STOP, SHOP, AND ROLL, INC: Cybersecurity Proposal

October 4th, 2019

Team 25 Consulting

Our Team

Terry Bae

Terry is from South Korea. Terry enjoys reading the news, working out at the gym, and drinking copious amounts of coffee.

Arpita Bali

Arpita is from India. Nature, adventure and wildlife are the great things that get her heart racing. Vroom!!!

Max Bublick

Max is from Carmel, Indiana. Max loves to travel and a good punch line.

Austin Rodgers

Austin is from Chicago and is passionate about football (BEARS!) and enjoying a cold one with his team members.

Agenda

- Understanding the problem
- Gap Analysis
- Cybersecurity Capability Maturity Analysis
- Recommendation
- Timeline
- Financials
- Risk analysis and risk mitigation
- Conclusion
- Appendix

Understanding the problem

Stop, Shop, and Roll, Inc. (SSR) is a new company formed in 2014 from the merger of three retail giants: Stop-n-Save, Shopology and Roll With It.

After the merger, there has been a lack of a central IT security system and Cybersecurity governance due to which Stop, Shop, and Roll, Inc. was a victim of a major Cybersecurity breach.

How can the SSR up-lift its cybersecurity function, establish an IT Security governance, and organization?

Gap Analysis

Current

- From the merger, three companies have different security practices
- Low budget for security
- Inefficient vendor management

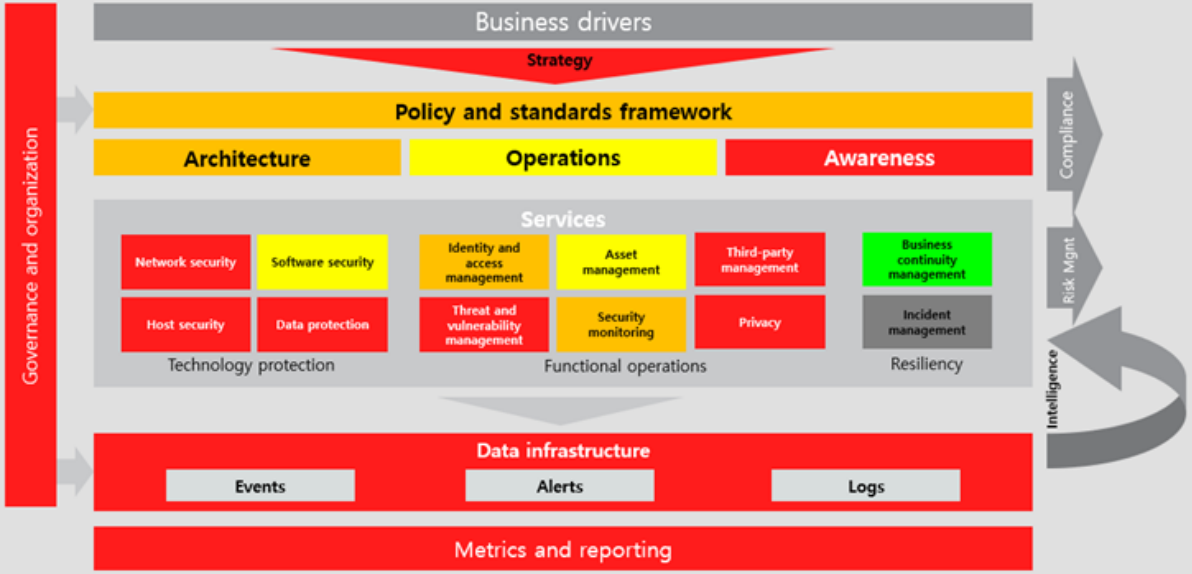
GAP

- Lack of governance
- Lack of incident management process
- Lack of awareness in security issues

Future

- Team dedicated to cyber security
- Policy and standards
  - Preventative measures to secure data
  - Reactive processes to security alarms
- Adequate budget for IT security
- Consolidated vendors

Capability Maturity: Current State of SSR Inc.



Rating	Definition
1	**Initial** Basic, ad-hoc, undocumented; changing capability may be in place with some technology and tools; limited local processes; limited organizational support.
2	**Managed** Partial capability is in place with a combination of some technology and tools; local processes covering some regions/business units or processes are repeatable but may not be good practice or maintained; limited organizational support to implement good practice.
3	**Defined** Defined capability is in place with significant technology and tools for some key resources and people; processes defined for some regions and/ or business units; organizational guidance and support is in place for some key regions and/or business units.
4	**Quantitatively managed** Mature capability is in place with advanced technology and tools for most key resources and people; consistent processes exist for most regions and/or business units; some governance is in place (accountability/responsibility/metrics) for most key regions and/or business units.
5	**Optimizing** Advanced capability is in place which is leading-edge technology and tools for all key resources and people; consistent process across regions and business units; effective governance is in place (accountability / responsibility/continual monitoring for improvement).

