Agenda

Strategic Business Review - Agenda

Executive Summary: (5 min)

The Galactic Empire's lax security standards left Scarif exposed to a data exfiltration and network breach that resulted in the complete forfeiture of the IT Assets at the facility.
Mission critical Intellectual Property has been exfiltrated which will have an impact on the organization's competitive edge and likely cause further financial losses.
Immeasurable reputation damage has occurred causing the loss of thousands of social media followers (may they rest in piece). Insufficient cyber liability insurance will result in the Galactic Empire having to cover the cost of reputation management out of pocket.
Due to the large amount of policy & procedure, training, and incident response work that needs to be undertaken, it is our recommendation that the Empire outsource day to day IT management to a qualified third party while they Dash and team refocus their efforts on improving the organization's security posture.

Relevant Action Items:(5 min)

Implement Improved IT Security Policy and Procedures
Implement Employee Cyber Security & Incident Response Training
Improve Network Security Posture
Acquire Cyber Liability Insurance Policy in preparation for future incidents
Outsource IT Support services to a qualified MSP

Recent Project Status Update: (5 min)

The battle station is fully armed and operational.

Client Updates & Changes: (15 min)

Significant future expansion into additional geographic regions is anticipated.
IT Support will need to scale accordingly.
A large construction project is key to future expansion and must not be allowed to fall behind due to this event.

Risk & Exposure Review:(45 min)

Review Latest Risk Assessment
Review Known Assets for:
Security Upgrades (out of date OS or vendor EOL)
Lifecycle Upgrades
Present/Review Budget and Proposed Projects

Issues list: Identify, Discuss, Solve (30 min)

Wrap up: (5 min)

Schedule first QBR
Document new action items (to become tickets)
MSP Action Items:

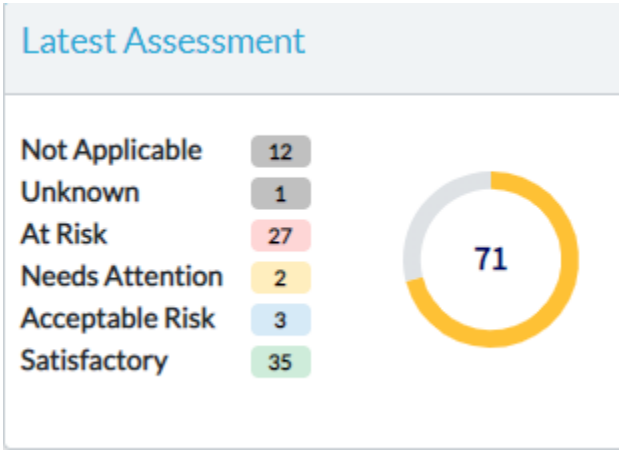
Client To-Do's:

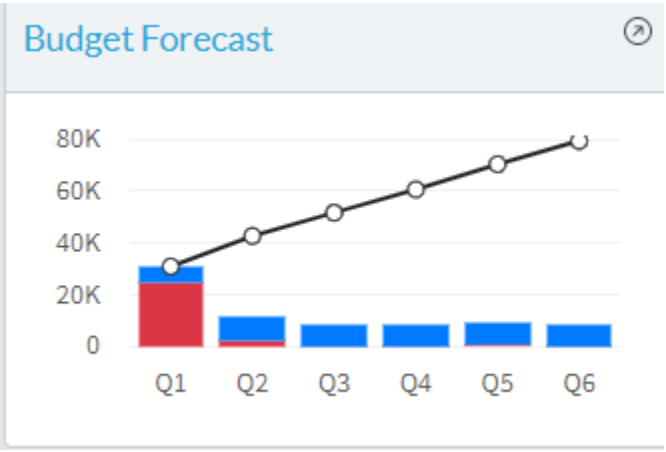
Alex's Executive Summary

Strategic Business Review - Executive Summary

The purpose of this meeting is to address risk and exposure within the organization as demonstrated by the recent Scarif breach, which has negatively impacted the business goals of your organization. Better alignment between IT and other business units will enable the organization to achieve the best ROI on technology purchases while ensuring that the investment is furthering the goals of other business units.

