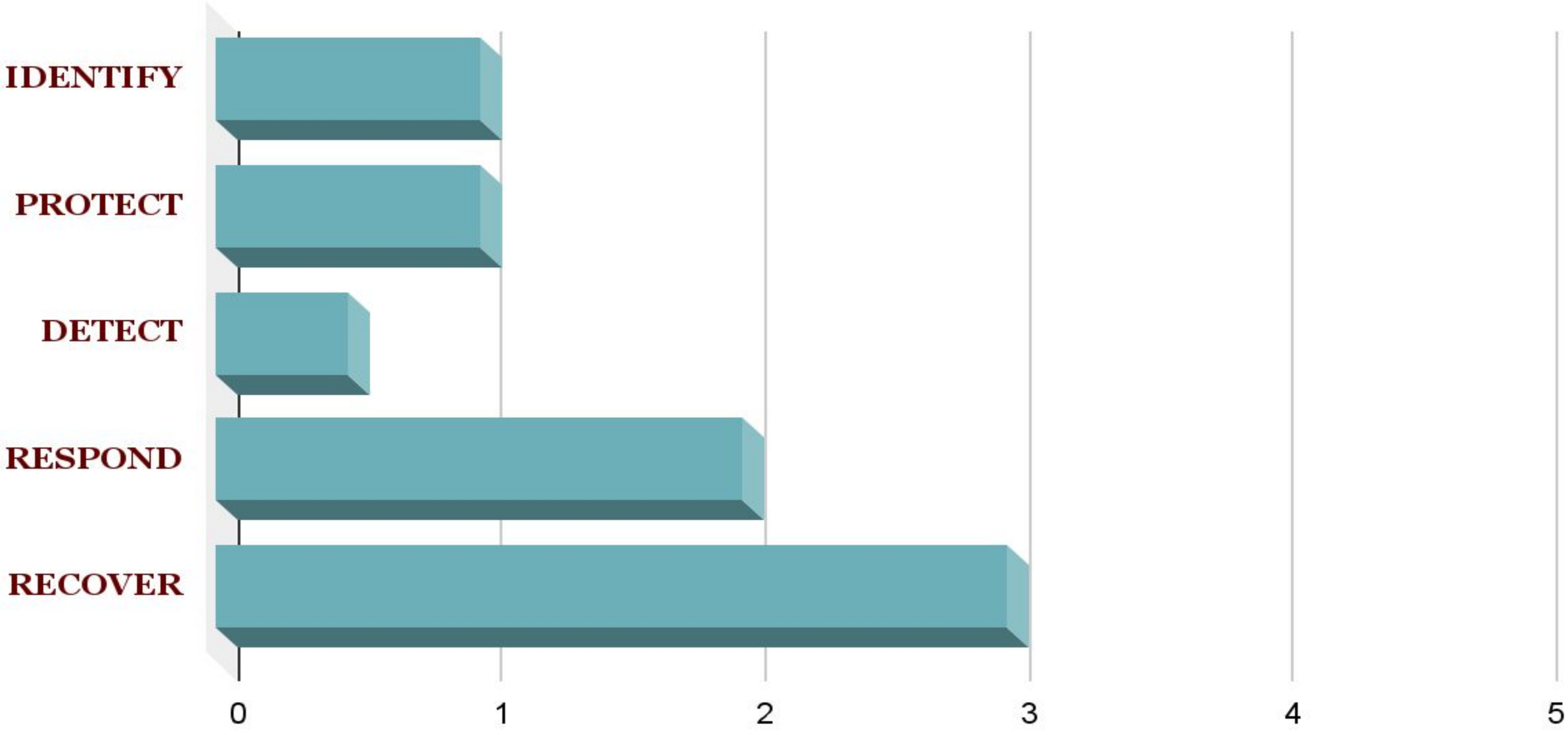
ATTACK — Hacked the system without any detection, may be by trojan horse or malwares.

INFILTRATE — They breached the network of school.

EXFILTRATE — Hackers extracted the personal and valuable information of parents, students and staff.

PROFIT — They threatened the school board and asked for ransom in return of breached data.

