CYBER SECURITY BUSINESS PLAN (Team 2)

06 Jan 2022

Dave Newman
Jeremy Wang
Chan Yin Seng
Matthew Tan

OUR COMPANY

Secure & Protect™ believes that security is essential for every organisation.

We help clients migrate their on premise IT services to Microsoft Azure while adding comprehensive security solutions.

This will enable Organisations to protect their data and services against potential cyber threats.

Matt

OUR TEAM

Dave Newman
Chief Architect

Jeremy Wang
Chief Strategy Officer

Bryan Chan
Chief Project Lead

Matthew Tan
Chief Operations Lead

Matt

Agenda

01 Problem Identification

02 Solution

03 NIST Framework

NIST

04 Business Plan

05 Conclusion

01 Problem Identification

Jeremy

What Happened - The Trigger

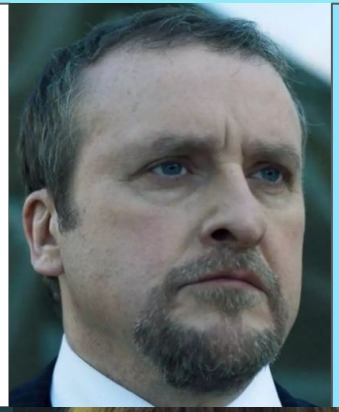
ACME Manufacturing Pte Ltd

1. correo a la CEO
2. dinero de licitación aprobado
3. de cfo
4. y de regreso a cfo

mail from: alicia.sierra@acme.com
rcpt to: luis.tamayo@acme.com
subject: final approval of tender
date: april 1, 2020 15:50:43 +0800 UTC
reply-to: professor@lacasedepapel.com

Evening Boss,
Please i need your final approval on the bid amount for the tender later.

Regards,
Alicia



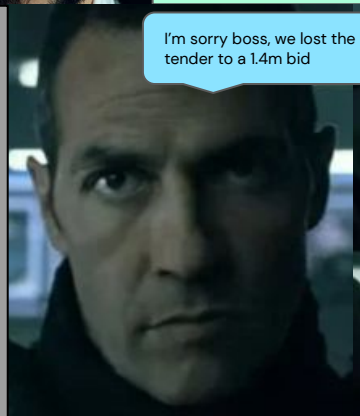
Dear Alicia,

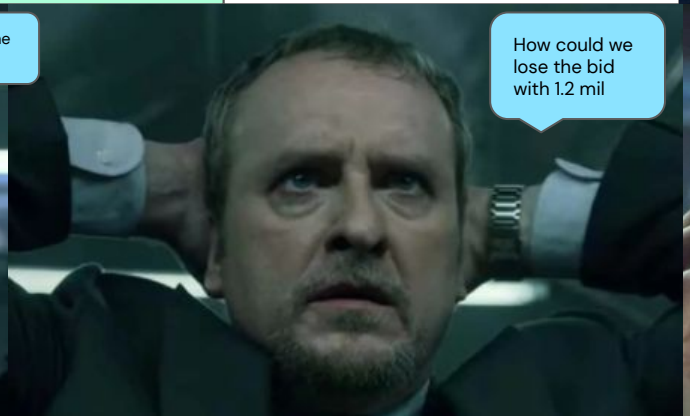
1.2 mil please go ahead.

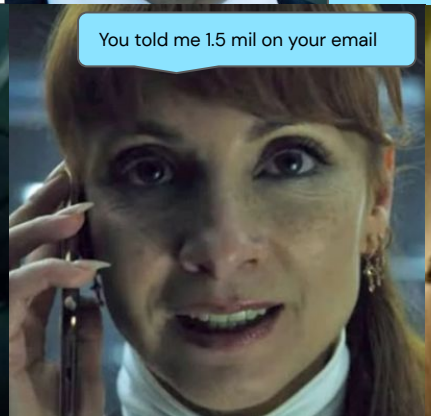
I bet this is the perfect amount for the bid.

Tamayo

A few weeks later...

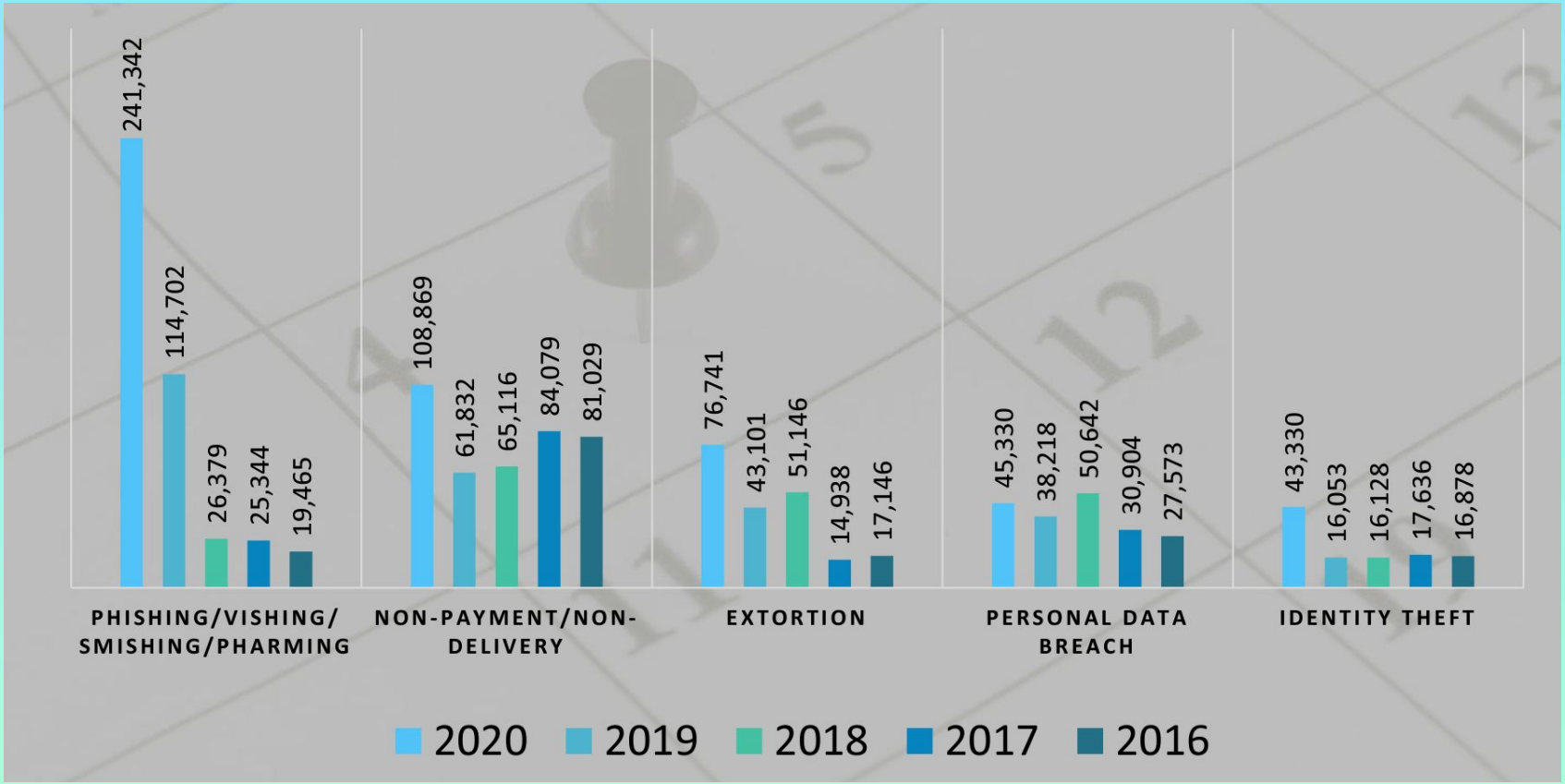






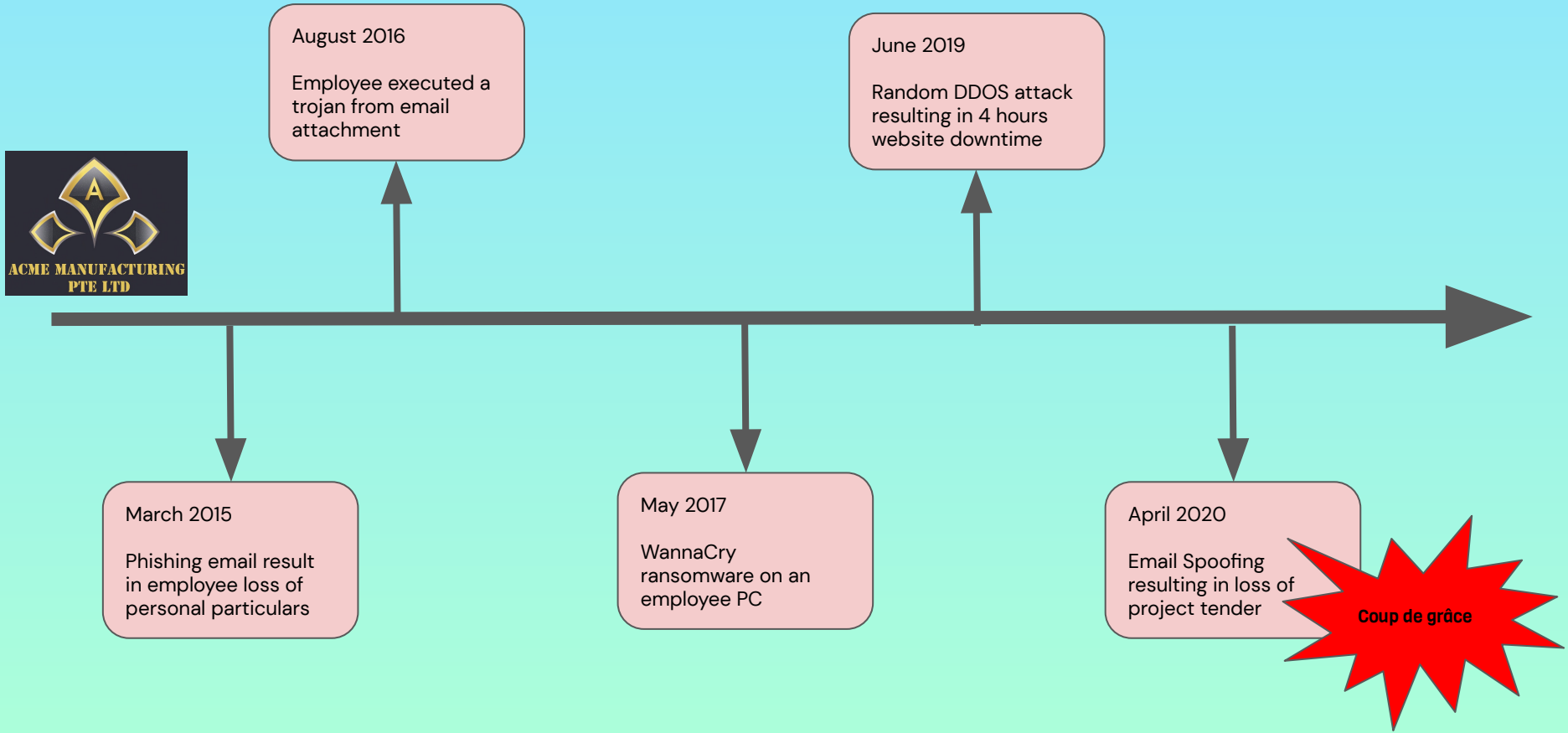
Whats Going On With The World Today

Jeremy



Jeremy

Client Sample - ACME Security Breaches History



Jeremy

Client Sample - ACME Current Infrastructure

Microsoft Server 2008 - Active Directory

Exchange Exchange 2010

FileZilla FTP and Apache Web Server running on Server 2008

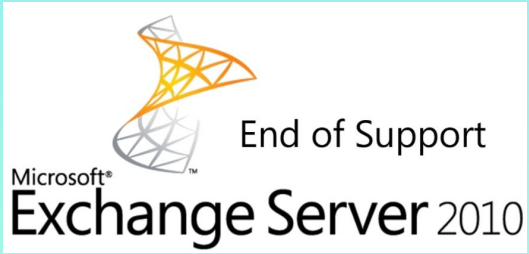
MS SQL 2008 on Server 2008

Asus Router/Firewall and Smart Switches

OpenSource PBX on Singtel ISDN

Consumer Antivirus

Windows 7 Desktops



Current Infrastructure was implemented in 2009 by a SI company without maintenance contract