Scorecard:





Project Updates:

The battle station is fully armed and operational.

Top Risks:

Breach
Data Loss / Exfiltration
Reputation Damage

Remediation Recommendations:

Implement Improved IT Security Policy and Procedures
Implement Employee Cyber Security & Incident Response Training
Improve Network Security Posture
Acquire Cyber Liability Insurance Policy in preparation for future incidents
Outsource IT Support services to a qualified MSP

Assessment Summary

SUMMARY

The overall summary report provides an overall score for each of the categories designed to show the overall health and compliance of your IT systems. Scores are weighted based on their respective importance to keeping your business in optimal range.

Summary Report for: Galactic Empire
Date Prepared: 2021-05-04
Assessment Template: Galactic Cyber Security Risk Assessment

Category	Description	Score
Level 1 - Foundational	Review different components related to client's infrastructure.	**89**
Level 2 - Emerging	Software Applications for Operating and Protecting the Business	**66**
Level 3 - Intermediate	Review critical areas of security in place for the client.	**67**
Level 4 - Advanced	Business Continuity and BDR	**58**
Level 5 - High Security	Does the company have the necessary Policies & Procedures in place to provide appropriate protections?	**50**
Ancillary Services		**100**

Overall Score	**71**

CATEGORIES

Category: Level 1 - Foundational

Review different components related to client's infrastructure.

Item	Summary	Score
Password Policy	While a Password policy exists, it allows for the use of 12345, which is amazing. I've got the same combination on my luggage.	**Needs Attention**
Patch Management Policy	Some droids cannot be patched due to vendor requirements. Additional steps should be taken to add additional protections but full remediation is impossible due to vendor requirements.	**Acceptable Risk**
Asset Inventory Management	Asset inventory exists but is not being used in conjunction with an incident response plan when droids, shuttles, and other assets are lost or stolen.	**At Risk**
Lifecycle Management Policy	Lifecycle Management is being performed regularly, limiting technology debt and decreasing risk for the organization.	**Satisfactory**
Workstations	Workstations are not approaching EOL or warranty expiration.	**Satisfactory**
Servers	Servers are not approaching EOL or warranty expiration.	**Satisfactory**
Storage	Primary data storage is located onsite and offers sufficient room for expansion/growth.	**Satisfactory**
Directory Services	User accounts and permissions are authenticated against an onsite Domain Controller.	**Satisfactory**
Hosted Email	Email is outsourced to a 3rd party Hosted Exchange provider or to Office 365	**Satisfactory**
Operating System	All Operating Systems are current and vendor supported.	**Satisfactory**
Power Management	Mission Critical equipment is protected by a UPS.	**Satisfactory**
Backup & Disaster Recovery	Backups are stored on non-encrypted portable media and do not appear to be geo-redundant. The risk of data loss is elevated.	**At Risk**

Infrastructure Wiring	Infrastructure wiring is reasonably clean and well labeled, speeding up the troubleshooting process in the event of a network issue.	**Satisfactory**
Internet Service	ISP is reliable and circuit speed is appropriate for the operations of the business.	**Satisfactory**
UTM Internet Security Appliance	Sophos UTM Firewall in included and managed.	**Satisfactory**
Switching	Client has deployed Next Generation cloud managed switches and refreshing them on a schedule as part of regular lifecycle management.	**Satisfactory**
WiFi	WiFi does not exist and the organization has no business case to introduce it into the environment.	**Not Applicable**
Acceptable Use Policy (AUP)	Unknown - more information is required.	**Unknown**
Endpoint Security Software	Traditional Anti-virus was replaced with or is supplemented by Next Gen Endpoint Protection with Endpoint Detection and Response.	**Satisfactory**
IT Support Services	Internal IT is incredibly stressed due to questionable leadership tactics and poor company culture. They cite "constant fear of being choked to death" for shoddy work.	**Needs Attention**
LoB Application Support	Client's Line of Business Applications are modern and under vendor support. These applications are included as part of Lifecycle Management planning.	**Satisfactory**
vCIO Consulting Services	The CISO is an internal role at The Galactic Empire. The current CISO is under significant pressure to get up to speed before another incident can occur.	**Not Applicable**