GAP ANALYSIS



STANDARDS AND REGULATIONS

The Personal Information Protection and Electronic Documents Act (PIPEDA)

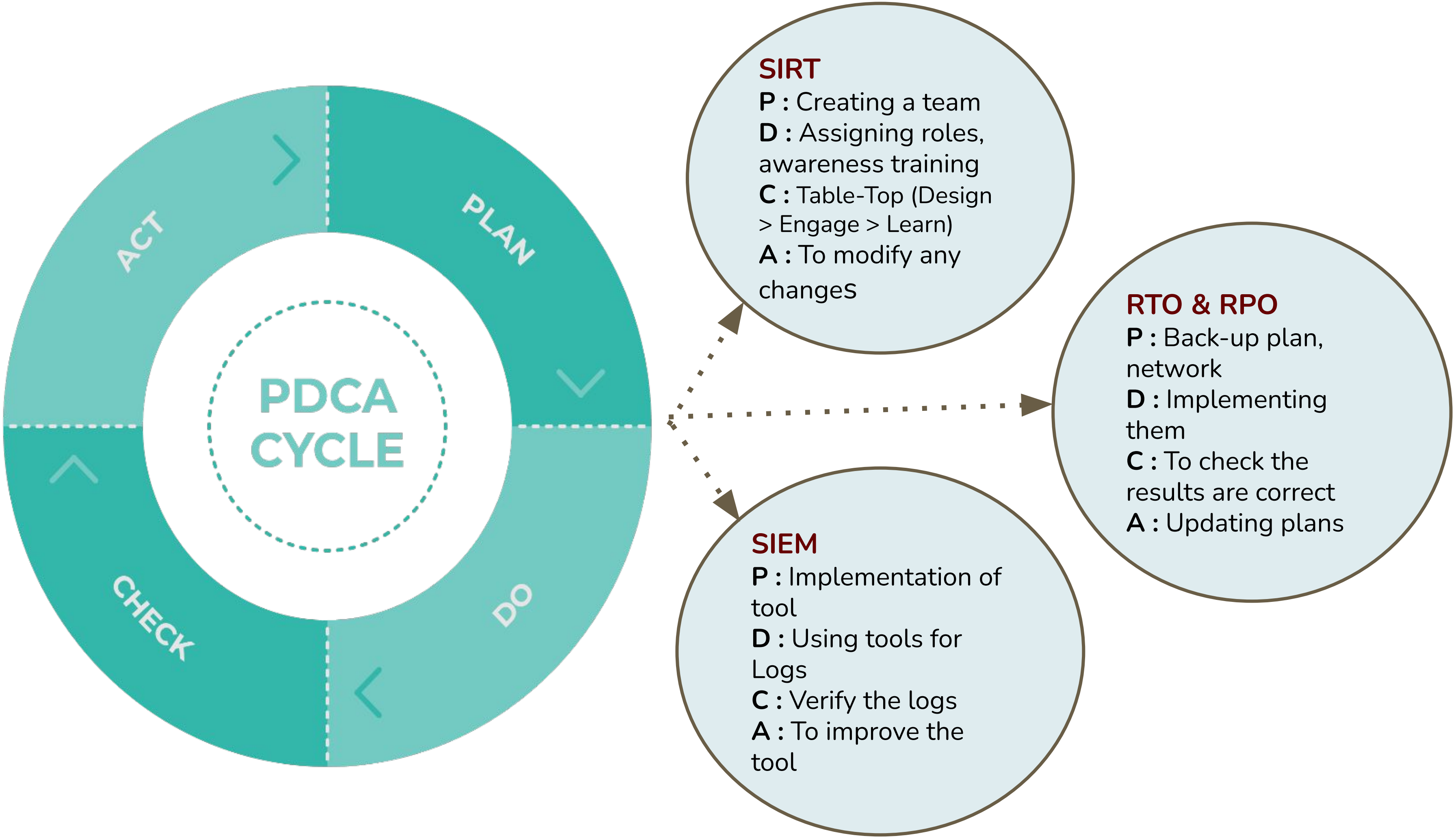
Under PIPEDA, personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- age, name, ID numbers, income, ethnic origin, or blood type;
- opinions, evaluations, comments, social status, or disciplinary actions; and
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).

RISK REGISTER & MITIGATION

RISK	DESCRIPTION	LIKELIHOOD (from 1 to 5)	IMPACT (from 1 to 5)	SCORE (L*I=25)	MITIGATION
DATA PRIVACY	Safety of data is the main priority.	5(would have been 3 before attack)	4	20	Following and implementing regulation PIPEDA, ISO 27701(data privacy)
FINANCIAL RISK	Banking Details, Personal Information	3	3	9	2-Step authentication, strict access control to data
NETWORK BREACH	Servers, Phishing emails, Click-baiting, Key-logging	5	3	15	SIEM helps in monitor and prevent and SIRT helps in reacting and restoring the business
PHYSICAL RISK	Operational risk, Wifi, Property Damage	3	2	6	Only restricted entries, authenticated Wifi usage

BUSSINESS CONTINUITY PLAN



SIRT

P : Creating a team

D : Assigning roles, awareness training

C : Table-Top (Design > Engage > Learn)

