SSR Inc.

Raising the Capability Maturity of Cybersecurity Function




Ray Chang
Will Dannacher
Akshitha Shankar
Vahin Vuppalanchi

September 15, 2023

These slides were part of an oral presentation by Team 9 for the MSIS Program GRC case study. These slides are not a complete record of that presentation, nor of the accompanying discussion. The slides are protected by copyright law and may not be reproduced, in whole or in part, without the express written consent of the author.

Agenda

- Introduction
- Solution
- Timeline
- Financial Analysis
- Risks & Mitigations
- Conclusion

Evaluating SSR's Cybersecurity Capability

Previously,

SSR Inc. is new firm formed from a merger of three distinct companies each specializing in a different sector. Despite the success of the organization, they initially struggled to implement an IT department. Since, they have continued a solid position in their industry and have organized their IT systems sufficiently.

However,

The security implementation process included a few gaps in their overall cybersecurity program which led to a ransomware hack compromising their systems, data, and daily operations.

Now,

How can SSR Inc. enhance their security protocols to create a more robust cybersecurity infrastructure and business environment?

https://thestrategystory.com/blog/kroger-swot-analysis

Our Recommendation is a Three-Pronged Approach to Restructure the Security Functions

Governance

Established dedicated **Security Department** with accountability & Responsibility to push effective **policies and standards** to secure SSR's Business

Control

Enforce Effective Security Control to **Monitor, Detect and Mitigate** Risk and Eventual Ensure the Security for SSR

Incident Management

Establish a robust **Business Continuity Plan** to ensure quick turnaround of operations

Outline a process for **Managing Security Incidents** and enhance knowledge base

It's Crucial to Bolster Cybersecurity Functions at SSR

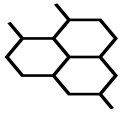
The 3 R's of Cybersecurity

Manage Risks
Effective threat mitigation allows a firm to assess incoming risks and develop preventative measures for the future

Quick Response & Recovery
Ensure that the firm can detect risks before they become a major issue
Minimize damages caused by threats and accelerate response time

Optimize Resource Allocation
Certify that investments made into cybersecurity align with what the firm is trying to accomplish

Governance



Ensure Responsibility & Accountability

- Promote Director Simmons to CISO, reporting to CIO, with accountability for IT risk management, compliance and cybersecurity to safeguard SSR's technology assets
- Increase budget towards IT risk management, IT compliance and cybersecurity to match organizations of this size and established a dedicated department
- Have multiple executives led by the CISO involved in the implementation and development of this greater cybersecurity function

Develop Security Metrics

- Enhance the existing measures by including additional metrics regarding other elements of security beyond SLAs and effectiveness tickets [APO13]
- Include specific metrics regarding employee competency and training completion
- Develop risk scenario simulations to determine percent effective security
- Continuously monitor these metrics via scheduled reviews and number of findings

https://www.paloaltonetworks.com/blog/2022/06/the-importance-of-a-consistent-security-policy/

https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/effective-security-metrics

https://blog.24by7security.com/you-probably-need-a-security-governance-committee-and-heres-why

Control

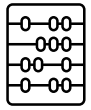
Manage Vendor Risk

- Subscribe to security and risk management providers to detect attacks and data breaches to quickly
- Determine if an attack that happens on the vendor side puts SSR at risk

https://www.nudgesecurity.com/

Standard Enforcement & Security Monitoring

- Enforce policies and standards like ISO 27001, ISO 27002, NIST800-53, NIST CSF and COBIT
- Enhance capabilities in detecting abnormal user and entity behavior within the network to identify and reduce insider threats
- Leverage AI to improve threat detection by identifying subtle anomalies and patterns that may be indicative of an attack
- Alerts the security analyst and administrators when the system detects a security incident or a potential threat for further investigation and response

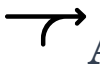


Consolidate Data and Maintain Integrity

- Create a centralized asset repository
- Capture, store, and monitor all data
- Track changes in the location of assets
- Automate the generation of inventory and asset reporting
- Develop a clear and accessible interface for all employees to use
- Automate data inflow and sanitization

https://www.hpe.com/emea_europe/en/what-is/central-repository.html

https://content.solarwinds.com/creative/pdf/whitepapers/it_asset_management_%20benefits_%20best_practices.pdf



Integration of Applications and Teams

- Ensure that the PCI and operational security team are not isolated
- Use a framework that allows teams to build off each other instead of forcing collaboration
- Continue to manage relationships between teams
- Maintain constant communication through a framework like SCRUM