Level 1 - Foundational Score	**89**

Category: Level 2 - Emerging

Software Applications for Operating and Protecting the Business

Item	Summary	Score
Access Logging	Client is not logging access to sensitive areas (server rooms, restricted printers, etc).	**At Risk**
Inactivity Timeout / System Lock Policy	Systems are not configured to lock on idle, allowing for use without authentication.	**At Risk**
Data Encryption Policy	No Data Encryption Policy exists.	**At Risk**
Removable Media Policy	Removable media is in use in the environment and not encrypted. Policy status is unknown.	**At Risk**
Electronic Funds Transfer Policy	Client has an established EFT Policy, updates it regularly, and reviews it with staff at least annually.	**Satisfactory**
Cyber Liability Insurance	The organization does not currently have Cyber Liability insurance. It is recommended that the organization consult an insurance expert and procure a suitable insurance policy.	**At Risk**
Multi-Factor Authentication	MFA is not deployed.	**At Risk**
Spare Device Inventory	The company maintains at least 5% spare equipment.	**Satisfactory**
Print Management	There are no printers - as if Star Wars wasn't already cool enough!	**Satisfactory**
Software License Management	License Management is handled by the IT Provider and the client is believed to be in compliance.	**Satisfactory**
Email Protection / Filtering	Sophos Central Email Advanced is deployed and protecting the email environment.	**Satisfactory**
Email Encryption	Sensitive information may be being sent by email without encryption.	**At Risk**
Cloud File Server	Not Applicable.	**Not Applicable**
Virtual Networks (VLANs)	The network does not have VLANs deployed which increases the threat from lateral movement of hackers and malware throughout the network.	**At Risk**

VPN / Remote Access	Not Applicable	**Not Applicable**
Mobile Device Policy	Client has a documented Mobile Device Policy. It has been shared and is on file with the Service Provider, and has been implemented. It includes policies and safeguards for personal and business own	**Satisfactory**
Social Engineering and Phishing Training	Insufficient social engineering and/or phishing training is being performed.	**At Risk**
Network Documentation	Network documentation is up to date and accurate.	**Satisfactory**
Website Management	The organization has an outsourced resource for managing the company website. That resource is documented and collaborates with the MSP for any DNS changes.	**Satisfactory**
Updated Contact Information	Due to the restrictive company culture, leadership is the sole point of all communications. Additional contact information at the MSP level is not required.	**Acceptable Risk**
Compliance - PCI	Client does not handle payment card data.	**Not Applicable**
Compliance - HIPAA Regulatory Compliance	Client does not operate as a Covered Entity or Business Associate.	**Not Applicable**
Compliance - HIPAA Business Associate Agreements	Client does not operate as a Covered Entity or Business Associate.	**Not Applicable**

Level 2 - Emerging Score	**66**

Category: Level 3 - Intermediate

Review critical areas of security in place for the client.

Item	Summary	Score
Controlled Access / Least Privilege Policy	The company has no policy in place to limit access rights for users to the bare minimum permissions they need to perform their work	**At Risk**
BYOD Policy	A liberal Bring Your Own Droid policy was a key factor in the data breach.	**At Risk**
User Account & Security Permissions Audit Policy	User accounts are not being audited, leaving potential for access from former employees or those with permissions above those required to perform their job function.	**At Risk**
Technology Budgeting	The organization has a formal budget in place for all IT products and services.	**Satisfactory**
BDR Test Restore	The organization has a plan in place for test restores. Test restores are performed on a scheduled basis and successful within acceptable RTO and RPO.	**Satisfactory**
Dark Web Monitoring	The Dark Web is being monitored for employee credentials and a process is in place to provide additional training if/when credentials are breached.	**Satisfactory**
Workstation/Server Encryption	TPM is activated and Bitlocker encryption is monitored on all systems authorized to contain sensitive information.	**Satisfactory**
Email Archiving	Email Archiving is in place to protect sensitive data from loss and/or simplify reporting in the event of a data request (i.e. FOYA).	**Satisfactory**
Intrusion Detection & Prevention	While IPS/IDS is deployed, the shield gate (Firewall) failed open, allowing unauthorized communications to pass through.	**At Risk**
Mobile Device Encryption	Mobile device encryption is not enforced or mandated by company policy.	**At Risk**
Backup of Cloud Services	No Cloud Services in use.	**Not Applicable**
Mobile Device Management	MDM is in place and company owned devices are managed and patched regularly.	**Satisfactory**