Client Sample - ACME Problem Identification

Jeremy

Problem Statement

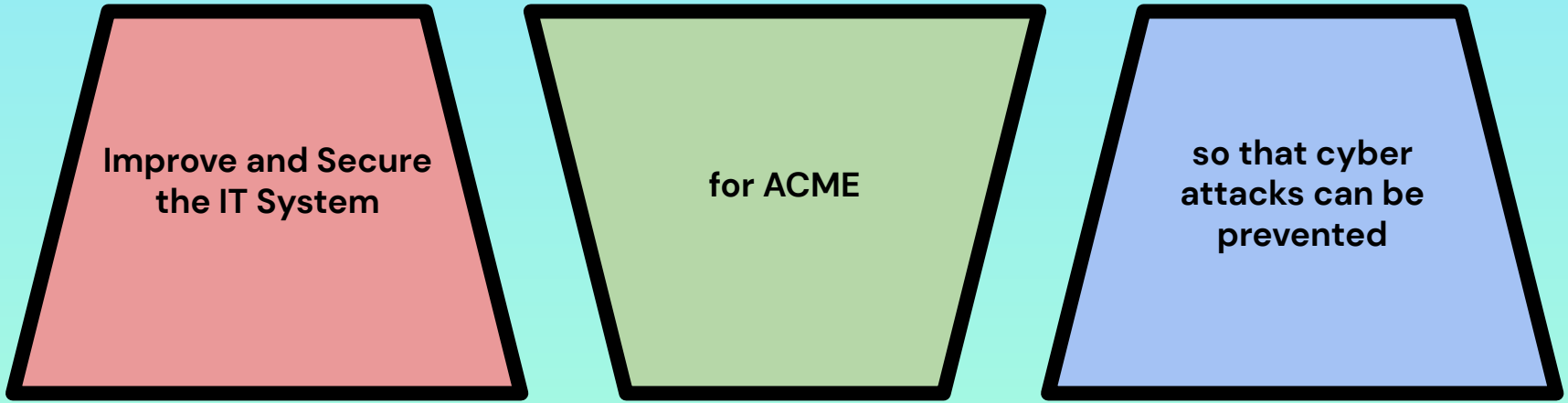
- Outdated Infrastructure
- End of Line Operating Systems
- Inadequate Email Security
- Lack of Monitoring Systems
- Consumer Antivirus & Firewall

Challenges

- Expansion of IT Budgets
- Inadequate IT Skills
- Attacks getting More Sophisticated
- Ongoing User Education on Cyber Hygiene

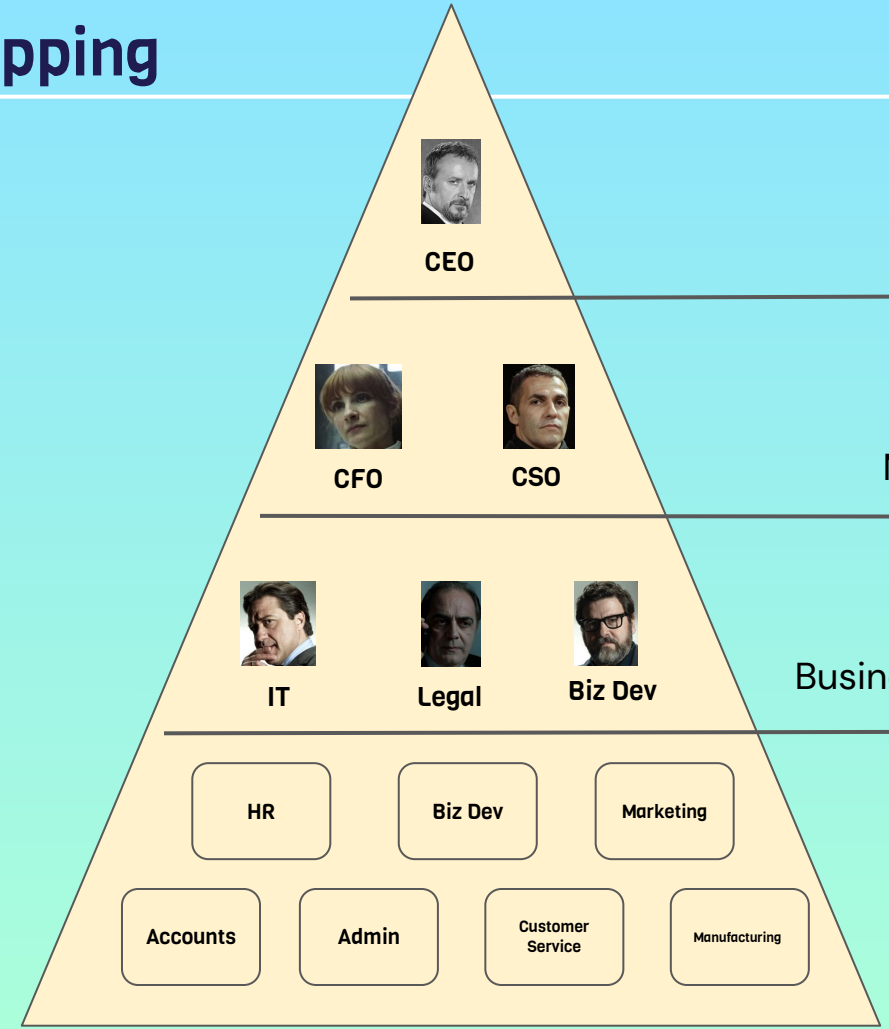
Jeremy

How Might We...



Stakeholder Mapping

Jeremy



Jeremy

User Persona 1 - The CEO

Name Luis Tamayo

Age 65

Luis is a business owner who started his own business 40 years ago, he is not good with computers and technology so he often relies on his employees to maintain the technological needs as the company progress

Motivations

Maintains the competitiveness of the company and pass on to his son

Goals

Compete with the biggest manufacturing firm in the country

Needs

Requires excellent work rate and dedication from his employees as the industry is very competitive

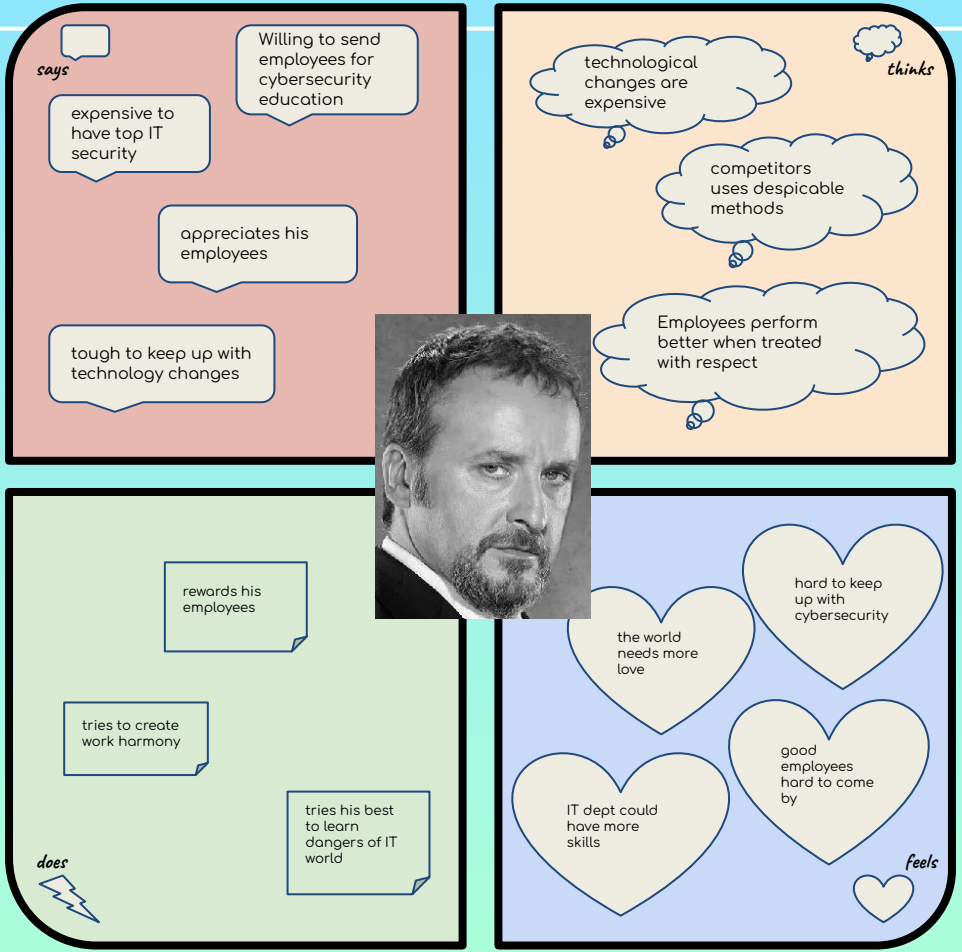
New generation to have better technological education and lead the company forward

Luis' Empathy Map

Jeremy

Luis feels that it is difficult to keep up with the changing world of IT especially cybersecurity attacks, and it generally will cost a lot to maintain top cybersecurity

He also appreciate what his employees are already doing and trying their best and is willing to invest more on IT needs and also training for employees too.



Jeremy

User Persona 2 - The Head of IT

Name Arturo Román

Age 45

Arturo is a system engineer who started off as a desktop engineer 20 years ago. He had slowly progressed to the head of IT

Motivations

Automate IT serviceability to reduce his workload

Goals

Catch up and improve on cybersecurity knowledge as he is not a specialist in this field

Needs

Hopes the company invest more on IT budget to make his life easier

Needs more IT personnel to help in the department as there are no specific person to do specific role.

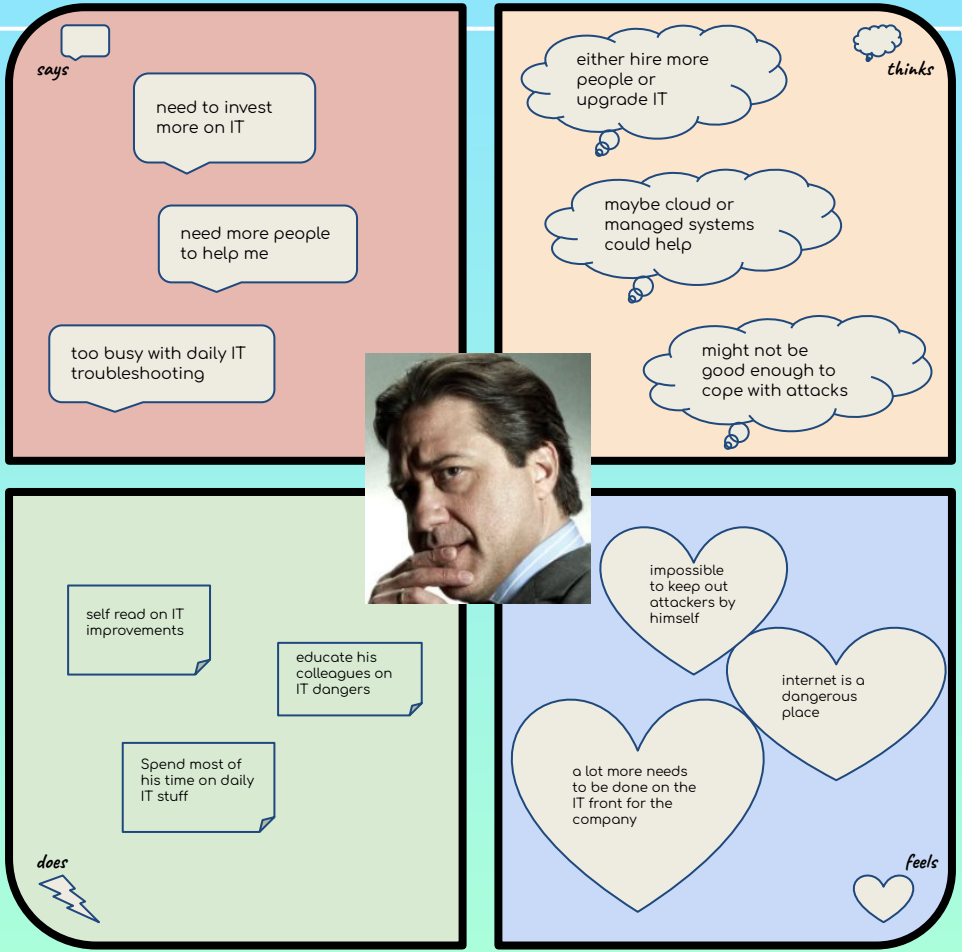
Arturo's Empathy Map

Jeremy

Arturo thinks the company had not invested enough on upgrading to the world technological changes

