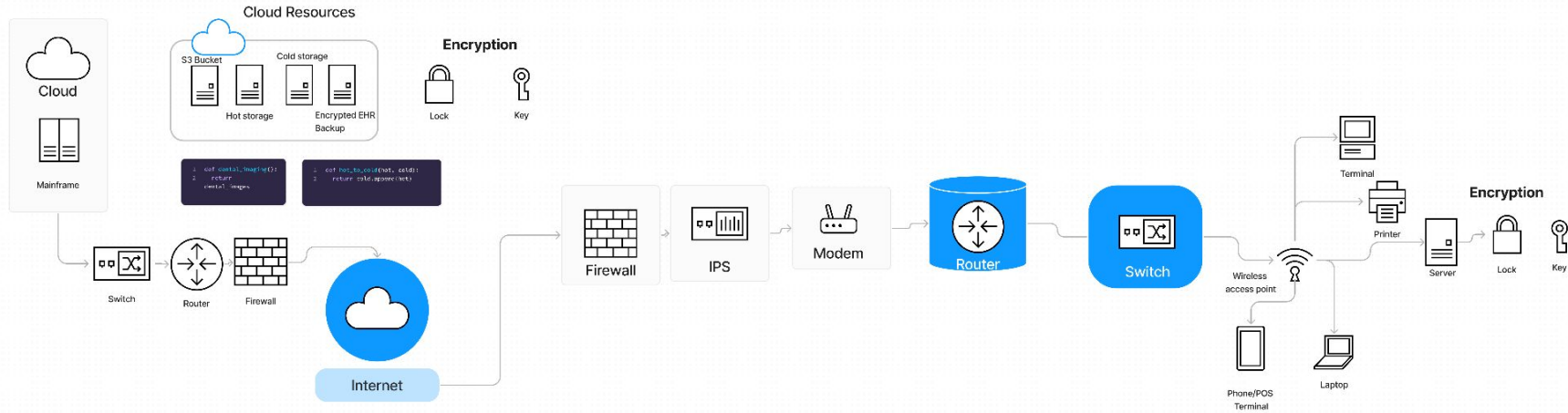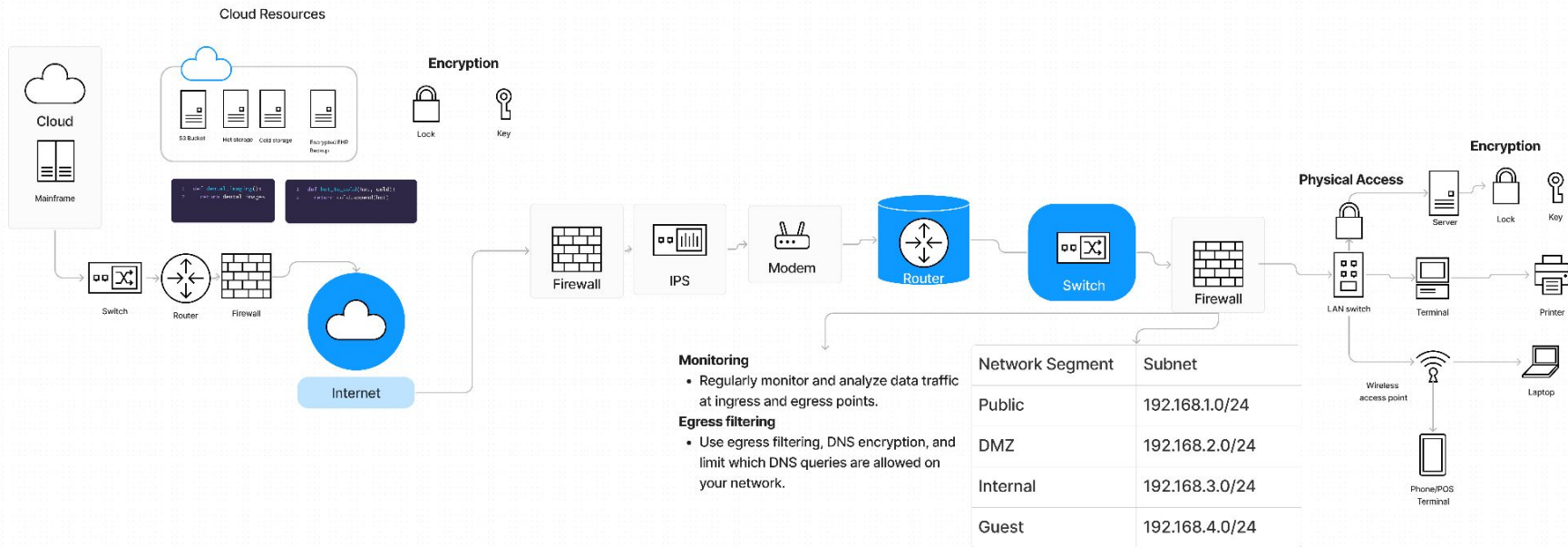# Defence Strategy

●●●

Improvements to security posture

Current Architecture

Target Architecture

Infrastructure Components

Enterprise Firewall:

- It controls traffic flow, filters out malicious traffic, and enforces security policies.
- Segmentation divides a network into smaller each with its own set of rules and security controls.
- This segmentation limits the impact of security breaches and prevents their spread to other areas of the network.
- An enterprise firewall with network segmentation capabilities integrates with other security tools, such as intrusion detection systems (IDS) and security information and event management (SIEM) systems.