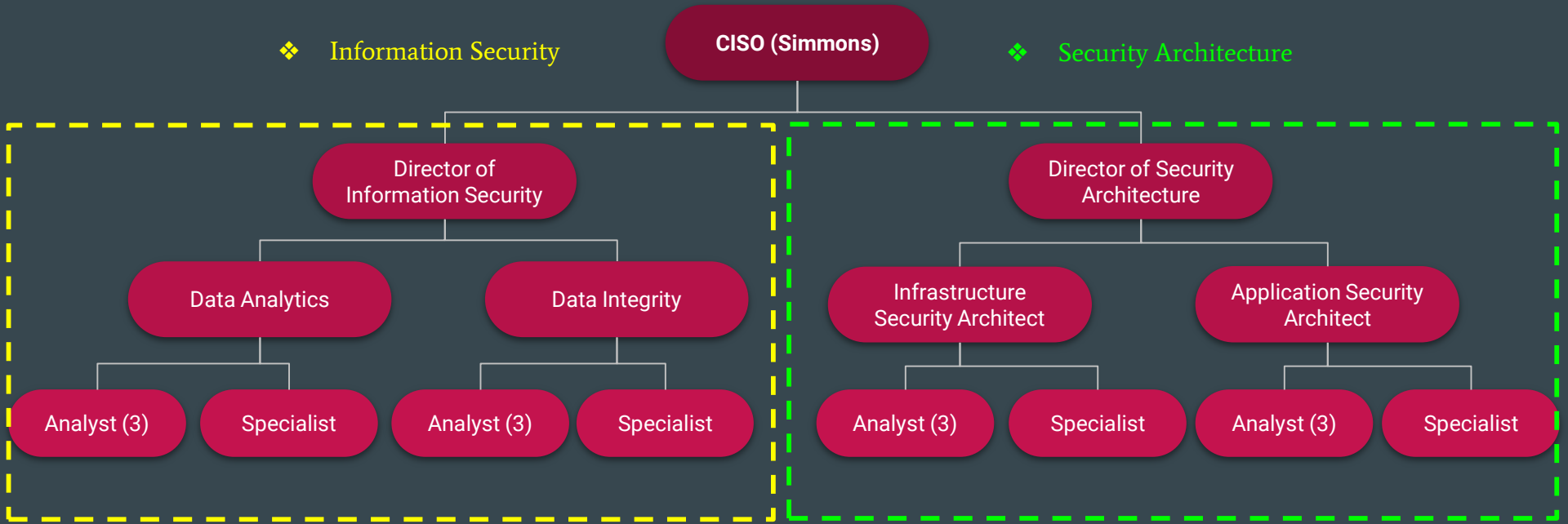
Recommendation

Our recommendation to SSR Inc. is to create a Cybersecurity initiative that focuses on:

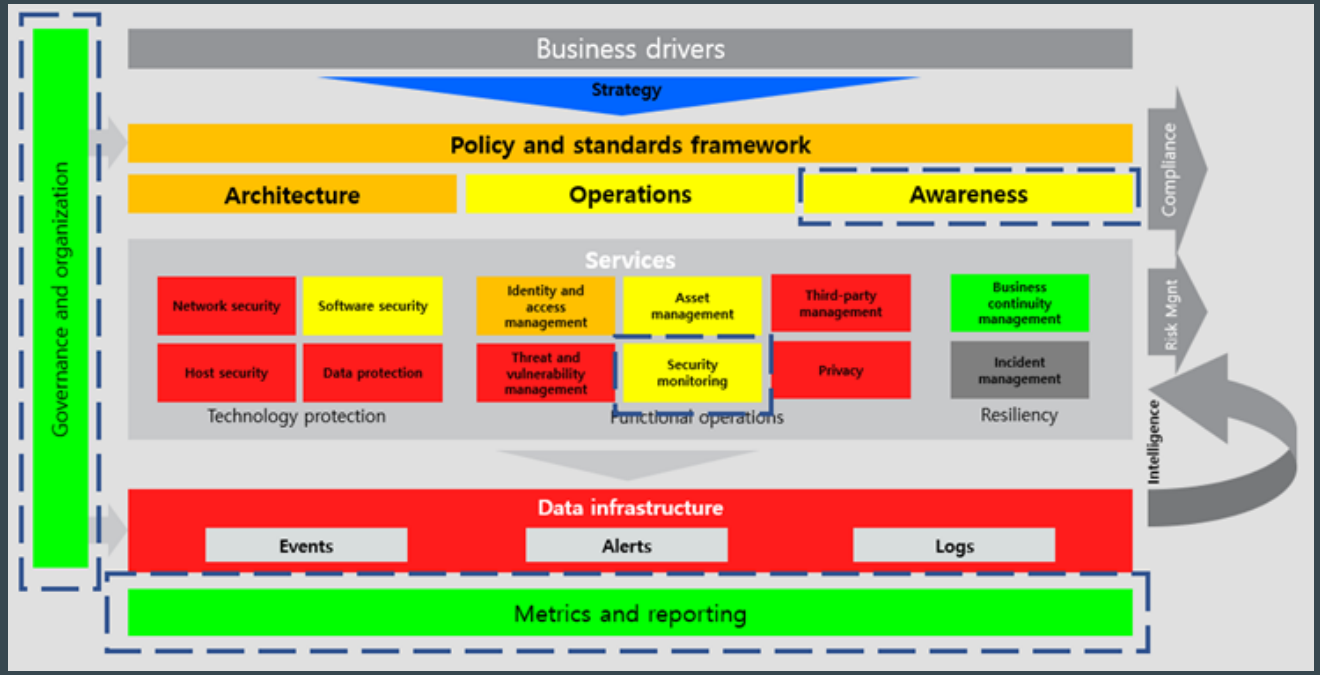
- IT Security organization and governance
  - Establishing an organization structure
  - Appointing IT Security Team and CISO
  - Budget allocation for security
  - Better governance over security monitoring
- Central Security System (Packaged security solution)
  - A central security system addressing key security functions:
    - Threat and Vulnerability
    - Identity Access Management
    - Data Protection and Privacy
    - Network and Host Security
    - Security Monitoring
    - Architecture
  - Raise the capability maturity of the SSR cybersecurity function
- Policies and Standard frameworks
  - Establishing mission and vision statement
  - 3rd party vendor selection criteria
  - Awareness around security

Governance Analysis

Promote Jean Simmons to CISO → Build New Security Team → Form Security Team Hierarchy



Capability Maturity after Governance Implementation



Cybersecurity Analysis

	Security solutions & Vendors	Threat and Vulnerability	Identity and Access Management	Data Protection & Privacy	Network Security	Architecture	Host Security	Data Infrastructure
1	Symantec: Cybersecurity solution for retail	✓	✓	✓	✓	✓	✓	✗
2	Microsoft Security: Azure Advanced Threat Protection	✓	✓	✗	✗	✗	✗	✗
3	Symantec: Zero Trust Protection	✗	✓	✓	✗	✗	✗	✗
4	Fortinet: NextGen Firewall NGFW	✓	✗	✗	✗	✗	✗	✓