Synchronized Security	Next Generation Endpoint Protection shares threat information with the UTM Firewall, enabling the two to work together to respond to detected threats immediately and without human interaction.	**Satisfactory**
Zero Trust Security	Zero Trust Security is not in place.	**At Risk**
Password Manager	No password management solution is in use, or users are left to find a solution on their own.	**At Risk**
Scan & Fax to Email	Fax and/or scan to email are in use, causing potentially sensitive information to be stored un-encrypted inside mailboxes.	**At Risk**
Vendor Risk Management	Vendors with access to sensitive data are required to complete an audit annually to ensure reasonable security. Policies are in place to address vendors who score poorly on an audit.	**Satisfactory**

Level 3 - Intermediate Score	**67**

Category: Level 4 - Advanced

Business Continuity and BDR

Item	Summary	Score
Business Continuity Plan	The organization relies on vendors to know what to do when disaster strikes and guide them through the reactionary steps.	**At Risk**
Infrastructure Capacity & Scalability	The organization's decision to move to the cloud means that capacity and scalability are flexible and cost effective. The organization can scale as it grows without undue expense or delays.	**Satisfactory**
Cybersecurity Endpoint Monitoring (SOC + EDR)	As new global threats emerge, it is recommended to add Cyber Security Monitoring of Workstations and Servers as an additional layer of protection to existing IT services.	**At Risk**
Cybersecurity Firewall Monitoring (SOC + EDR)	Rocket Cyber has been deployed to add 24/7 Cyber Security Monitoring of Firewalls as an additional layer of protection to existing IT services.	**Satisfactory**
Disable Unused Physical Access Ports	Unused ports were found to be enabled at the time of the Scarif Incident.	**At Risk**
SIEM	SIEM is deployed and monitored 24/7	**Satisfactory**
Monitor Sensitive Files, Communications, and Data Flows	No solution is in place to monitor for the transmission of unencrypted communications and/or data.	**At Risk**
Vulnerability Scanning & Management	No vulnerability management solution is in place.	**At Risk**
Compliance - CIS-20	Client is not obligated to maintain CIS-20.	**Not Applicable**
Compliance - NIST 800-171	Client is not obligated to maintain NIST 800-171.	**Not Applicable**
Compliance - NIST 800-53	Client is not obligated to maintain NIST 800-53.	**Not Applicable**
Compliance - ISO/IEC 27002	Client is not obligated to maintain ISO/IEC 27002.	**Not Applicable**

Level 4 - Advanced Score	**58**

Category: Level 5 - High Security

Does the company have the necessary Policies & Procedures in place to provide appropriate protections?

Item	Summary	Score
Incident Response Planning	No incident response planning has taken place.	**At Risk**
Active Threat Hunting	Active Threat Hunting is not deployed	**At Risk**
Honeypot Deployment	Deployed with monitoring and alerting.	**Satisfactory**
Third Party Penetration Testing	Client is in a high compliance industry, yet is not hiring a third party to perform Penetration Testing at regular intervals.	**At Risk**

Level 5 - High Security Score	**50**

Category: Ancillary Services

Item	Summary	Score
VoIP Telephone Service	The organization is using a modern VoIP service with features that match company requirements and accommodate flexibility and scalability.	**Satisfactory**

Ancillary Services Score	**100**

Remediation Plan

At Risk Items:

Item	Summary	Comments
Asset Inventory Management	Asset inventory exists but is not being used in conjunction with an incident response plan when droids, shuttles, and other assets are lost or stolen.	Recommendation - Train the incident response team on best practices for dealing with lost/stolen IT assets.
Backup & Disaster Recovery	Backups are stored on non-encrypted portable media and do not appear to be geo-redundant. The risk of data loss is elevated.	Recommendation - Convert to a cloud based BDR solution with geo-redundant storage and immutable storage for added ransomware protection.
Access Logging	Client is not logging access to sensitive areas (server rooms, restricted printers, etc).	Recommendation - Deploy access logging technology and related policy & procedure to protect sensitive locations and their contents.
Inactivity Timeout / System Lock Policy	Systems are not configured to lock on idle, allowing for use without authentication.	Recommendation - Deploy inactivity timeout for all devices, blocking access for unauthorized users.
Data Encryption Policy	No Data Encryption Policy exists.	Recommendation - Encrypt all data in transit and at rest.
Removable Media Policy	Removable media is in use in the environment and not encrypted. Policy status is unknown.	Recommendation - Confirm the existence and quality of the existing Removable Media Policy. Train end users of the potential impact of not adhering to the policy.
Cyber Liability Insurance	The organization does not currently have Cyber Liability insurance. It is recommended that the organization consult an insurance expert and procure a suitable insurance policy.	Recommendation - Procure Cyber Liability Insurance sufficient to cover the loss of proprietary data and/or the destruction of a planet or moon sized facility. Reputation

		management coverage is also HIGHLY encouraged.
Multi-Factor Authentication	MFA is not deployed.	Recommendation - Deploy MFA on all key applications and platforms.
Email Encryption	Sensitive information may be being sent by email without encryption.	Recommendation - Encrypt all data in transit and at rest.
Virtual Networks (VLANs)	The network does not have VLANs deployed which increases the threat from lateral movement of hackers and malware throughout the network.	Recommendation - Deploy additional VLANs where appropriate to segment network traffic to protect critical information.
Social Engineering and Phishing Training	Insufficient social engineering and/or phishing training is being performed.	Recommendation - Provide an employee training solution that includes social engineering and anti-phishing training.
Controlled Access / Least Privilege Policy	The company has no policy in place to limit access rights for users to the bare minimum permissions they need to perform their work	Recommendation - Roll out a Least Privilege policy across the organization.
BYOD Policy	A liberal Bring Your Own Droid policy was a key factor in the data breach.	Recommendation - Deploy a Mobile Droid Management solution and lock down BYODs as well as Galactic Empire owned Droids.
User Account & Security Permissions Audit Policy	User accounts are not being audited, leaving potential for access from former employees or those with permissions above those required to perform their job function.	Recommendation - Roll out a User & Permissions Audit Policy in accordance with security best practices.
Intrusion Detection & Prevention	While IPS/IDS is deployed, the shield gate (Firewall) failed open, allowing unauthorized communications to pass through.	Recommendation - Existing shield gates and firewalls should be reconfigured to fail closed, blocking communications in the event of a failure.
Mobile Device Encryption	Mobile device encryption is not enforced or mandated by company policy.	Recommendation - Encrypt all data in transit and at rest.