He also feels that he is short handed and it is impossible for him to monitor traffic or read logs with his limited time therefore maybe outsourcing some parts of IT could help

Arturo feels he tried his best but he could not prevent cyber attacks on his own



Jeremy

ACME's Pain Points

Dedicated Attention on IT Services

IT Systems Not Good Enough for Today's Standard

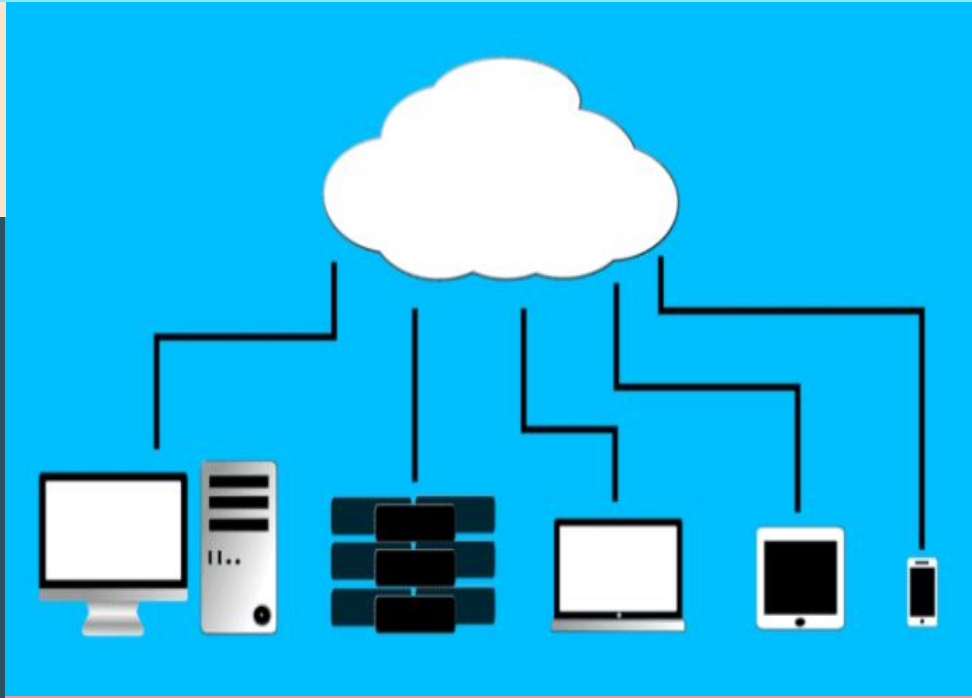
Lack of Manpower in IT

BIG Ideas for ACME/Similar Setups

Jeremy

Migration to Hosted Services

- platform as a service
- automated updates and security patches by service providers
- security defense based on service providers



Migration to Cloud Services

- infrastructure as a service
- pay on demand cost effectiveness
- redundancy and security of data

BIG Ideas for ACME/Similar Setups

Jeremy

Increase IT manpower

- specialised role for different technological needs
- more brains and innovation

IT Infrastructure Major Revamp

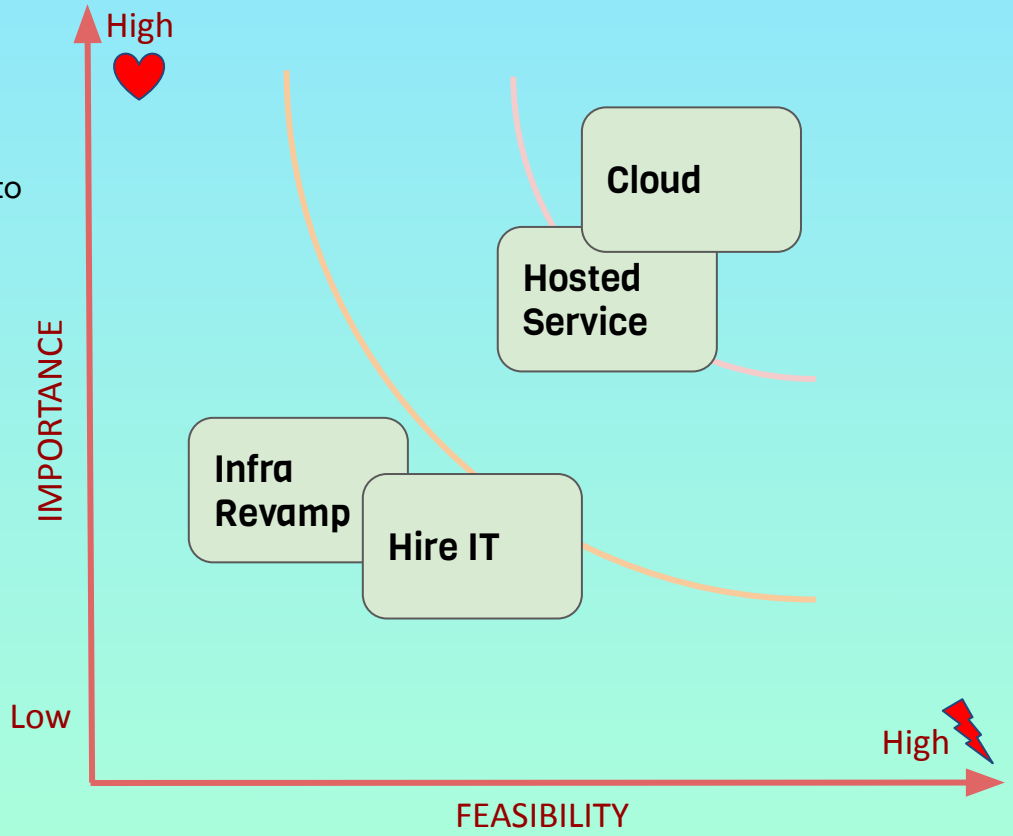
- state of the art IT Systems
- highly customized
- costly

Prioritization

Jeremy

Migration to Cloud stands out as the best solution on importance and feasibility due to its advantage on technological security

- automatic software updates
- automatic security patches
- service provider cyber defenses
- redundancy and backup
- monitored environment

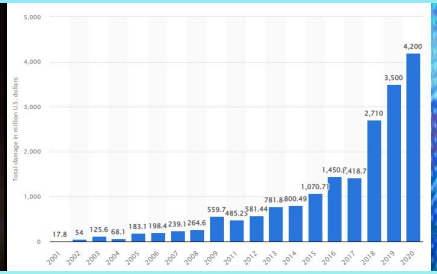


Jeremy

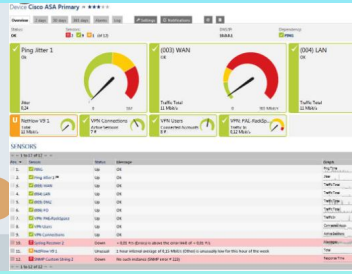
Storyboard

Arturo could not cope with the demands of technological change and targeted attacks of cyber warfare

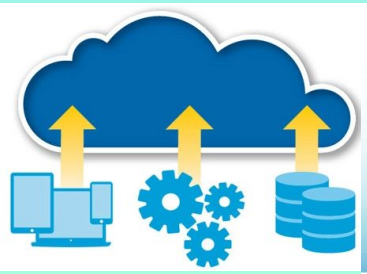
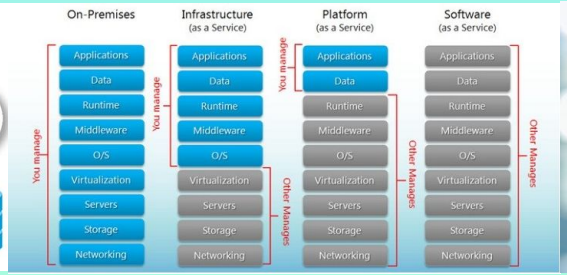








He spend most of his time troubleshooting his colleague desktop and neither does he have the time to monitor network traffic

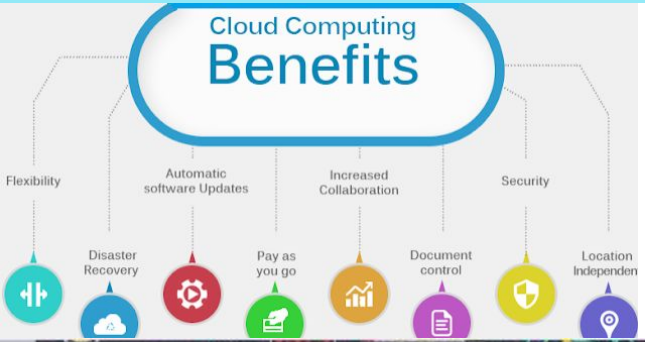


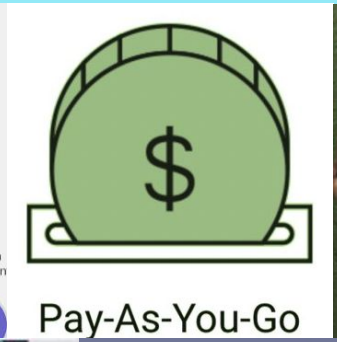
Cloud computing serverless infrastructure now reduce his workload with the service provider taking over much of the cybersecurity defenses

Storyboard

Jeremy

The pay per usage scheme reduced IT cost, and secured systems brought confidence to Luis





With the company IT system monitored by professionals,
They can now resume their manufacturing business just like the good ol’ days

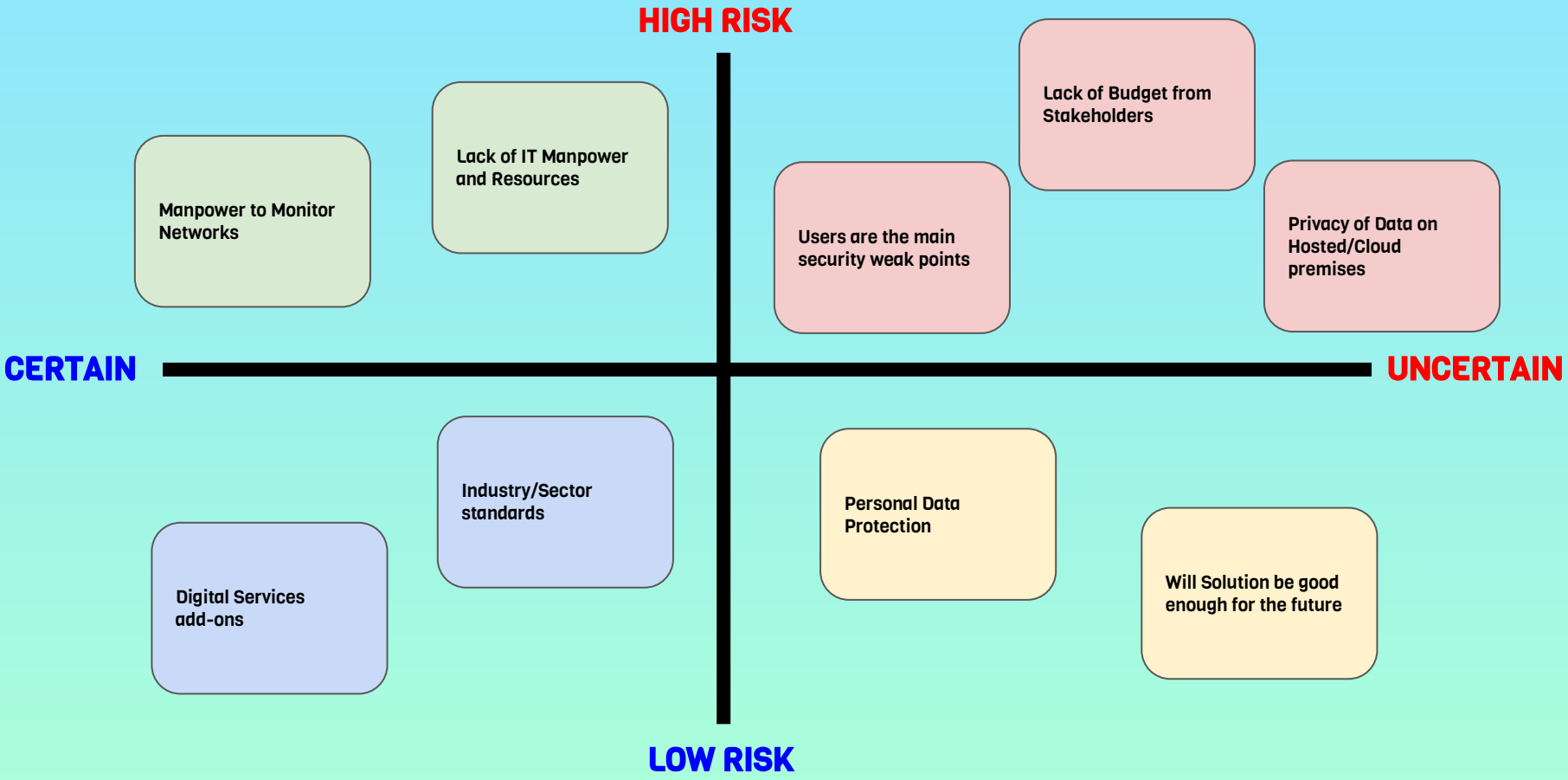
Hills

Jeremy

Who Specific user	What Specific enablement	Wow Specific market value / differentiation
Business Owners and IT Managers	can Upgrade to a Highly Secured and Closely Monitored IT system can add more Digital Services in a Highly Secured and Closely Monitored way	with good Cost Efficiency on Manpower and IT Budgets without needing to hire more IT Manpower and with a cost-effective budget