Implement a central IT Security system

Ensures consistent IT security across all SSR offices

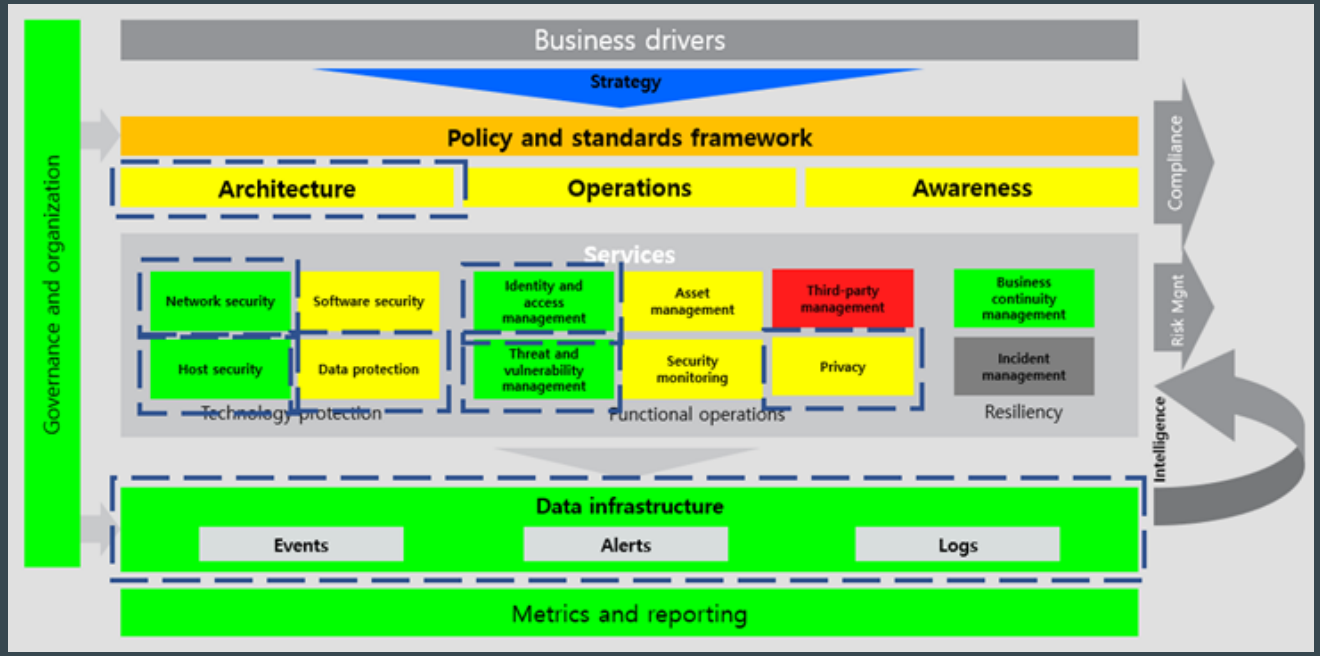
Select security solutions that addresses key issues listed

Conduct RFP from Vendors for security solution

Raises the capability maturity of the SSR cybersecurity function

Form committee for Cybersecurity vendor selection - *CISO (Jean Simmons), CIO (Jason Piggott), New directors under CISO, Senior management from all business units*

Capability Maturity with central Cybersecurity system



Policy and Standard Frameworks Analysis

MISSION

"Through our new governance and cybersecurity methods, we strive to define security performance standards by guiding our employees to help establish our secure framework"

VISION

"We strive to create a more secure network so our customers can shop without worry"

Data protection and privacy law compliance

Compliance with laws such as GDPR, HIPAA and security standards such as PCI, ISO and NIST

Preventative and reactive security measures

Security measures must be adopted by 3rd party vendor systems for threat prevention and IT risk mitigation

Accurate and thorough description of data flow

What services will the vendor provide?

What customer, employee, and company data and information will the vendor collect and/or have access to?

Where will this data and information be processed and stored?

Encrypted data

Sensitive company, employee or customer data should be encrypted on Vendor's storage media, portable devices like laptops and smartphones.

3rd party vendor selection security criteria

Annually assess vendor security, verify vendor contracts, monitor vendor risk

Building awarenesses around security

COMMUNICATION:

Make security a part of conversation through company-wide emails and presentations