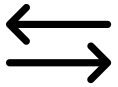
https://nickols.us/~nickols1/Learning.pdf

COBIT 2019 Framework: Governance and Management Objectives

Incident Management

Business Continuity Plan

- Establish a Cross-functional Team comprising IT, Cybersecurity, Forensics and Legal
- Comprehensive continuity plan and scope determined by key stakeholders outlining roles, responsibilities and procedures [DSS04]
- Enable efficient communication channels
- Identify internal and external business processes and activities critical to operations and impact on security [DSS 04]
- Establish Recovery Protocols – Third Party Services
- Regular Employee Cyber Training to reduce human errors



Change Management

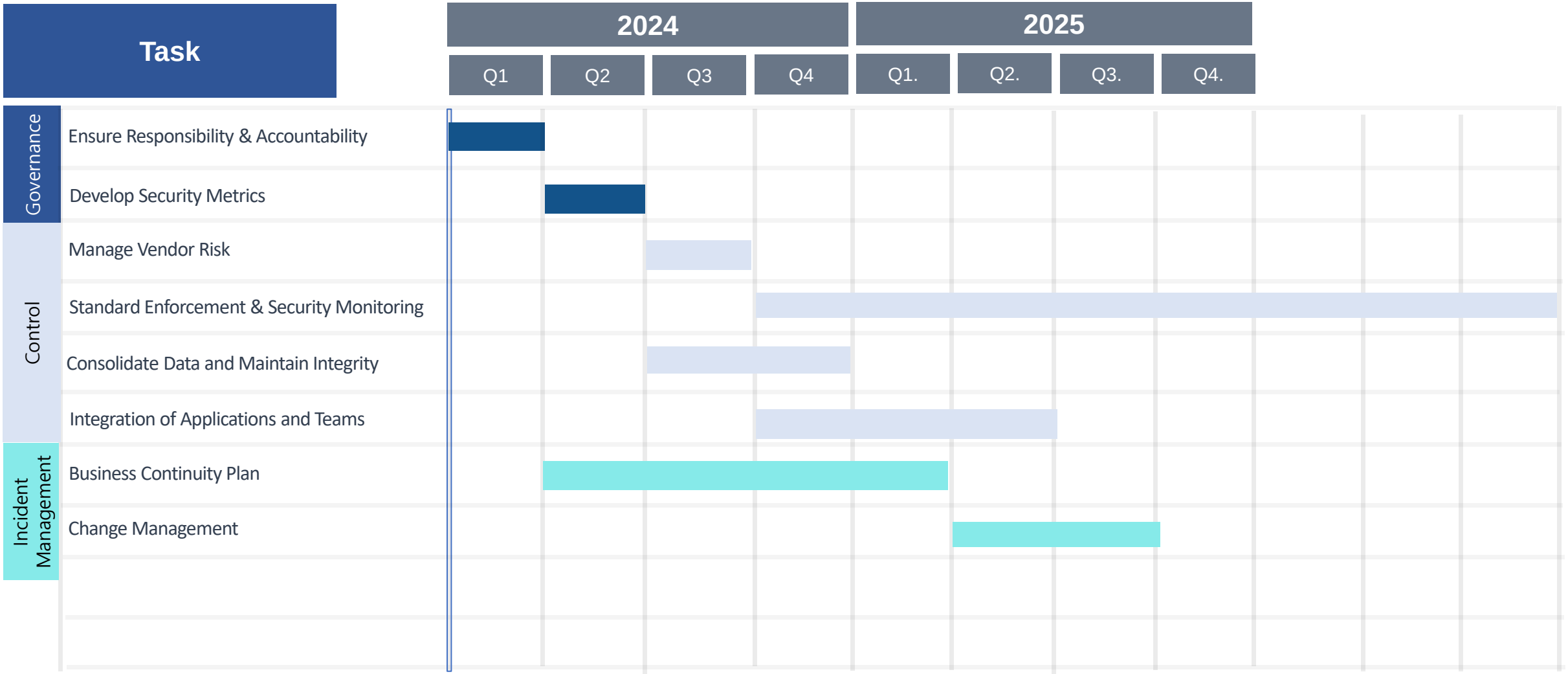
- Identify security incidents and classify them into groups based on the severity or impact on operations [DSS02]
- Establish knowledge resources and provide extensive Training for the team [DSS02]
- Handle all incidents formally with access to all relevant data [DSS03]
- Define appropriate support teams to assist with root cause analysis and optimal solution determination [DSS 03]

https://www.salvagedata.com/phases-of-an-effective-incident-response-plan/
https://www.salvagedata.com/data-recovery-services/
COBIT 2019 Framework: Governance and Management Objectives