Risk & Assumptions

Jeremy



Jeremy

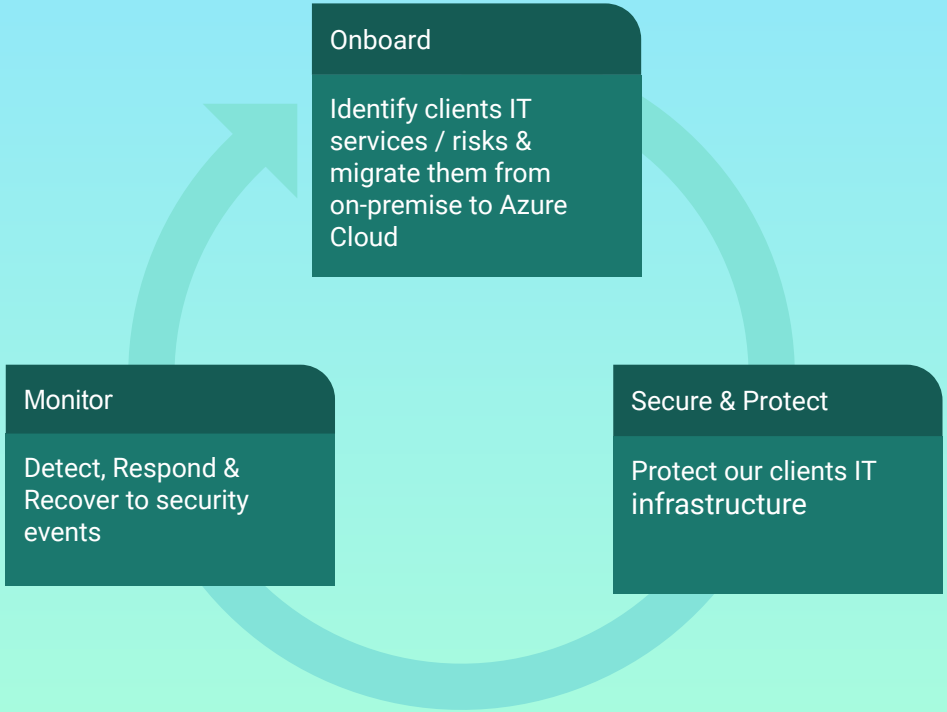
High Risk Uncertainties

Assumption Questions	Means to Resolve
Lack of Budget from Stakeholders	Minimum IaaS on pay per usage; Minimum PaaS on pay per usage
Users are the main security weak points	Users must be educated on good practise frequently
Privacy of Data on Hosted/Cloud premises	Access Control List must be well maintained; Multi Factor Authentication; Segregation of Domains

02 SOLUTION

What are we doing

Dave



Dave

How are we doing it

Migration team:

- Understand and document client's current situation
- Migrate basic services to Azure
- Set up logging for all on-premises and Azure services
- Logs go to a centralised SIEM (Microsoft Sentinel)

Security Operations Centre team:

- Monitor and investigate any security events that are detected and flagged in the centralised SIEM (Microsoft Sentinel)

Services mapping

Dave

- Active Directory
- Exchange
- Microsoft Office
- Apache Website
- FileZilla FTP
- Asus Consumer Wifi/Router

- Azure Active Directory
- Exchange 365
- Microsoft 365
- Microsoft Azure Web Apps
- Microsoft OneDrive
- Cisco Firewall/Gateway/Switch/AP connecting to Azure VPN Gateway

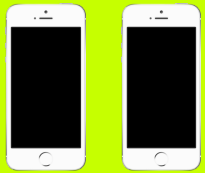
- Consumer Antivirus

- Microsoft Defender for Endpoints

- Unmonitored Web Browsing
- Singtel ISDN

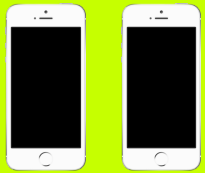
- Monitored Web Browsing
- Skype for Business

ACME Manufacturing Pte Ltd



www.acme.com

ACME Manufacturing Pte Ltd



www.acme.com

Dave

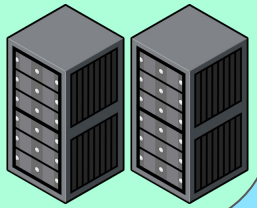
WAN GATEWAY

Microsoft Office 365
Microsoft OneDrive
Skype for Business

General Web Browsing

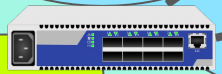
CLOUD INFRASTRUCTURE

Azure Active Directory
Azure SQL Database
Azure Web Apps
Azure Defender
Azure Sentinel
Azure IoT Suites



WAN

VPN to Microsoft Azure



ACME Manufacturing Pte Ltd

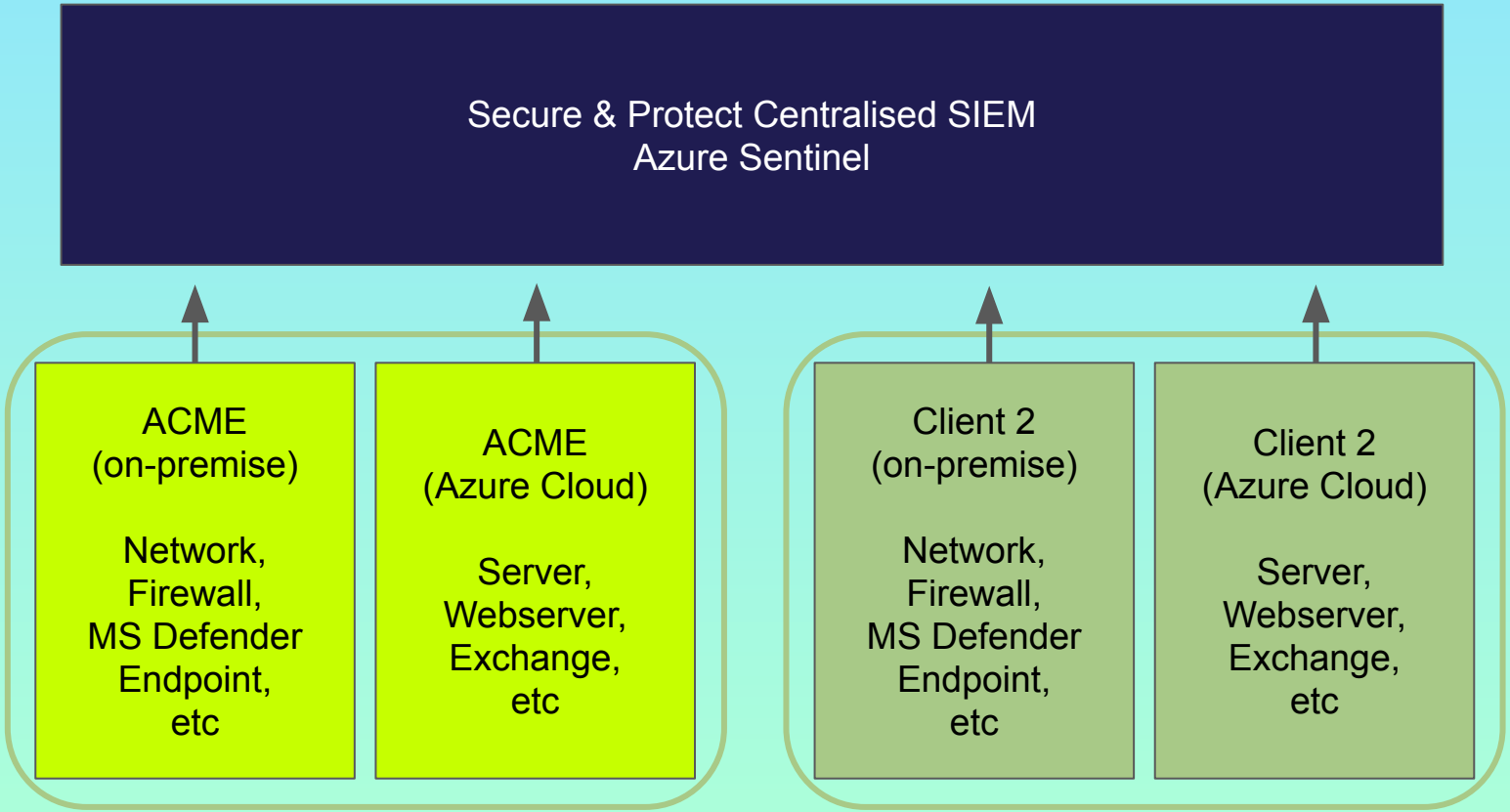
Dave

Security tools

- PC/Laptops – Microsoft Defender for Endpoints
- Mobile Phones – Microsoft Defender ATP
- Azure Cloud – Azure Defender
- SIEM – Azure Sentinel
- IOT – Azure IOT Suites
- Phones – Skype for Business
- WAN – Cisco Firewall and VPN