Zero Trust Security	Zero Trust Security is not in place.	Recommendation - Deploy Zero Trust to all IT assets.
Password Manager	No password management solution is in use, or users are left to find a solution on their own.	Recommendation - Roll out a Password Manager and include password management training for all employees.
Scan & Fax to Email	Fax and/or scan to email are in use, causing potentially sensitive information to be stored un-encrypted inside mailboxes.	Recommendation - Encrypt all data in transit and at rest. Deploy encrypted fax/scan solutions or stop using those platforms.
Business Continuity Plan	The organization relies on vendors to know what to do when disaster strikes and guide them through the reactionary steps.	Recommendation - Include table top exercises for Incident Response in employee training.
Cybersecurity Endpoint Monitoring (SOC + EDR)	As new global threats emerge, it is recommended to add Cyber Security Monitoring of Workstations and Servers as an additional layer of protection to existing IT services.	Recommendation - Deploy SOC + EDR solution for all network connected assets.
Disable Unused Physical Access Ports	Unused ports were found to be enabled at the time of the Scarif Incident.	Remediation - Unused ports should be set to interface down status.
Monitor Sensitive Files, Communications, and Data Flows	No solution is in place to monitor for the transmission of unencrypted communications and/or data.	Recommendation - Deploy a solution to monitor the transmission and storage of unencrypted data.
Vulnerability Scanning & Management	No vulnerability management solution is in place.	Recommendation - Deploy vulnerability scanning and management & build policy around the remediation of any issues that are identified.
Incident Response Planning	No incident response planning has taken place.	Recommendation - As part of outsourced vCIO services, IR planning and tabletop exercises will be included in future engagements.

Active Threat Hunting	Active Threat Hunting is not deployed	Recommendation - Deploy Active Threat Hunting and Honeypots across the network.
Third Party Penetration Testing	Client is in a high compliance industry, yet is not hiring a third party to perform Penetration Testing at regular intervals.	Recommendation - Outsource Pen Testing ASAP.

Needs Attention Items:

Item	Summary	Comments
Password Policy	While a Password policy exists, it allows for the use of 12345, which is amazing. I've got the same combination on my luggage.	Recommendation - Change the password on my luggage.
IT Support Services	Internal IT is incredibly stressed due to questionable leadership tactics and poor company culture. They cite "constant fear of being choked to death" for shoddy work.	Recommendation: Implement a Co-Managed IT structure to provide relief for internal IT teams.

Project Summary

Project Overview

Project Name:	Security Policy & Procedure Implementation	**Project Dates:**	2021-05-04 thru 2021-05-04
Status:	Proposed	**Priority:**	Medium
Location:	Primary	**Contacts:**	Company Contacts / Internal Contacts
Description:	Implement new and improved Policies and Procedures to align cyber security culture with the operational outcomes desired by The Galactic Empire.		

Project Cost Estimates – Total Estimated Project Cost: 45,000

Costs	2021-May
Labor	45,000
Materials	
Replacement	
Total Cost	45,000

Linked Assessment Items

Score	Item	Response	Type	Template	Category	Date
At Risk	Controlled Access / Least Privilege Policy	The company has no policy in place to limit access rights for users to the bare minimum permissions they need to perform their work	Baseline	Galactic Cyber Security Risk Assessment	Level 3 - Intermediate	2021-05-04
At Risk	Access Logging	Client is not logging access to sensitive areas (server rooms, restricted printers, etc).	Baseline	Galactic Cyber Security Risk Assessment	Level 2 - Emerging	2021-05-04
At Risk	Data Encryption Policy	No Data Encryption Policy exists.	Baseline	Galactic Cyber Security Risk Assessment	Level 2 - Emerging	2021-05-04
At Risk	Removable Media Policy	Removable media is in use in the environment and not encrypted. Policy status is unknown.	Baseline	Galactic Cyber Security Risk Assessment	Level 2 - Emerging	2021-05-04
At Risk	User Account & Security Permissions Audit Policy	User accounts are not being audited, leaving potential for access from former employees or those with	Baseline	Galactic Cyber Security Risk Assessment	Level 3 - Intermediate	2021-05-04

		permissions above those required to perform their job function.				
Needs Attention	Password Policy	While a Password policy exists, it allows for the use of 12345, which is amazing. I've got the same combination on my luggage.	Baseline	Galactic Cyber Security Risk Assessment	Level 1 - Foundational	2021-05-04
At Risk	BYOD Policy	A liberal Bring Your Own Droid policy was a key factor in the data breach.	Baseline	Galactic Cyber Security Risk Assessment	Level 3 - Intermediate	2021-05-04
At Risk	Business Continuity Plan	The organization relies on vendors to know what to do when disaster strikes and guide them through the reactionary steps.	Baseline	Galactic Cyber Security Risk Assessment	Level 4 - Advanced	2021-05-04
At Risk	Incident Response Planning	No incident response planning has taken place.	Baseline	Galactic Cyber Security Risk Assessment	Level 5 - High Security	2021-05-04
At Risk	Inactivity Timeout / System Lock Policy	Systems are not configured to lock on idle, allowing for use without authentication.	Baseline	Galactic Cyber Security Risk Assessment	Level 2 - Emerging	2021-05-04