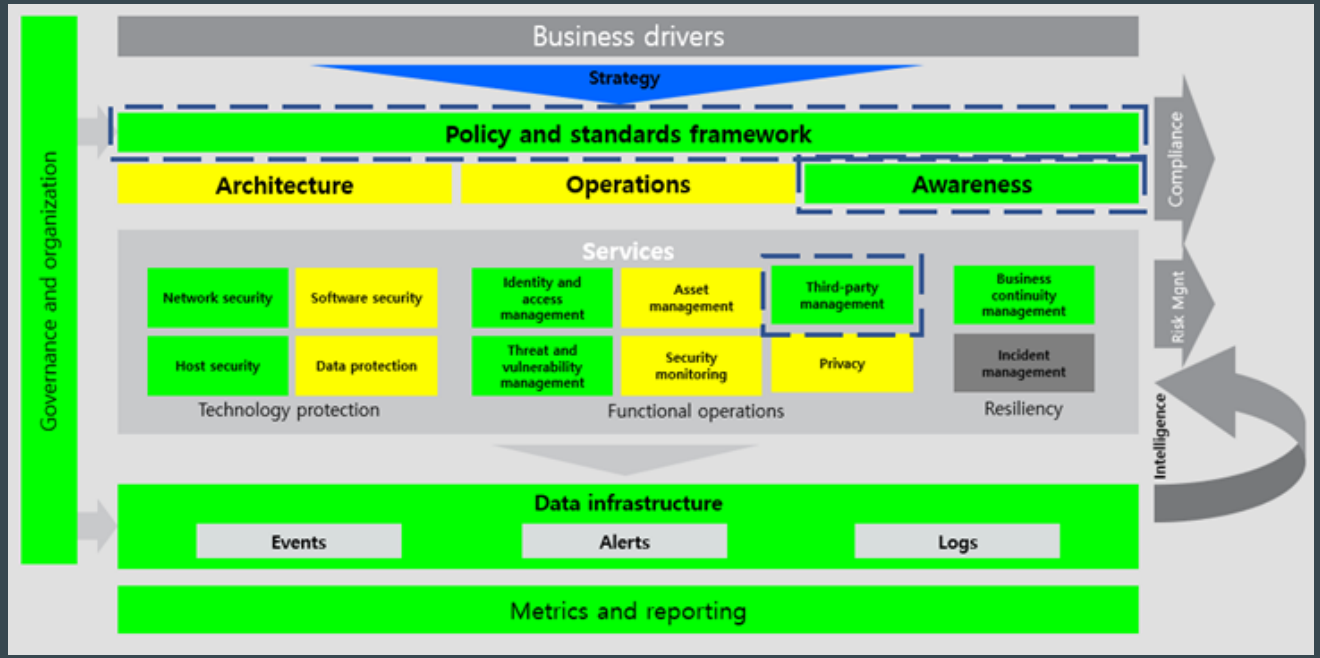
CONTENT:

- A PDF security handbook
- Chat channel for reporting suspected security issues
- Training programs for new hires

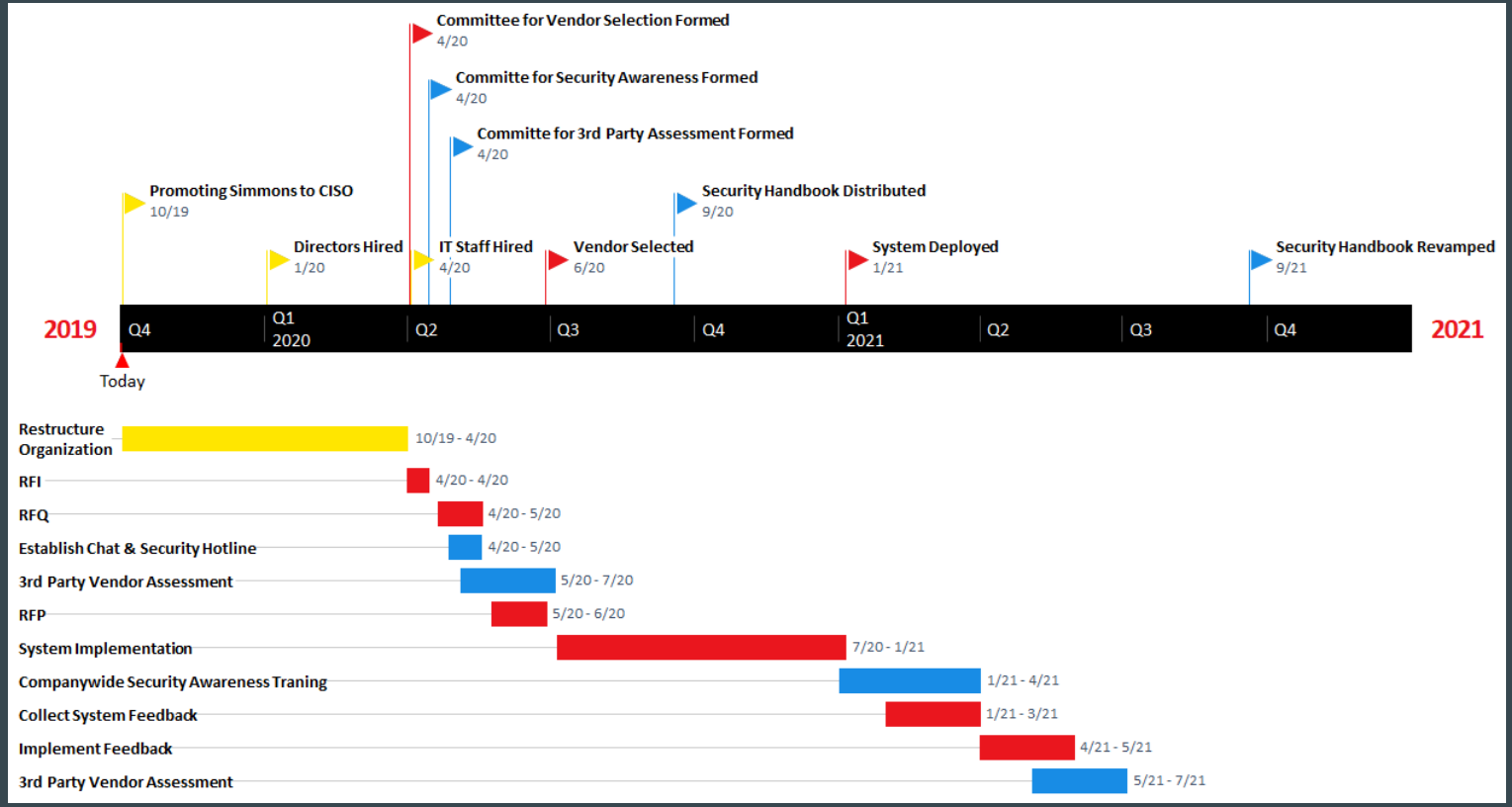
CONTROLS:

Ensuring that people and systems are only able to do what their roles dictate and only with the appropriate approval.

Capability Maturity after Policy and Standards Frameworks



Timeline



Reorganization and governance

Cybersecurity system

Policies and standard frameworks

Financials

$2,260,000	Salary expenditures for IT team
$16,000,000	Security alert triage
$96,000	Rebuild infected machines
$30,000	Emergency patching
$160,000	Advanced threat protection
$44,000	Next-generation antivirus software
$30,000	Whitelisting/blacklisting solutions
$112,000	Denotation environments
$18,732,000	Total Cost

Risk analysis and risk mitigation

SCALE OF LIKELIHOOD	ACCEPTABLE	TOLERABLE	GENERALLY UNACCEPTABLE
NOT LIKELY	Human error	Accidental internal hacking	Failure to detect data breach
POSSIBLE	Adjustment Period	Lack of security knowledge	Data Breach
PROBABLE	User Resistance	Difficulty diagnosing attack	Overconfidence in the system

SCALE OF SEVERITY

Mitigations

- Breaches can be detected quicker and on a bigger scale, potentially solving a problem before it even starts
- Be up to date on security trends and hacking activities
- Know what information is valuable and plan accordingly
- Do not let an iron defense stem overconfidence, always be vigilant
- Take budget beyond assumed risks
- Test, test, and test again

Conclusion

Governance

Build a cybersecurity team to tackle current and future security concerns

System

Strategically select security system vendors to keep safe from future breaches

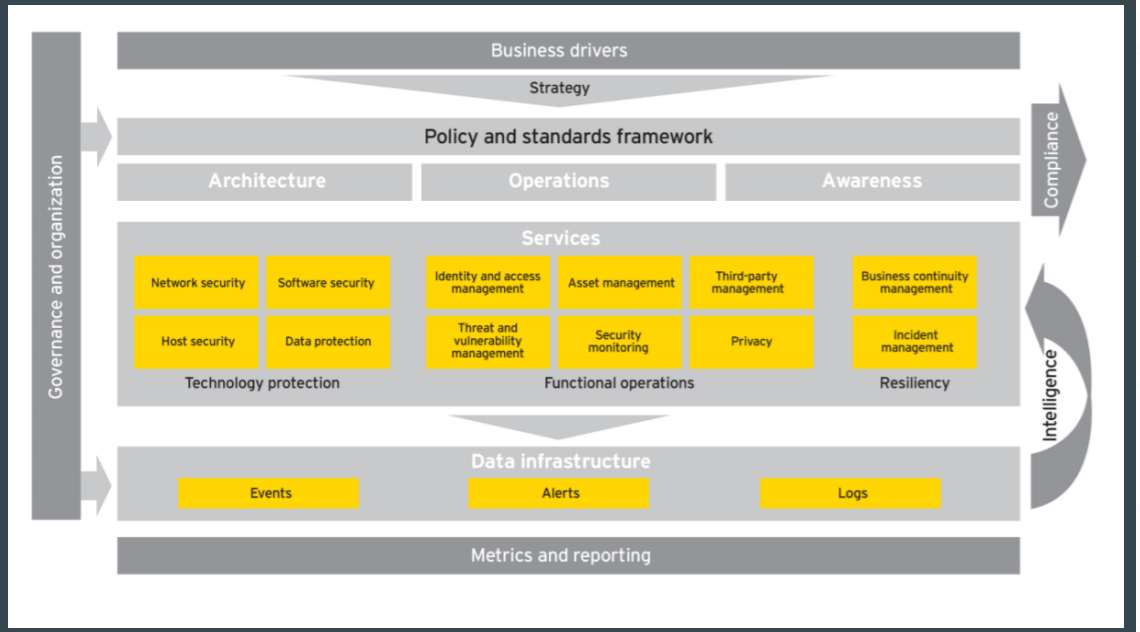
Policy & Standards

Articulate the changes, train employees and engage everyone to abide by new policies