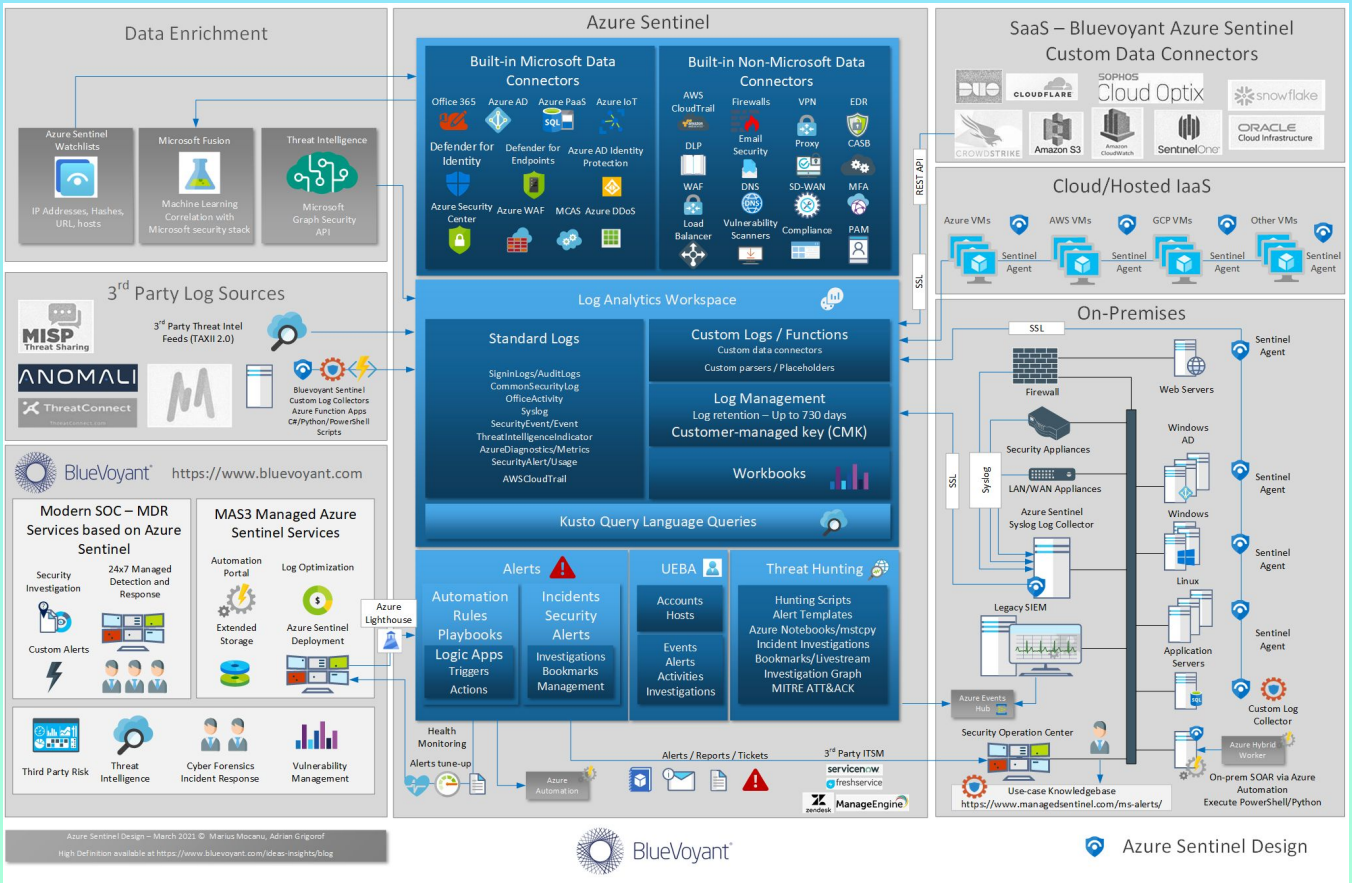
Centralised SIEM

Dave



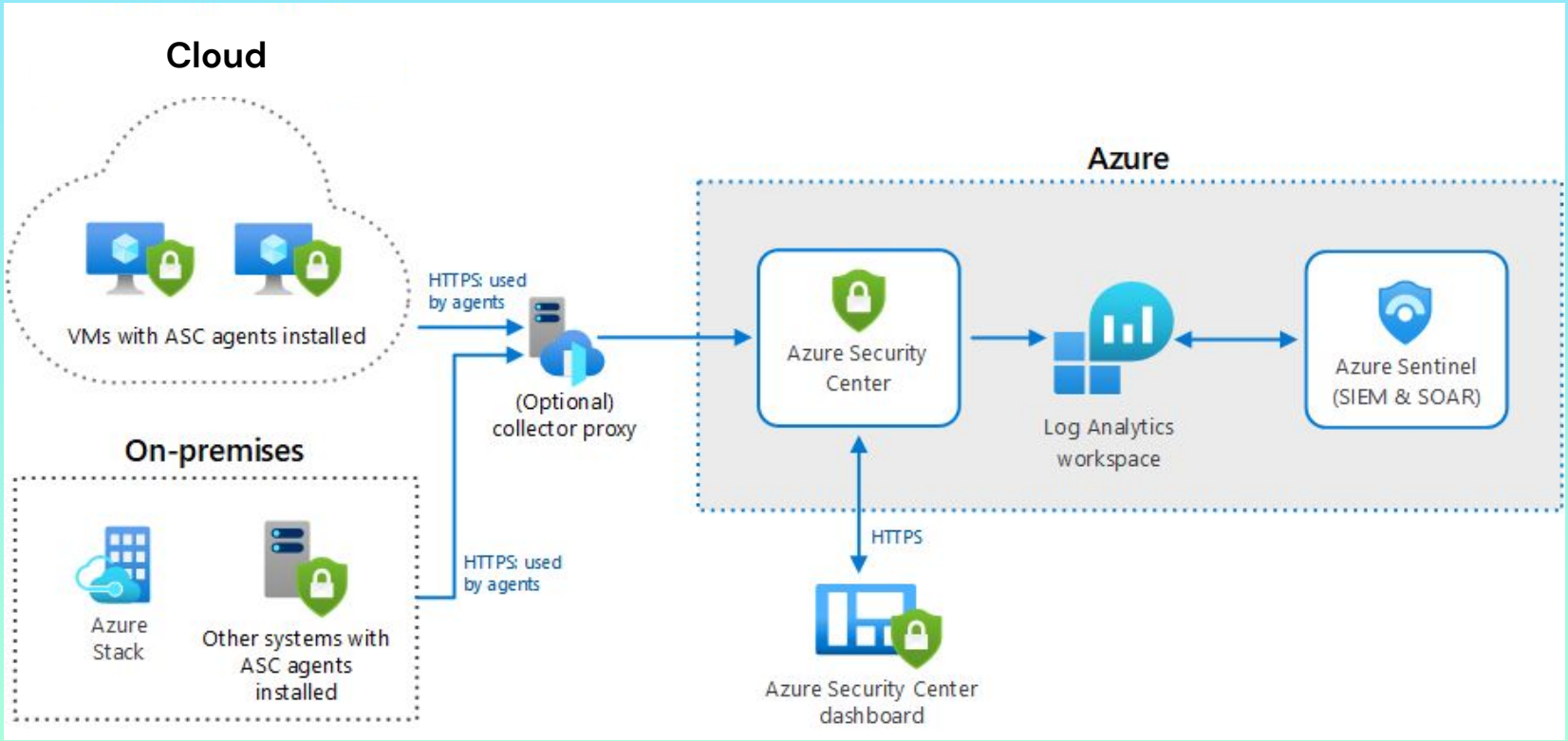
Architecture

Dave



Architecture

Dave



Dave

Client Onboarding Process

- Asset inventory
- Document current users / identity mgmt
- Document data / data mgmt
- Document needs
- Document current processes
- Assess and prioritise current security risks

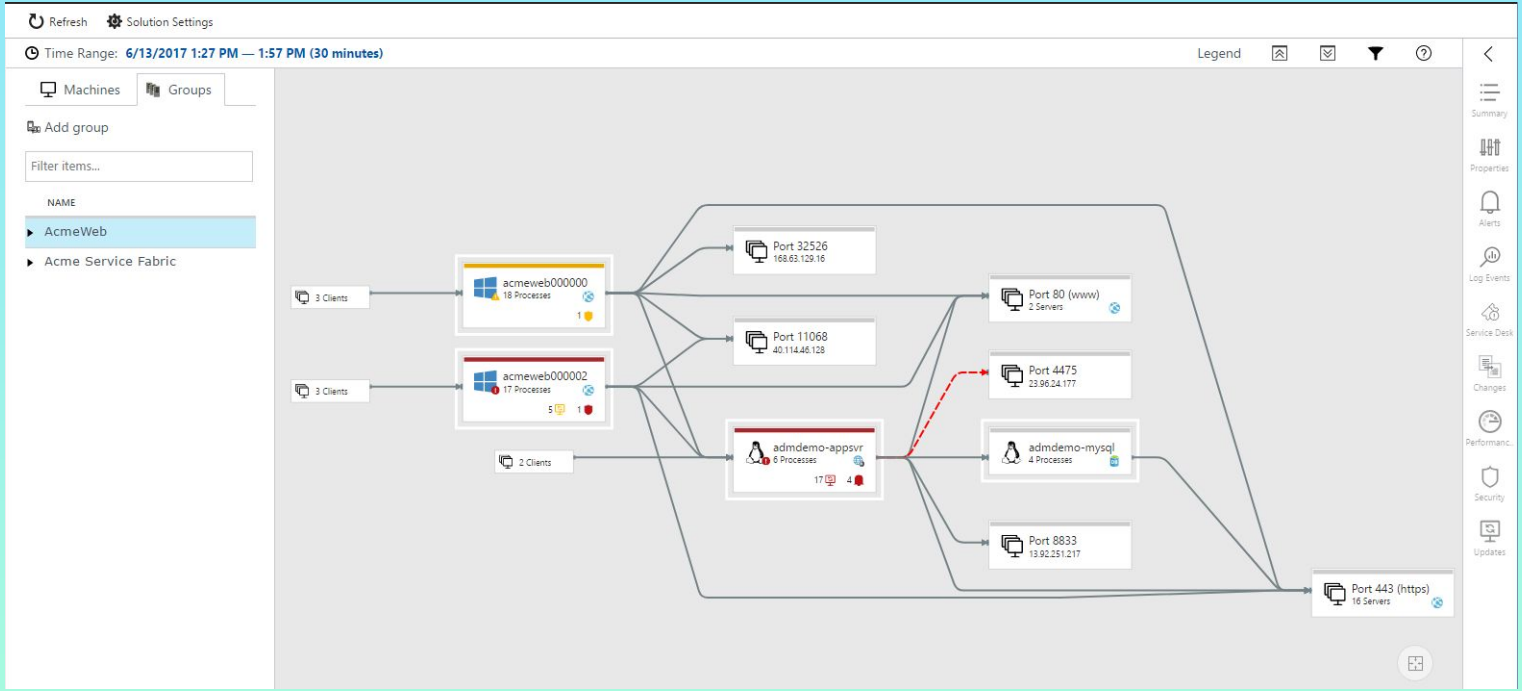
- Setup Identity management
- Setup network monitoring
- Setup patching and maintenance processes
- Setup backup processes
- Setup network intrusion protection
- Setup incident response plan
- Setup staff training plan

- Setup endpoint protection
- Lift and shift AD servers, Exchange, etc
- Migrate websites / DB to Azure
- Customise comms plans

- Evolve security plan as the client matures
- Migrate monolithic apps to microservices

Migration tools

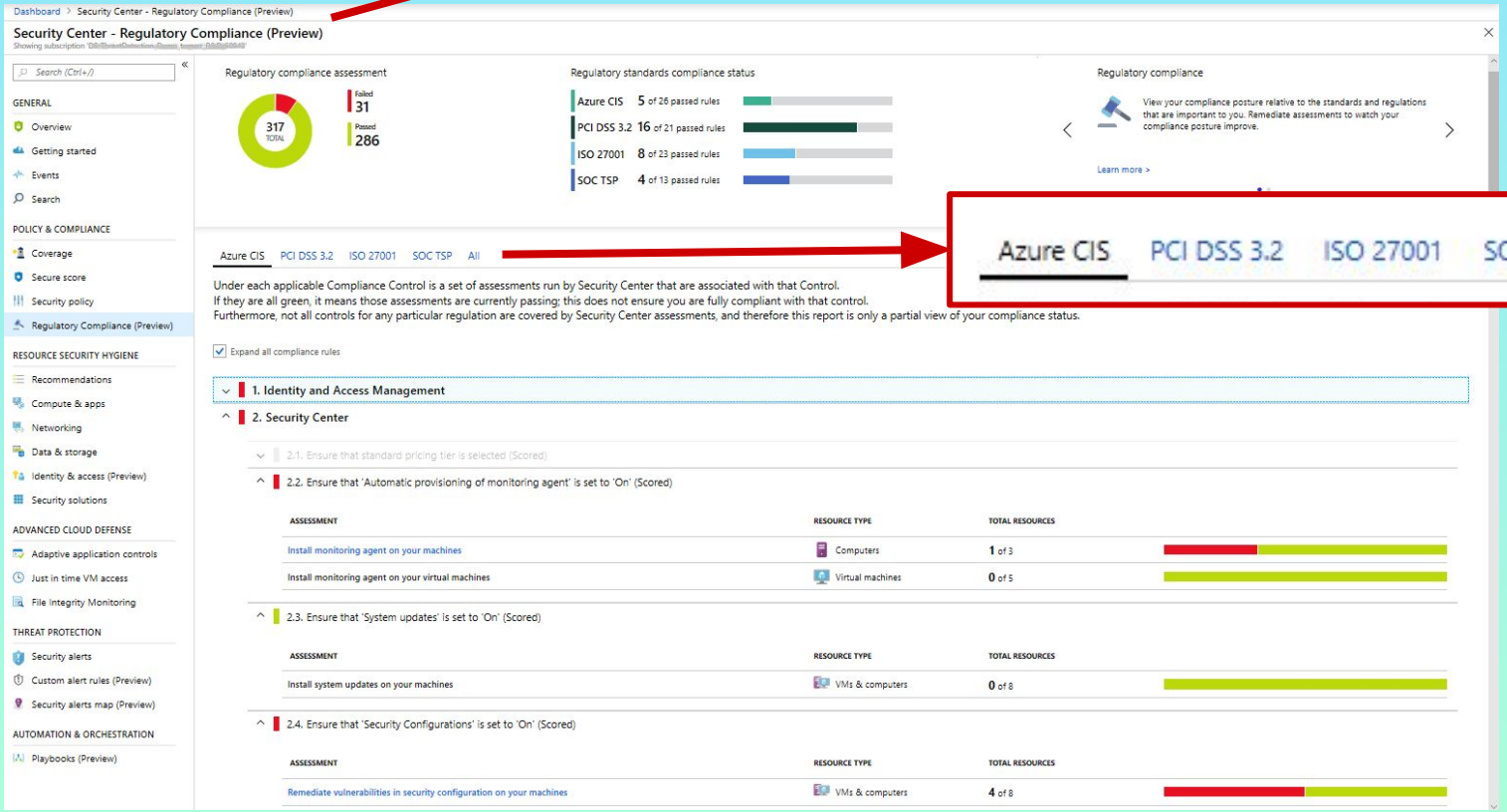
Dave



Microsoft Service Map -> Azure Migrate

Dave

Reports and dashboards



Why Azure improves cybersecurity / resilience

Dave

Security of the Cloud – Security in the Cloud

Control

Easier access and control.
Blueprints and easier / faster patching.
Central / secure place for logs.