Project Summary

Project Overview

Project Name:	Improve Network Security Posture	**Project Dates:**	2021-05-04 thru 2021-05-04
Status:	Proposed	**Priority:**	High
Location:	Primary	**Contacts:**	Company Contacts / Internal Contacts
Description:	Deploy products, services, and technical best practices to provide The Galactic Empire with a more secure, stable, and reliable network infrastructure.		

Project Cost Estimates – Total Estimated Project Cost: 350,000

Costs	2021-May
Labor	350,000
Materials	
Replacement	
Total Cost	350,000

Linked Assessment Items

Score	Item	Response	Type	Template	Category	Date
At Risk	Asset Inventory Management	Asset inventory exists but is not being used in conjunction with an incident response plan when droids, shuttles, and other assets are lost or stolen.	Baseline	Galactic Cyber Security Risk Assessment	Level 1 - Foundational	2021-05-04
At Risk	Email Encryption	Sensitive information may be being sent by email without encryption.	Baseline	Galactic Cyber Security Risk Assessment	Level 2 - Emerging	2021-05-04
At Risk	Intrusion Detection & Prevention	While IPS/IDS is deployed, the shield gate (Firewall) failed open, allowing unauthorized communications to pass through.	Baseline	Galactic Cyber Security Risk Assessment	Level 3 - Intermediate	2021-05-04
At Risk	Password Manager	No password management solution is in use, or users are left to find a solution on their own.	Baseline	Galactic Cyber Security Risk Assessment	Level 3 - Intermediate	2021-05-04
At Risk	Multi-Factor Authentication	MFA is not deployed.	Baseline	Galactic Cyber Security Risk Assessment	Level 2 - Emerging	2021-05-04

At Risk	Third Party Penetration Testing	Client is in a high compliance industry, yet is not hiring a third party to perform Penetration Testing at regular intervals.	Baseline	Galactic Cyber Security Risk Assessment	Level 5 - High Security	2021-05-04
At Risk	Mobile Device Encryption	Mobile device encryption is not enforced or mandated by company policy.	Baseline	Galactic Cyber Security Risk Assessment	Level 3 - Intermediate	2021-05-04
At Risk	Virtual Networks (VLANs)	The network does not have VLANs deployed which increases the threat from lateral movement of hackers and malware throughout the network.	Baseline	Galactic Cyber Security Risk Assessment	Level 2 - Emerging	2021-05-04
At Risk	Scan & Fax to Email	Fax and/or scan to email are in use, causing potentially sensitive information to be stored un-encrypted inside mailboxes.	Baseline	Galactic Cyber Security Risk Assessment	Level 3 - Intermediate	2021-05-04
At Risk	Cybersecurity Endpoint Monitoring (SOC + EDR)	As new global threats emerge, it is recommended to add Cyber Security Monitoring of Workstations and Servers as an additional layer of protection to existing IT services.	Baseline	Galactic Cyber Security Risk Assessment	Level 4 - Advanced	2021-05-04
At Risk	Zero Trust Security	Zero Trust Security is not in place.	Baseline	Galactic Cyber Security Risk Assessment	Level 3 - Intermediate	2021-05-04
At Risk	Active Threat Hunting	Active Threat Hunting is not deployed	Baseline	Galactic Cyber Security Risk Assessment	Level 5 - High Security	2021-05-04
At Risk	Monitor Sensitive Files, Communications, and Data Flows	No solution is in place to monitor for the transmission of unencrypted communications and/or data.	Baseline	Galactic Cyber Security Risk Assessment	Level 4 - Advanced	2021-05-04
At Risk	Backup & Disaster Recovery	Backups are stored on non-encrypted portable media and do not appear to be geo-redundant. The risk of data loss is elevated.	Baseline	Galactic Cyber Security Risk Assessment	Level 1 - Foundational	2021-05-04
At Risk	Disable Unused Physical Access Ports	Unused ports were found to be enabled at the time of the Scarif Incident.	Baseline	Galactic Cyber Security Risk Assessment	Level 4 - Advanced	2021-05-04
At Risk	Vulnerability Scanning & Management	No vulnerability management solution is in place.	Baseline	Galactic Cyber Security Risk Assessment	Level 4 - Advanced	2021-05-04