A : To modify any changes

RTO & RPO

P : Back-up plan, network

D : Implementing them

C : To check the results are correct

A : Updating plans

SIEM

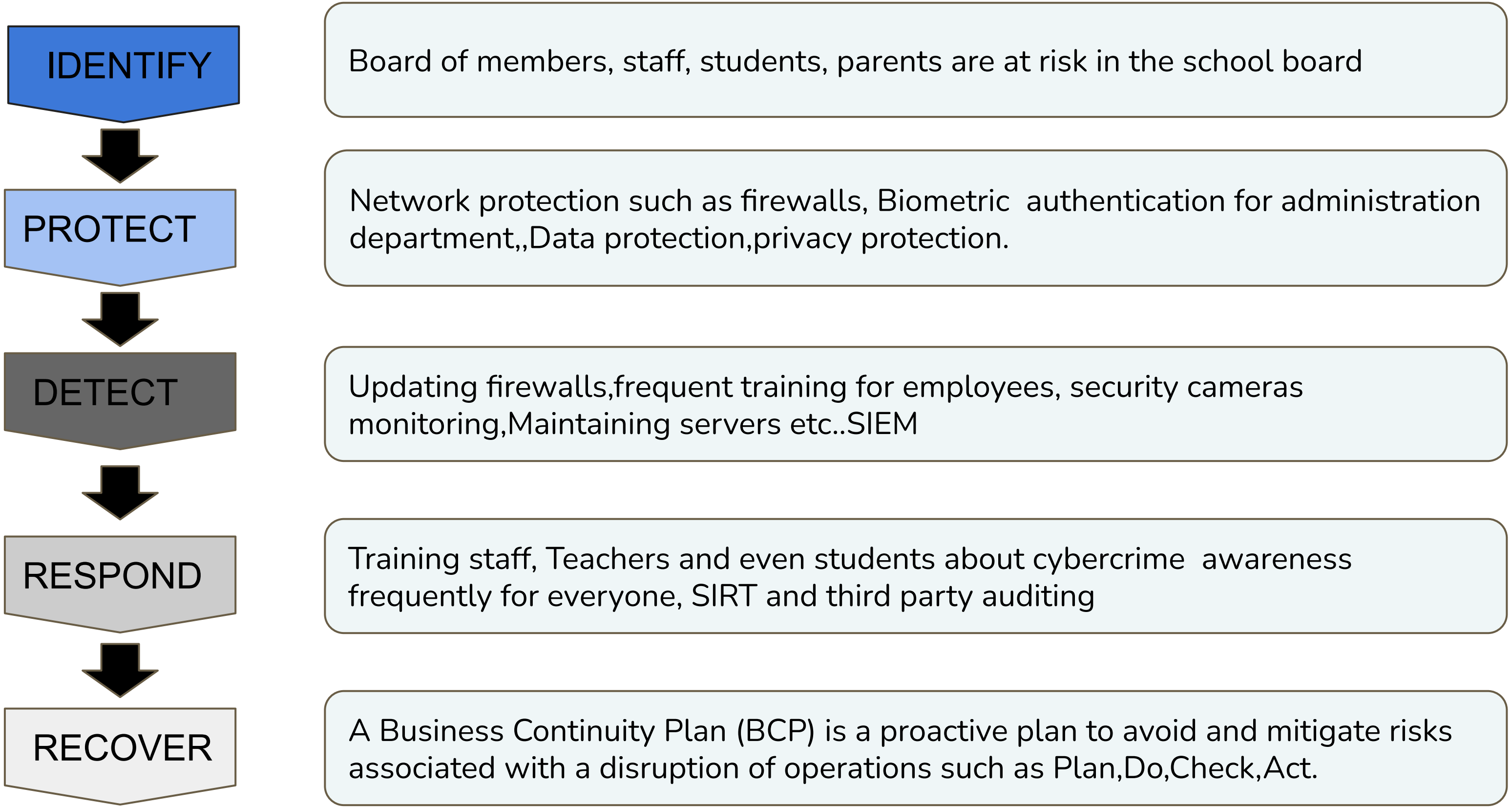
P : Implementation of tool

D : Using tools for Logs

C : Verify the logs

A : To improve the tool

CYBER SECURITY FRAMEWORK



IDENTIFY

Board of members, staff, students, parents are at risk in the school board

PROTECT

Network protection such as firewalls, Biometric authentication for administration department,,Data protection,privacy protection.

DETECT

Updating firewalls,frequent training for employees, security cameras monitoring,Maintaining servers etc..SIEM

RESPOND

Training staff, Teachers and even students about cybercrime awareness frequently for everyone, SIRT and third party auditing

RECOVER

A Business Continuity Plan (BCP) is a proactive plan to avoid and mitigate risks associated with a disruption of operations such as Plan,Do,Check,Act.

QUESTIONS & ANSWERS

THANK YOU!