Performance

Reliability - HW.
DDoS.
Better security with web microservices.

Resilience

Reduce risk of theft / fire / loss of servers, etc.
BCP / backup recovery.

Scalability

We (MSP) can manage multiple clients efficiently.

Alternative SIEMs

Dave

08 NIST Framework

Why is NIST Framework is important
The Framework Core

Establishes a Common Language

Matt

	Function
What process & assets need protection?	Identify
What safeguards are available?	Protect
What techniques can identify incidents?	Detect
What techniques can contain impacts of incidents?	Respond
What techniques can restore capabilities?	Recover

- Describes desired outcomes
- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

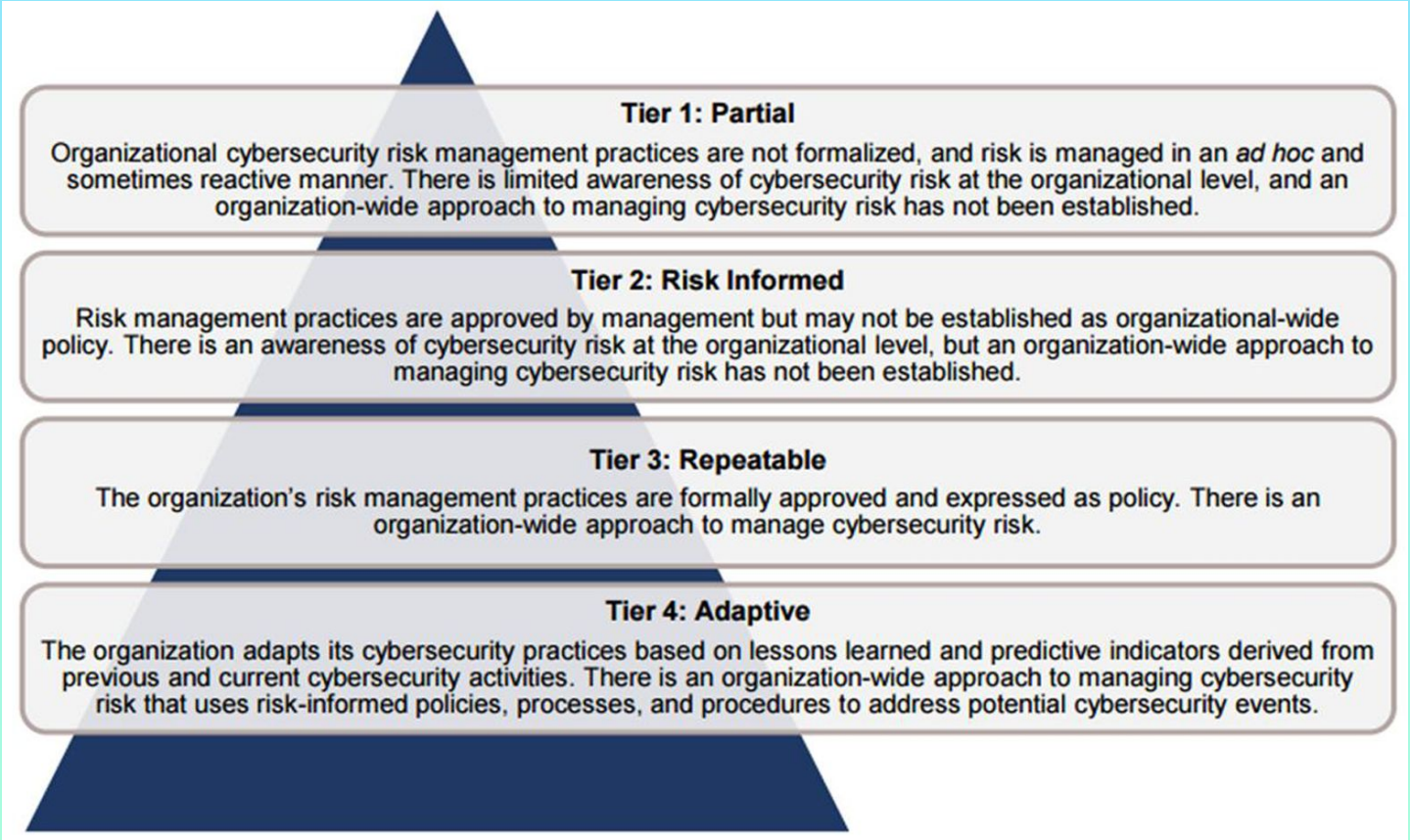
Framework Core

Matt

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Matt

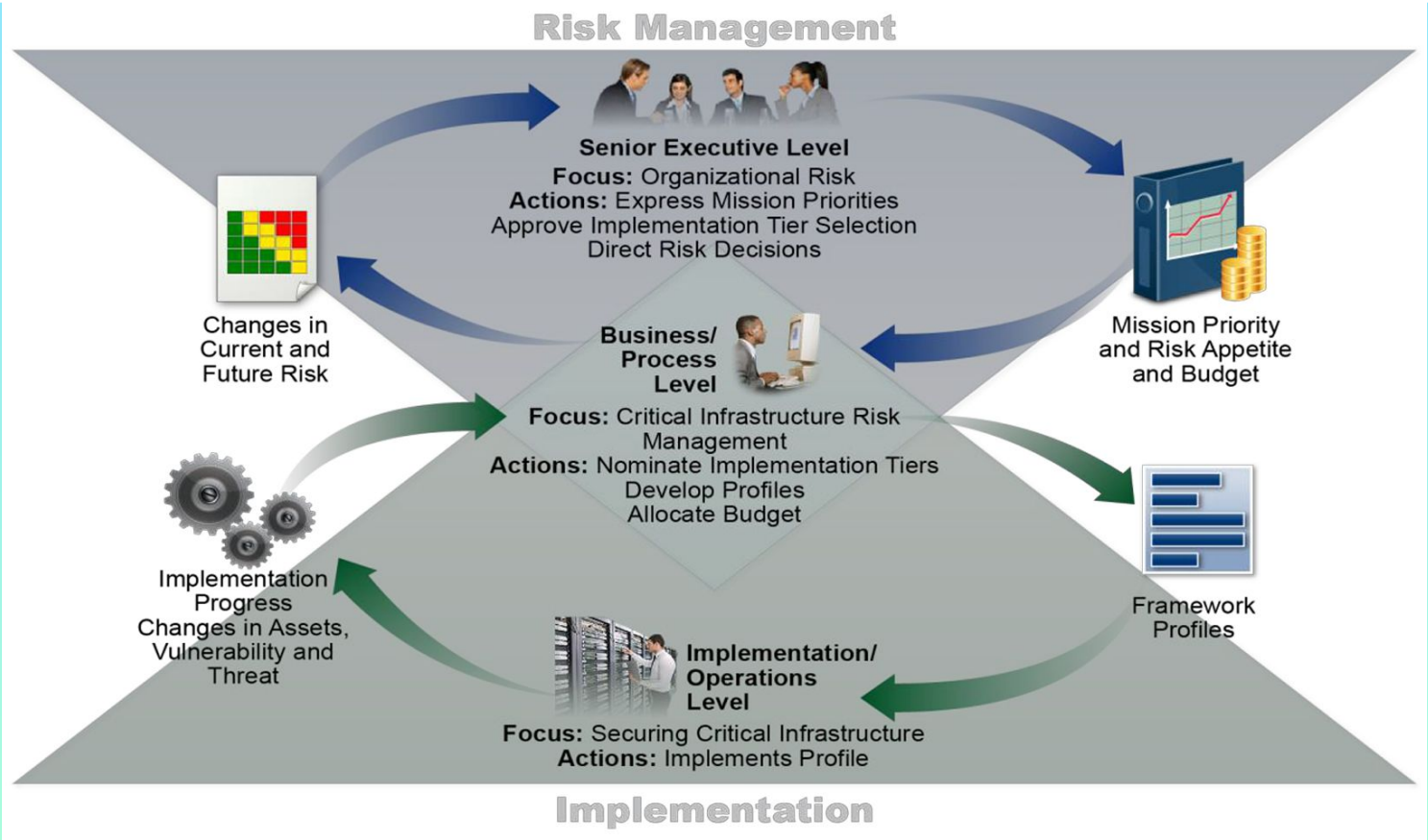
Framework Implementation Tiers



Provide context for how an organization views cybersecurity risk and the processes in place to handle the risks

Matt

Framework Profile



Notional Information and Decision Flows within an Organization

Matt

IDENTIFY

Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.

1) **Maintain hardware and software inventory – MVE 1**
   -Make a list of all equipments, software & data ACME use including laptops, smartphones, tablets & point-of-sales devices.

2) **Establish policies for cybersecurity that include roles and responsibilities – MVE 1**
   -Role & responsibilities for employees, vendors & anyone else with access to sensitive data.

3) **Document information flows – MVE 1**
   - Steps to take to protect against an attack & limit the damage if one occurs.

4) **Identify threats, vulnerabilities, and risk to assets – MVE 1 & MVE 2**

5) Identify critical enterprise processes and assets – MVE 2

NIST Cybersecurity Framework -IDENTIFY

Matt

Focus on laying groundwork to develop knowledge of organisation

1) Asset Management

Use Azure Migrate to efficiently map out all existing equipments and softwares of ACME.

2) Establish policies

ACME expectations for cybersecurity activities and how they support critical enterprise processes.

3) Data governance

- Type of data collected
- Data location and flow
- External vendors accessing the data

4) Risk Assessment

- Identify possible vulnerabilities
- Initial benchmark and
- Reloop identified, assessed, and documented

Matt

PROTECT

Develop and implement the appropriate safeguards to ensure delivery of services.

1) **Manage access to assets and information - MVE 1**
   - Control who logs on to your network and uses your computers and other devices.

2) **Protect sensitive data - MVE 1**
   - 1) Encrypt sensitive data, at rest & in transit.
   - 2) Use security software to protect data.
   - 3) Update security software regularly, automating those updates if possible.

3) **Conduct regular backups - MVE 1**

4) **Train users - MVE 1**
   - Train everyone who use your computers, devices and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

5) Securely protect your devices - MVE 2

6) Manage device vulnerabilities - MVE 2

NIST Cybersecurity Framework -PROTECT

Matt

Focus on appropriate safeguard and ensure critical service remain available

1) Identity Management

- Create unique accounts
- Authenticate users
- Manage and track physical access
- Remove access

