ORDER 66 CONSULTING

WE FIND YOUR LACK OF FAITH DISTURBING.

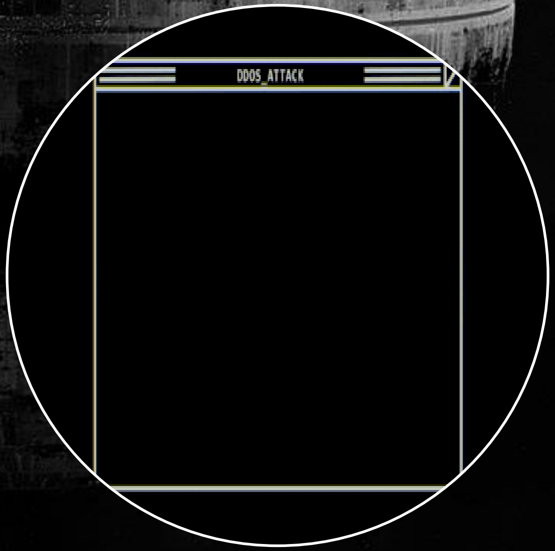
Security Solution Proposal for Death Star, Inc.

ENPM686 – 0201, Final Project

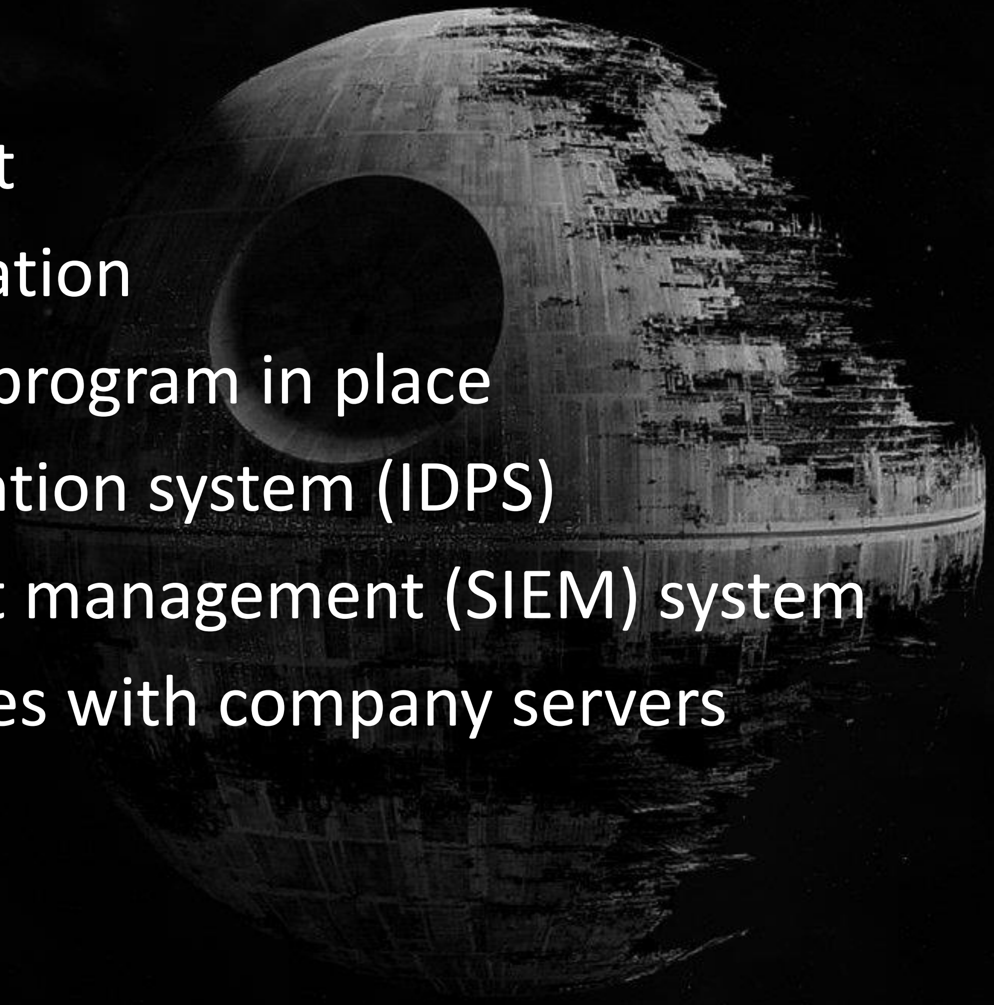
Bhavik Shah - 118547640
Akshat Mehta - 119229194