Appendix

- Cyber Program Management (CPM) Framework
- Vendor security assessment plan
- Available third-party vendor assessment programs
- SSR Committees
- Individual role salary
- Individual role description
- Average cost of IT Security

Cyber Program Management (CPM) Framework



Rating	Definition
1	**Initial** Basic, ad-hoc, undocumented; changing capability may be in place with some technology and tools; limited local processes; limited organizational support.
2	**Managed** Partial capability is in place with a combination of some technology and tools; local processes covering some regions/business units or processes are repeatable but may not be good practice or maintained; limited organizational support to implement good practice.
3	**Defined** Defined capability is in place with significant technology and tools for some key resources and people; processes defined for some regions and/ or business units; organizational guidance and support is in place for some key regions and/or business units.
4	**Quantitatively managed** Mature capability is in place with advanced technology and tools for most key resources and people; consistent processes exist for most regions and/or business units; some governance is in place (accountability/responsibility/metrics) for most key regions and/or business units.
5	**Optimizing** Advanced capability is in place which is leading-edge technology and tools for all key resources and people; consistent process across regions and business units; effective governance is in place (accountability / responsibility/continual monitoring for improvement).

Vendor security assessment plan

- Determine scope of data
  - Determine the type of data or information that is most important to protect, including customer data and employee information.
  - Determine sensitivity of company data
- Determine flow of data
  - What services will the vendor provide?
  - What customer, employee, and company data and information will the vendor collect and/or have access to?
  - What will the vendor do with this data and information?
  - Where will this data and information be processed and stored?
  - How will the data get to the vendor?
  - Will any subcontractors be used?
- Third party vendor assessment programs to send, receive and process assessment data.
- Review assessment and update the business unit and vendor accordingly
- Take inventory of vendors that SSR utilizes and determine whether or not they have been assessed.
- Conduct vendor security assessment annually

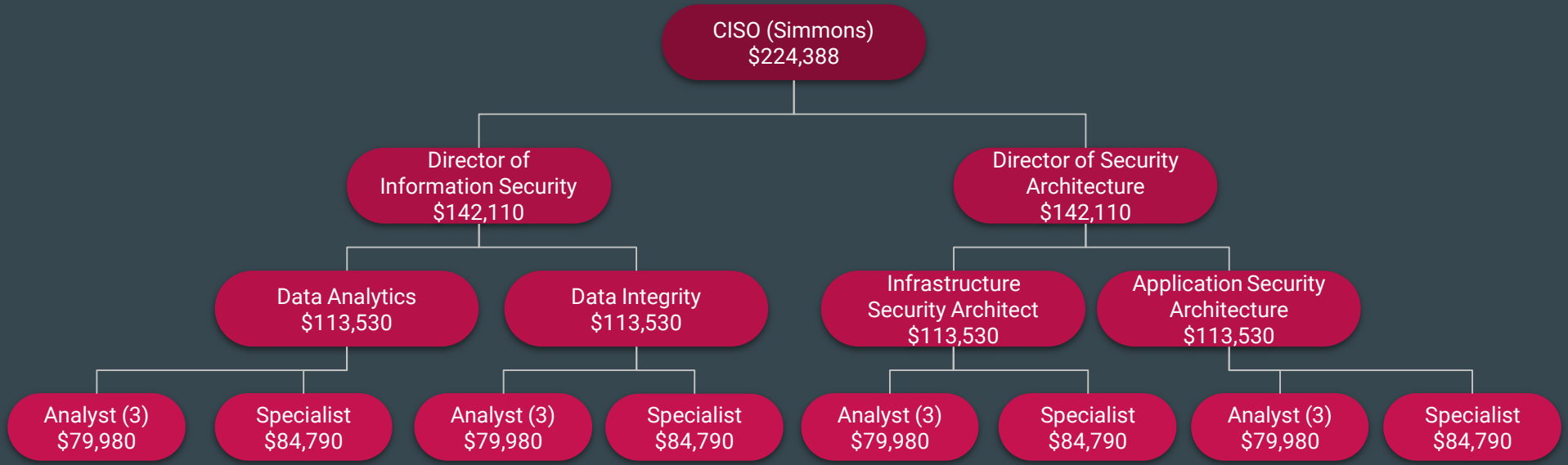
Available third-party vendor assessment programs