2) Data Security

- Data encrypted
- Software and hardware integrity
- Securely delete of Data

3) Backups

- Automate the backup on Azure
- Offline backups

4) Awareness & Training

- Cybersecurity policies and procedures
- Construct Risk Scenarios

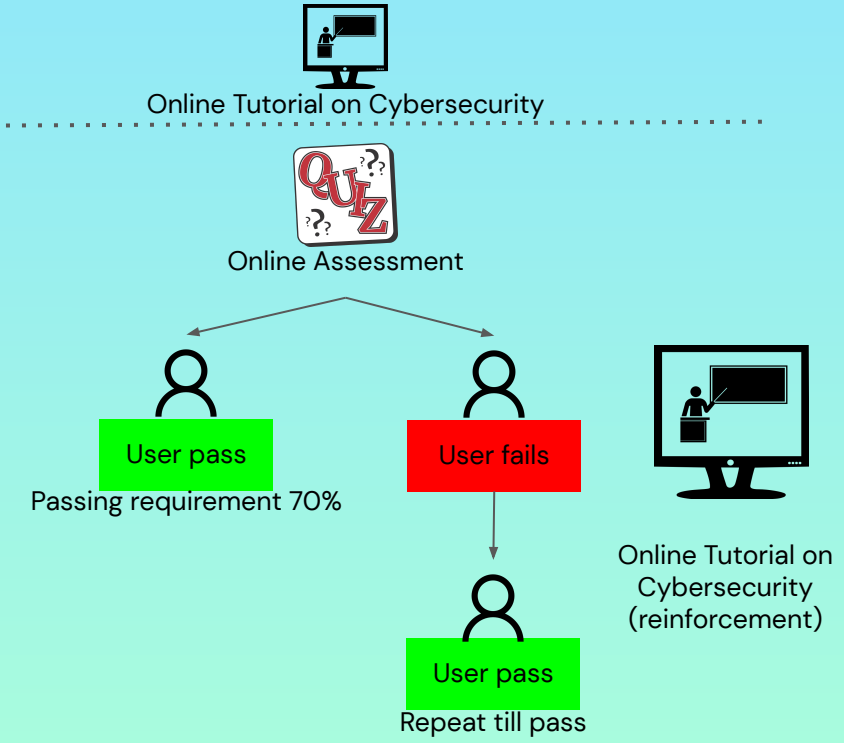
2. **PROTECT**

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

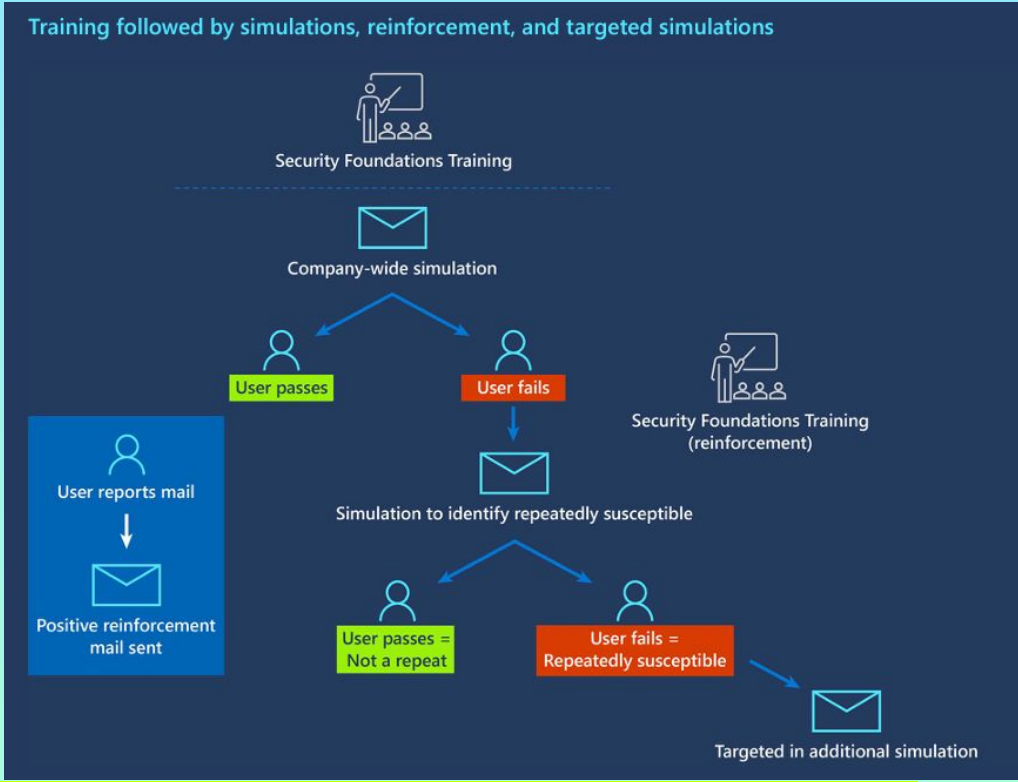
Matt

Security Foundation Training (Workflow)

1) Assessment for all employees that required access



2) Construct Risk Scenarios - Simulation on phishing email



Beyond detection & protection, it is imperative that we cultivate a security-conscious culture

DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

1) Maintain and monitor logs – MVE 1

- 1) Monitor computers for unauthorized personnel access, devices (eg USB drives) and software
- 2) Check network for unauthorized user or connections.
- 3) Investigate any unusual activities on network or by staff.

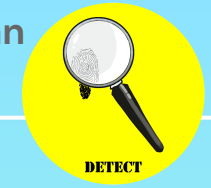
2) Test and update detection processes - MVE 2

3) Know the expected data flows for your enterprise - MVE 2

4) Understand the impact of cybersecurity events - MVE 3

NIST Cybersecurity Framework -DETECT

Bryan

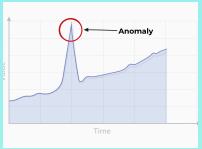


Focus on operational activities to identify cybersecurity events

Anomalies and Events

Establish a baseline of ACME's network operations and expected data flow for users and systems,thus establishing its expected network behaviors.

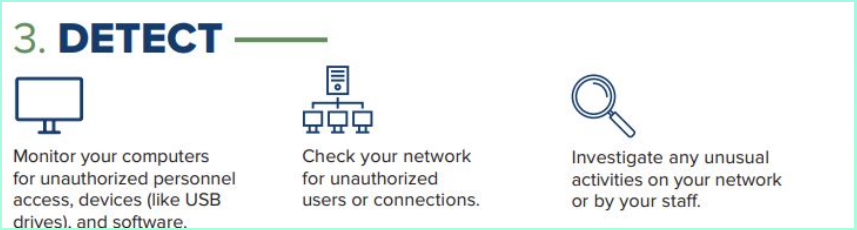
Establish Incident Alert Thresholds according to ACME's Senior Executives needs



Security Continuous Monitoring

S&P's SOC Team will provide ACME constant monitoring of its network activities thru our Centralized SIEM on Azure Sentinel.

Flag and Updates ACME upon detection of any abnormal personnel activities



Detection Processes

Establish with ACME how Event Detection will be communicated to them

Established well defined roles and responsibilities upon detections to ensure accountability

Bryan

RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

1) Ensure response plans are updated - MVE 1 & MVE 2

2) Coordinate with internal and external stakeholders - MVE 1

- Notifying customers, employees and others whose data may be at risk.
- Investigating & containing an attack.
- Keeping business operations up & running.
- Updating cybersecurity policy & plan with lesson learned.
- Reporting the attack to law enforcement & other authorities.
  - SingCERT Cyber Incident Reporting, Singapore Police Force & PDPC
- Prepare for inadvertent events that may put data at risk.

3) Ensure response plans are tested - MVE 2

NIST Cybersecurity Framework -Response

Bryan

Focus on taking action in the case of cybersecurity incident

Communications/Response Planning

-Establish Response Plan: Develop and implement effective response operation procedures with ACME Senior Executives

-Train ACME personnel in their roles and order of operations when an incident had occurred: how to communicate with internal and external stakeholders and coordinate a consistent response to public

-Generate Incidents report that are easy to understand for ACME Senior Executives, assist in crafting reports to authorities.

Analysis, Mitigation & Improvement

-S&P to investigate detected notifications from Sentinel quickly and inform ACME, quickly contain affected Data and mitigate damages.

-Provide feedback and suggestions to improve Response Plan as well as future Training Lessons.

Bryan

RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security event.

1) **Communicate with internal and external stakeholders – MVE 1**
   - Keep employees and customers informed of the response and recovery activities.
   - Repair and restore the equipment and parts of our network that were affected.

2) **Ensure recovery plans are updated – MVE 1 & MVE 2**

3) Manage public relations and company reputation – MVE 3

NIST Cybersecurity Framework -Recover

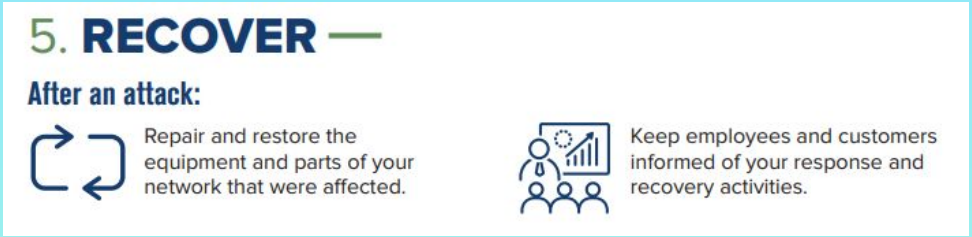
Bryan

Focus on restoring capabilities and services from security incidents

Recovery Planning

-Establish Basic Recovery Plan with ACME's Senior Executive

-Perform Recovery Plan for ACME during or after the incident, depending on severity and ACME's decision



Communication

-Keep ACME personnel informed of the recovery process

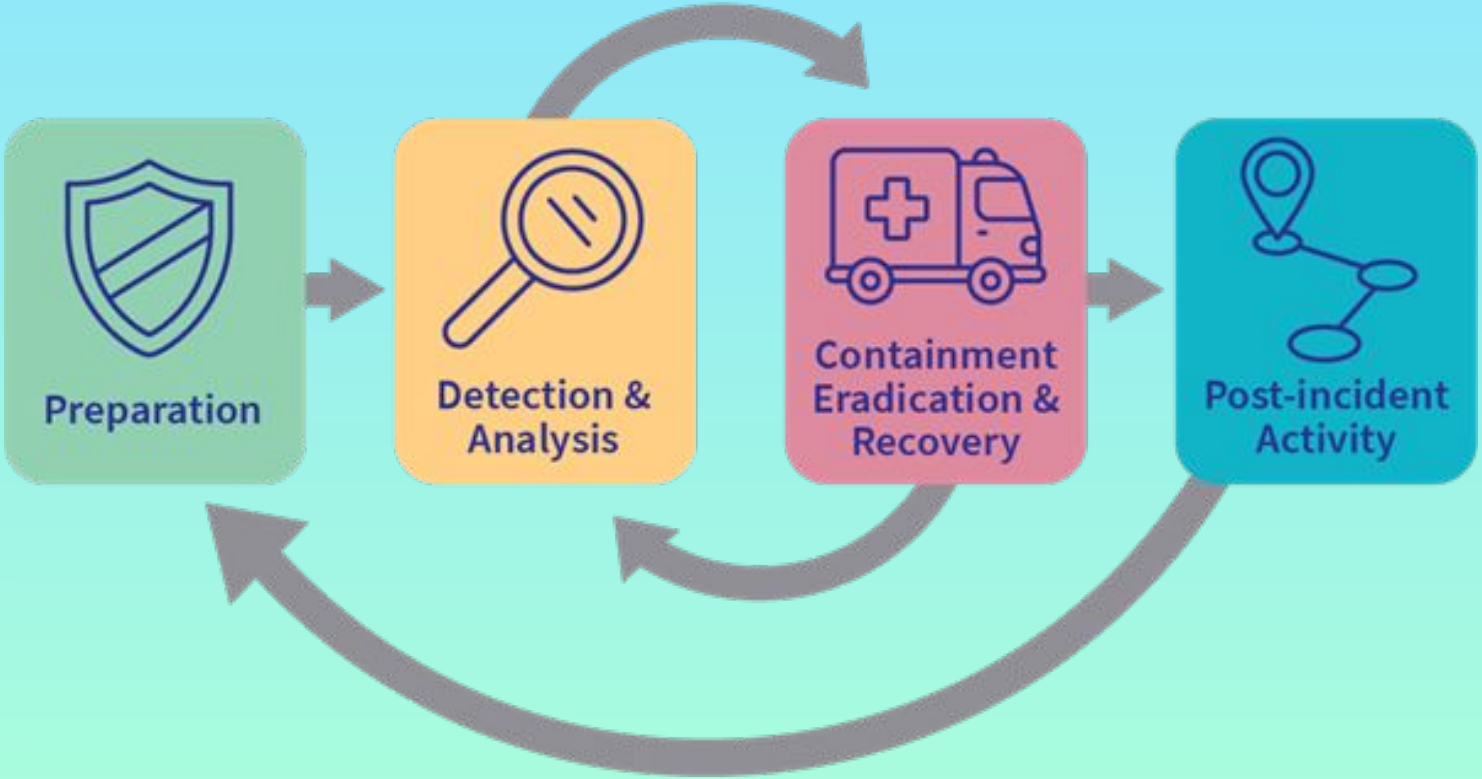
-Provide updates and advises to ACME Senior Executives on how to communicate Recovery activities to stakeholders, repairing damages to its reputations and public relations

Improvements

-Review Recovery Plans to incorporate lessons learned: etc if loss of data occurred/equipments become unrecoverable, and update future Strategies and Personnel Training Lessons Plan.