Overview of Security Incidents

- Targeted via spear-phishing campaigns, ransomware attacks, and DDoS
- Rendered 3 out of 5 machines unrecoverable via ransomware attack



Current State of Death Star, Inc.’s Infrastructure



- Outdated and unencrypted equipment
- Firewall capable only of layer 2 verification
- No employee training and awareness program in place
- Lack of intrusion detection and prevention system (IDPS)
- Lack of security information and event management (SIEM) system
- Insecure connectivity of remote devices with company servers

Objectives to be achieved

- Prevent further cyber attacks; detect and log attacks which cannot be prevented
- Design solutions and tolerance for undetected attacks
- Ensure secure connectivity between internal and external devices and networks
- Ensure security of the mainframe and failover mainframe
- Ensure security of the sales and customer support web application

Proposed Solutions

Proposed Solutions #1 - Local Deployment

- Hire Dedicated Security Staff
- Equipment Upgrade
- Network Upgrade and Management
- XDR Infrastructure
- SIEM Deployment
- Firewall Upgrade
- Multi Factor Authentication
- VPN Services for Remote Devices
- Employee Training and Awareness

Cost Estimates for Local Deployment Proposal

	Description	Cost ($/year)
Infrastructure Upgrade		
Network Infrastructure	Upgrade of routers and WAN devices	50,000 (one time cost)
Workstation and Laptop Upgrades	Upgrade and Patches on all devices	100,000 (one time cost)
Personnel Hire Salary	Salary for dedicated security staff	150,000
Security Solutions Upgrade		
MFA	Google Authenticator	Free
XDR Security Solution	Sophos Central Intercept X Advanced with XDR	180,000
Firewall Solution	Sophos XGS 3100 with XStream protection	9,978
VPN	Cisco AnyConnect VPN	4,018
Miscellaneous		
Periodical Security Assessment	Conduct assessments on quarterly level	18,000
Employee Training and Awareness Program	Training session for employees	2,000-12,000
Total		513,996 - 523,996

Proposed Solutions #2 - Cloud Deployment

- Hire Dedicated Security Staff
- Cloud Upgrade
- IAM System
- Network Upgrade and Management
- XDR Infrastructure
- Firewall Upgrade
- Multi Factor Authentication
- VPN Services for Remote Devices
- Employee Training and Awareness