Security Information and Event Management (SIEM) System:

- SIEM collects and analyzes security events from various sources.
- It provides a centralized view of security events, enabling faster response times and improved security posture.

Physical Access Control:

- Prevents unauthorized access from external or internal threats.

Roles and Responsibilities

	Patch Management	Network Security	Security Training
Responsible	IT Operations	IT Security	HR
Accountable	CIO	CISO	CISO
Consulted	IT Security	IT Operations	IT Security
Informed	All Employees	All Employees	All Employees

Documentation Requirements

➔ Firewall Configuration
   ◆ Document and implement and manage firewall rules to control traffic flow.
➔ On-Boarding Security Training
   ◆ Document employee training on security best practices.
➔ Ingress/Egress Rules
   ◆ Establish policies for controlling data movement.
➔ Multi-Factor Authentication (MFA) Setup
   ◆ Document the implementation of MFA to add an extra layer of security.
➔ Patching Protocol
   ◆ Document a regular patching schedule to address vulnerabilities.

Cost Analysis

Enterprise Firewall $200-$500 *once*
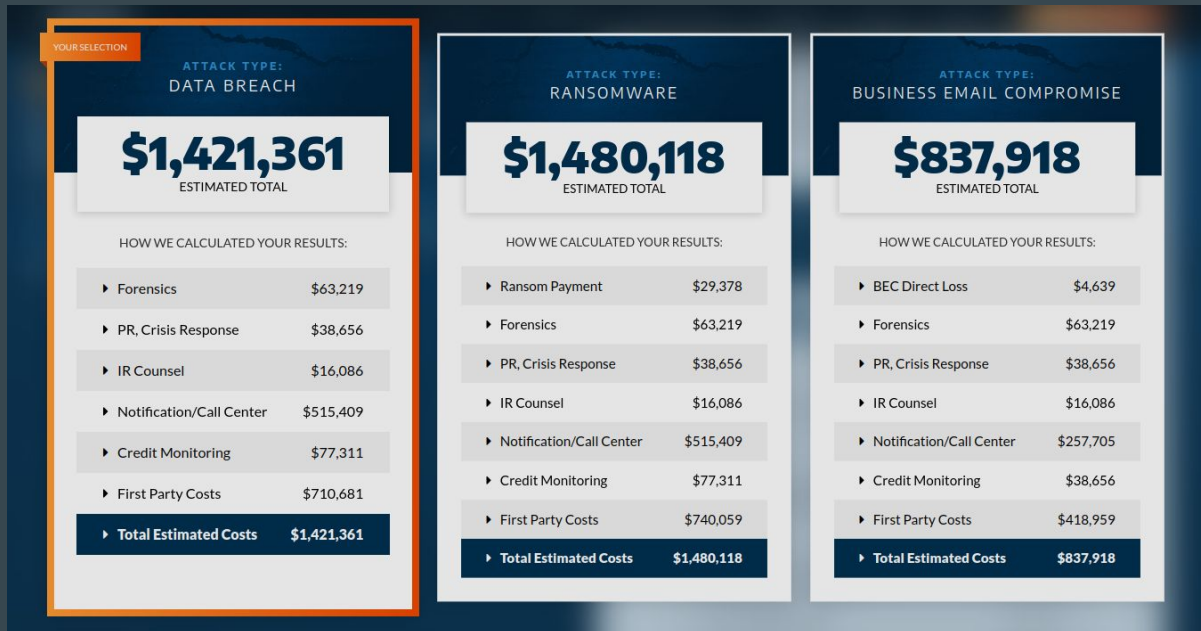
Patch Management $350-$600 *annually*

Security Training $500-$1000 *annually*

Physical Access $50-$100 *once*

Total $1100-$2200

IBM Estimates a $4.45 million average cost of attack in 2023.

Arctic Wolf Breach Estimate

YOUR SELECTION	ATTACK TYPE: DATA BREACH		ATTACK TYPE: RANSOMWARE		ATTACK TYPE: BUSINESS EMAIL COMPROMISE	
	$1,421,361 ESTIMATED TOTAL		**$1,480,118** ESTIMATED TOTAL		**$837,918** ESTIMATED TOTAL	
	HOW WE CALCULATED YOUR RESULTS:		HOW WE CALCULATED YOUR RESULTS:		HOW WE CALCULATED YOUR RESULTS:	
	Forensics	$63,219	Ransom Payment	$29,378	BEC Direct Loss	$4,639
	PR, Crisis Response	$38,656	Forensics	$63,219	Forensics	$63,219
	IR Counsel	$16,086	PR, Crisis Response	$38,656	PR, Crisis Response	$38,656
	Notification/Call Center	$515,409	IR Counsel	$16,086	IR Counsel	$16,086
	Credit Monitoring	$77,311	Notification/Call Center	$515,409	Notification/Call Center	$257,705
	First Party Costs	$710,681	Credit Monitoring	$77,311	Credit Monitoring	$38,656
	Total Estimated Costs	**$1,421,361**	First Party Costs	$740,059	First Party Costs	$418,959
			Total Estimated Costs	**$1,480,118**	**Total Estimated Costs**	**$837,918**

For 100 employee's and $500,000 annual revenue