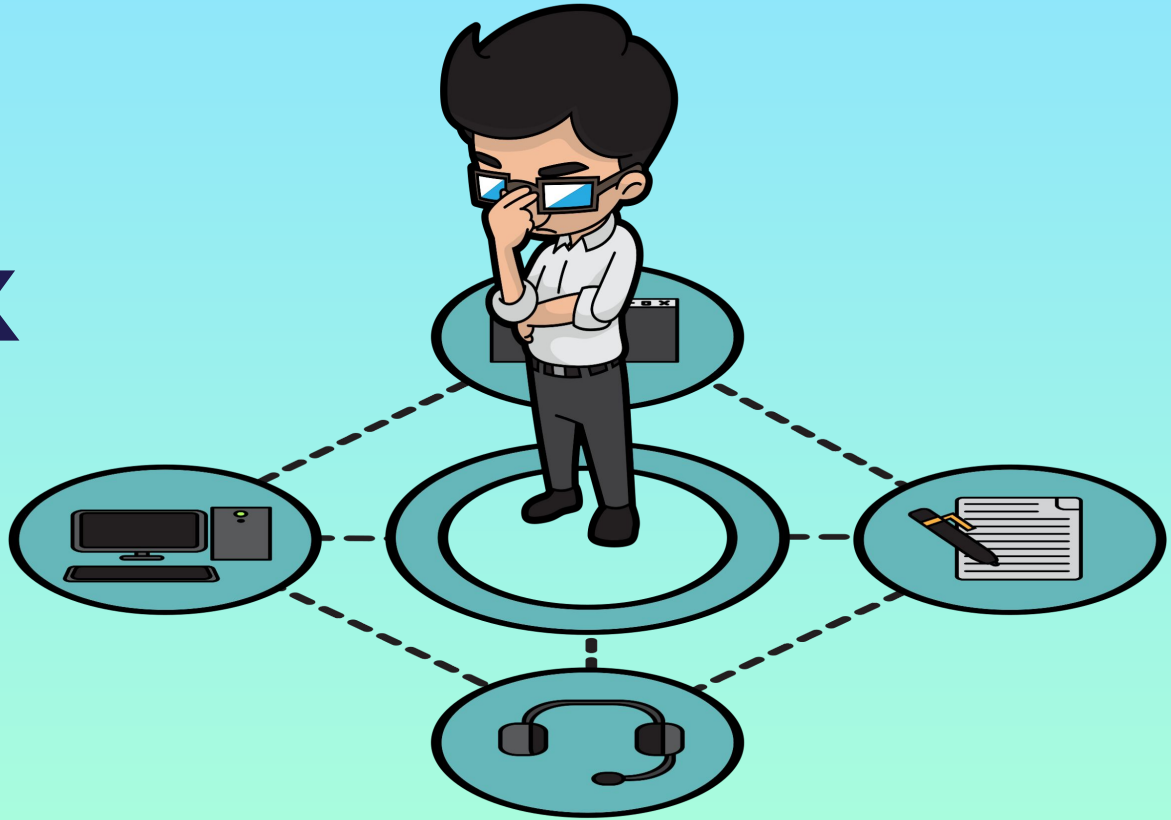
Bryan

Cyber Incident Response Cycle



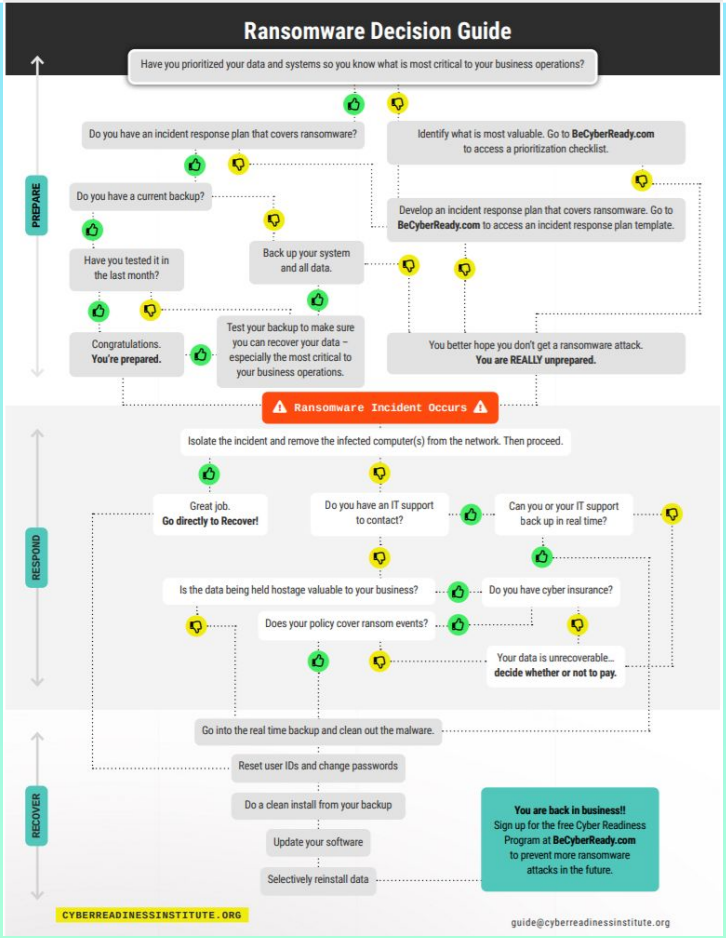
Bryan

Playbook



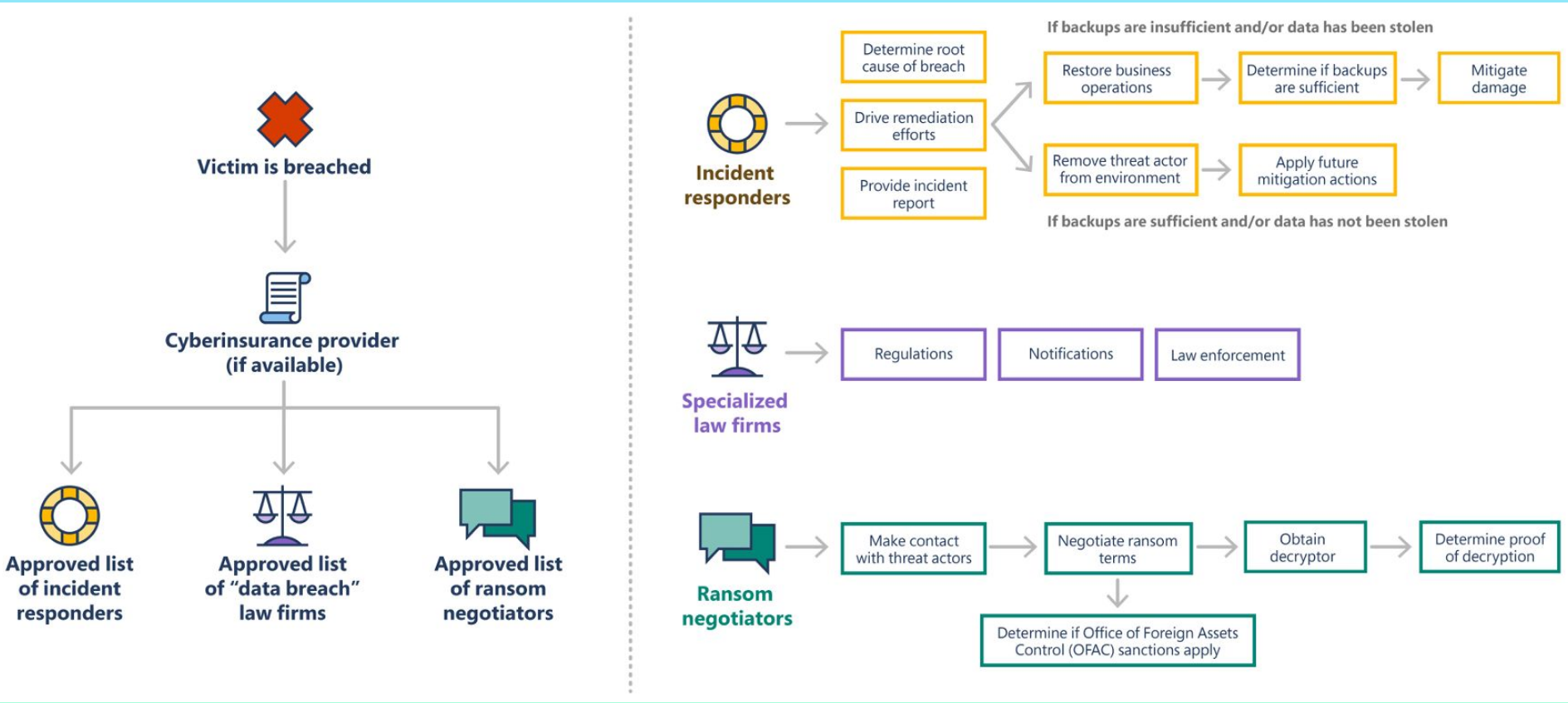
Ransomware Playbook

Bryan



Bryan

Stakeholders and roles involved in post-breach response



04 BUSINESS PLAN

Minimum Viable Environment

Bryan

Jul 2022
MVE 1

1) Maintain hardware & software inventory

2) Document information flows

3) Basic identify threats, vulnerabilities, and risk to assets

4) Establish policies for CS that includes roles and responsibility

5) Manage access to assets and information

6) Protect sensitive data

7) Establish a response plan

8) Conduct regular backups

9) Establish a recovery plan

10) Train User

11) Maintain & monitor logs

12) Coordinate with internal & External stakeholders

13) Communicate with internal & External stakeholders

Dec 2022
MVE 2

1) All of MVE 1 plus;

2) Identify critical enterprise processes & assets

3) Update identify threats, vulnerabilities, & risk to assets

4) Securely protect your devices

5) Test & update detection processes

6) Know the expected data flows for your enterprise

7) Ensure response plan are tested

8) Ensure response plan are updated

9) Ensure recovery plan are updated

Jun 2023
MVE 3

1) All of MVE 1 & 2 plus;

2) Understand the impact of cybersecurity events

3) Manage public relations & company reputation

Dec 2023
MVE 4

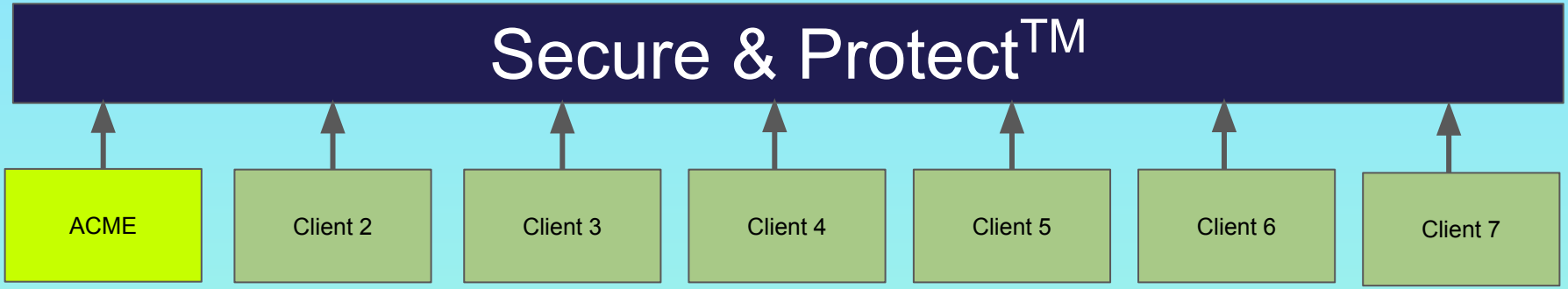
1) All of MVE 1, 2 & 3 plus;

2) Multi cloud environment eg AWS, GCP etc

3) Upscaling, adding microservices etc

Secure & Protect™ Business Model

Bryan



Cost / revenue for Secure & Protect™ ;

1) Azure costs are passed through to client
2) Implementation fee / migration fee
3) Tiered Subscription Fee

Secure & Protect™ - Upscaling

Bryan

1) We will have a couple of implementation consultants for the Migration team

2) We start off with a small team for the SOC (not 24/7)

3) Secure & Protect™ aims to expand our operations team to comprehensive SOC operations

4) Operating 24/7 across the globe by having regional manpower

5) Expansion to overseas market

Bryan

05 Conclusion

References

Bryan

1) Microsoft FY2021 Microsoft Digital Defense Report – URL
2) Ransomware Playbook - Cyber Readiness Institute – URL
3) Internet Crime Report 2020 by Internet Crime Complaint Center (IC3) – URL
4) Cybersecurity Framework NIST – URL
5) Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide – URL
6) Azure Sentinel Design Update - Managed Sentinel – URL

Q & A


WELCOME
ON BOARD