Quarterly Key Milestones & Capability Improvements

2024 Q1	2024 Q2	2024 Q3	2024 Q4
Dedicated Security Department	Security Metrics Established	Configured and Integrated Nudge Security into SSR's System	Consolidate Data and Maintain Integrity
2025 Q1	**2025 Q2**	**2025 Q3**	**2025 Q4**
Business Continuity Plan Complete	Integration of Applications and Teams Completed	Change Management Process Finished	Monitor Enforcement and Security

A 2 Year Blueprint for Developing Governance, Controls, and Incident Management



Financials

Ensure Security Quickly and Cost Effectively

Cost Breakdown:

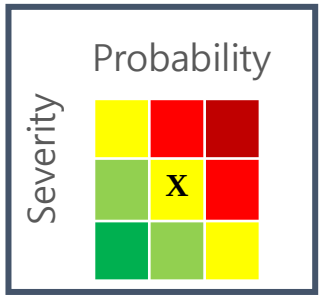
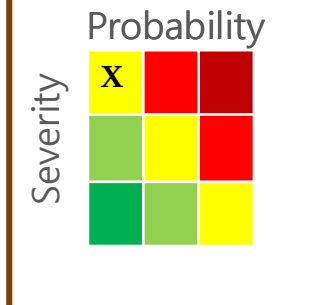
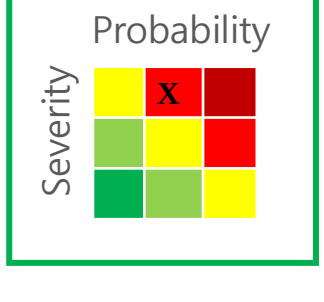
Cost	Amount	Type	Frequency
Vendor Risk Management Platform Subscription	$2-3 per verification minimum 150 users	Recurring	Monthly
Labor	$300K-350K	Recurring	Monthly
Security Monitoring Capabilities Enhancement	$150K	Recurring	Quarterly
Data Consolidation	$400K – $1M	Upfront	N/A
Integration and Collaboration	$100K	Upfront	N/A
Data Recovery Service	$40K	As Needed	N/A

https://www.capterra.com/resources/risk-management-software-pricing-report/

https://www.scnsoft.com/analytics/data-consolidation#:~:text=Data%20Consolidation%20Project%20Costs&text=Small%20companies%3A%20%2470%2D200K,Large%20companies%3A%20%24400%2D1%2C000K

Risks & Mitigations

Operational and Compliance Consequences Might Occur Without Proper Planning

	Risk	Degree	Mitigation
Governance	• **Communication Breakdown** Shifting responsibilities can cause disruption in communication channels inside the organization.		• Be transparent in all communications with employees and higher up business personnel • Communicate the hierarchy of responsibility for all aspects of the operational model to all employees of SSR
Control	• **Reliance on a Single Data Repository** Relying on a single vendor for a centralized system can restrict current flexibility and future innovation • **Regulatory Compliance** Failure to comply with legal boundaries can result in regulatory and financial consequences.		• Ensure that when a contract with a repository vendor ends, all data is backed up and able to be transferred to a new system • Do research on the legal landscape of all regions SSR will operate in
Incident Management	• **Loss of Essential Data During Recovery** Losing data in the event of a security breach can be devastating to companies and result in financial and legal concerns.		• Align with data protection regulations (ISO27001/ISO27002, NIST CSF, COBIT, etc.) • Partner with third-party data recovery vendor to minimize risk of data loss

business.com/articles/rfid-for-retail/
holisticai.com/blog/recommendation-systems

A Proactive Step to Shape SSR's Future

With the presence of cyberthreats to companies in any industry, a sound cybersecurity practice is vital to an organization's long-term health.

Preventing against any incoming cybersecurity threats is key to ensuring business continuity, financial safety, and overall protection from outside threats if these standards are in place.

Following all steps of the recommendation will ensure the highest level of confidence possible to protect against future attacks and help sustain **Shop, Stop, and Roll** as a prominent figure in their industry for years to come.

Thank you!