Project Summary

Project Overview

Project Name:	Employee Cyber Security & Incident Response Training	**Project Dates:**	2021-05-04 thru 2021-05-04
Status:	Proposed	**Priority:**	Medium
Location:	Primary	**Contacts:**	Company Contacts / Internal Contacts
Description:	Employee security training, phish testing, and incident response tabletop exercises.		

Project Cost Estimates – Total Estimated Project Cost: 0

Costs	2021-May
Labor	
Materials	
Replacement	
Total Cost	0

New Recurring Costs

Vendor/Service	Cost	Cycle	Account	Description	Location	Begin Date	End Date
Bantha Tracks IT Consulting	75000	Quarterly	Technology	Employee security training, phish testing, and incident response tabletop exercises.	Primary	2021-05-04	2023-05-03

Linked Assessment Items

Score	Item	Response	Type	Template	Category	Date
At Risk	Social Engineering and Phishing Training	Insufficient social engineering and/or phishing training is being performed.	Baseline	Galactic Cyber Security Risk Assessment	Level 2 - Emerging	2021-05-04

Cyber Insurance Recommendation

Project Overview

Project Name:	Recommendation - Cyber Liability Insurance Policy Improvements	**Project Dates:**	2021-05-04 thru 2021-05-04
Status:	Proposed	**Priority:**	Medium
Location:	Primary	**Contacts:**	Company Contacts / Internal Contacts
Description:	The Galactic Empire should obtain a more inclusive Cyber Security Liability Insurance Policy with protections against operational downtime, property destruction (including terrorism), and reputation management services.		

Project Cost Estimates – Total Estimated Project Cost: 0

Costs	2021-May
Labor	
Materials	
Replacement	
Total Cost	0

Linked Assessment Items

Score	Item	Response	Type	Template	Category	Date
At Risk	Cyber Liability Insurance	The organization does not currently have Cyber Liability insurance. It is recommended that the organization consult an insurance expert and procure a suitable insurance policy.	Baseline	Galactic Cyber Security Risk Assessment	Level 2 - Emerging	2021-05-04

Managed Services

Project Overview

Project Name:	Managed IT Support Services	**Project Dates:**	2021-05-04 thru 2021-05-04
Status:	Proposed	**Priority:**	Medium
Location:	Primary	**Contacts:**	Company Contacts / Internal Contacts
Description:	One of the quickest ways that Bantha Tracks IT Service Provider can assist the Galactic Empire in creating bandwidth to remediate the findings from our audit would be to provide IT Managed Services, allowing the limited internal resources to focus on remediation of existing threats and fostering an internal culture of Cyber Security Awareness.		

Project Cost Estimates – Total Estimated Project Cost: 450,000

Costs	2021-May
Labor	450,000
Materials	
Replacement	
Total Cost	450,000

New Recurring Costs

Vendor/Service	Cost	Cycle	Account	Description	Location	Begin Date	End Date
Bantha Tracks IT Consulting	1000000	Monthly	Technology	Managed IT Support agreement - see SOW for details.	Primary	2021-05-04	2023-05-03

Linked Assessment Items

Score	Item	Response	Type	Template	Category	Date
Needs Attention	IT Support Services	Internal IT is incredibly stressed due to questionable leadership tactics and poor company culture. They cite "constant fear of being choked to death" for shoddy work.	Baseline	Galactic Cyber Security Risk Assessment	Level 1 - Foundational	2021-05-04