	01 UpGuard VendorRisk	• Monitor vendors • Vendor security ratings • Automate security questionnaires • Prioritize and remediate risks
	02 Whistic	• Identify vendors • Access potential cybersecurity threats • Track vendor security information
	03 Venminder	• Identify areas of possible weaknesses • Meet regulatory requirements • Comprehensive cybersecurity and information security risk assessment for each vendor

SSR Committees

- Committee for Cybersecurity vendor selection - *CISO (Jean Simmons), CIO (Jason Piggott), New directors under CISO, Senior management from all business units*
- Committee for 3rd party vendor selection- *CISO (Jean Simmons),Legal team, IT's senior management,, Senior management of impacted business units*
- Committee for raising security awareness- *HR, CISO, volunteer employees*

Individual Role Salary



Individual Role Description

Director:	**Security Architect**	• Establishes disaster recovery procedures and conducts breach of security drills • Reviews current system security measures, recommends and implements new enhancements
Manager:	Infrastructure Security Architect	• Perform vulnerability testing, risk analyses and security assessments • Test final security structures to ensure they behave as expected
Manager:	Application Security Architect	• Support of application development, infrastructure, and enterprise technology projects to ensure the integrity of the SSR architecture • Identify any gaps in existing application security infrastructure to meet project requirements
Director:	**Information Security**	• Manages security programs and supervise security departments • Ensures policies, procedures and protocols are being executed
Manager:	Data Analytics	• Design and build technical processes to address business issues • Examine, interpret and report results of analytical initiatives to stakeholders in leadership, technology, sales, marketing and product teams
Manager:	Data Integrity	• Maintain customer and contact database including additions, deletions, research, corrections and cleaning • Implement controls and compliance metrics to reduce data issues and improve data quality

Average cost of IT security

Simple conversion between revenue and company net worth

Approximate Revenue = Company value / 4

Average enterprise IT budget = 3.2% of Revenue

Average IT security budget = 10% of IT budget

$25 billion /4 = $6.25 billion Revenue

$6.25 billion * 3.2% = $200 million IT budget

$200 million * 10% = $20 million Security budget

Works Cited:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Compliance/Compliance_DG/PCI_Compliance_DG/ch2_PCI.html

https://www.symantec.com/solutions/retail

https://www.symantec.com/solutions/zero-trust-ecosystem

https://blog.whistic.com/top-10-tips-for-effectively-assessing-third-party-vendors-9eb35a08f796

https://www.threatstack.com/blog/how-to-implement-a-security-awareness-program-at-your-organization

http://certmag.com/salary-survey-extra-salaries-job-hierarchy/

https://www.ccsinet.com/blog/common-security-risks-workplace/

https://championsg.com/12-steps-mitigate-cyber-threats

https://www.darkreading.com/cloud/it-takes-an-average-of-3-to-6-months-to-fill-a-cybersecurity-job/d/d-id/1334135

https://www.careerexplorer.com/careers/information-security-director/#targetText=Information%20security%20directors%20are%20in,security%20measures%20throughout%20an%20organization.&targetText=Responsibilities%20of%20an%20information%20security,Allocate%20resources%20correctly%20and%20efficiently

Works Cited:

https://www.roberthalf.com.au/our-services/it-technology/security-architect-jobs#targetText=A%20Security%20Architect%20job%20description,and%20recommending%20and%20implementing%20enhancements&targetText=Ensuring%20all%20personnel%20have%20access,conducting%20breach%20of%20security%20drills

http://www.isaca.org/chapters1/Calgary/newsandannouncements/Documents/Application%20Security%20Architect-UoC.pdf

http://www.laerdaltraining.com/HumanResources/DataIntegrityManagerJD.pdf

https://www.quora.com/How-much-yearly-revenue-or-profit-would-make-a-company-worth-1-million

https://blog.techvera.com/company-it-spend

https://www.blackstratus.com/how-much-should-your-company-invest-in-cybersecurity/