Cost Estimates for Cloud Deployment Proposal

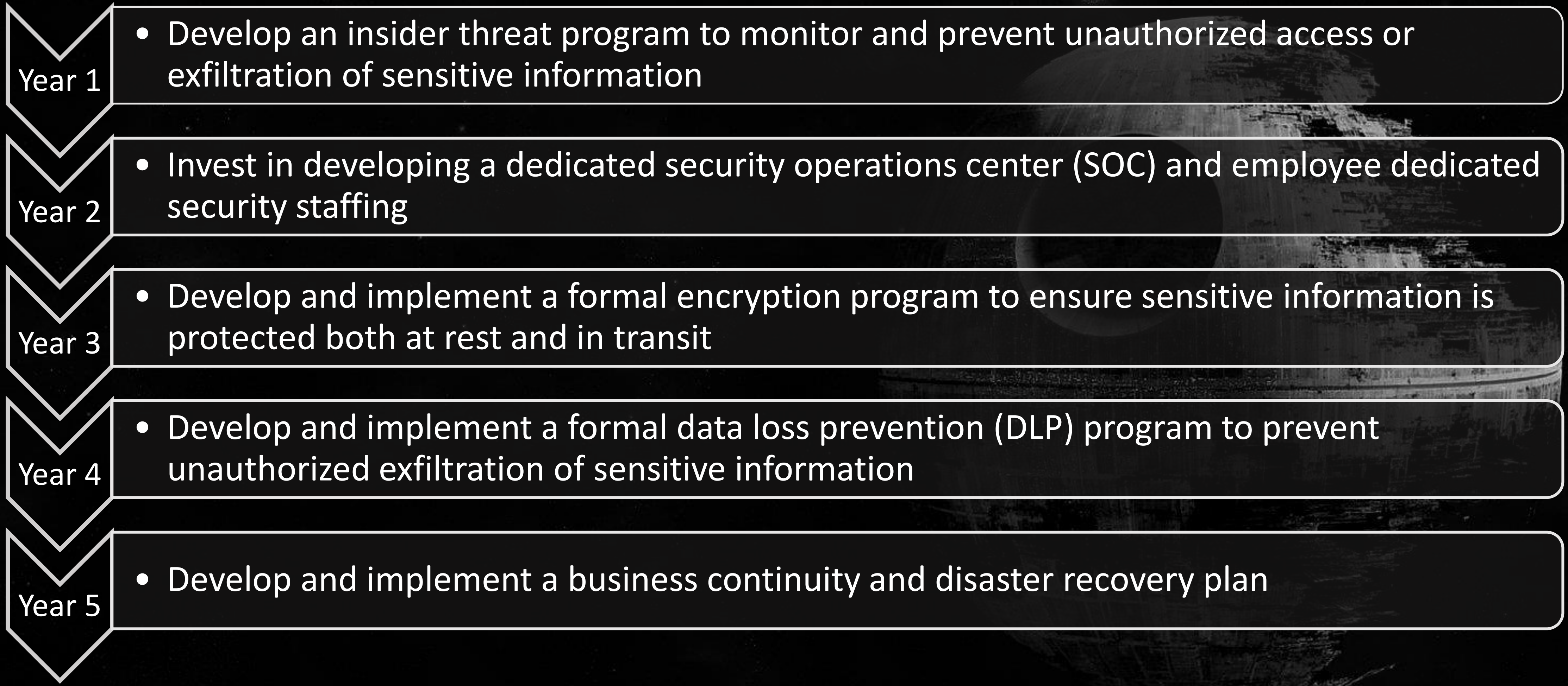
	Description	Cost ($/year)
Infrastructure Upgrade		
Network Infrastructure	Upgrade of routers and WAN devices	50,000 (one time cost)
Workstation and Laptop Upgrades	Upgrade and Patches on all devices	100,000 (one time cost)
Webserver on cloud	Host webserver on AWS	5,630
Mainframes on cloud	Host mainframe and backup on cloud	2,338
Personnel Hire Salary	Salary for dedicated security staff	150,000
Security Solutions Upgrade		
MFA	Google Authenticator	Free
XDR Security Solution	Sophos Central Intercept X Advanced with XDR	180,000
Firewall Solution	AWS Web Application and Network Firewall	7,325
VPN	Cisco AnyConnect VPN	4,018
Miscellaneous		
Periodical Security Assessment	Conduct assessments on quarterly level	18,000
Employee Training and Awareness Program	Training session for employees	2,000-12,000
Total		569,311 – 579,311

Future Pipeline

Pipeline for the next 5 years

ORDER 66 CONSULTING

WE FIND YOUR LACK OF FAITH DISTURBING.



Year 1
- Develop an insider threat program to monitor and prevent unauthorized access or exfiltration of sensitive information

Year 2
- Invest in developing a dedicated security operations center (SOC) and employee dedicated security staffing

Year 3
- Develop and implement a formal encryption program to ensure sensitive information is protected both at rest and in transit

Year 4
- Develop and implement a formal data loss prevention (DLP) program to prevent unauthorized exfiltration of sensitive information

Year 5
- Develop and implement a business continuity and disaster recovery plan

Note: Organization needs to review and update the existing cybersecurity program in place to ensure that it remains effective, and if any change needed, they need to be given priority.

ORDER 66 CONSULTING

WE FIND YOUR LACK OF FAITH DISTURBING.