Stop, Shop, and Roll

How not to lose in the new cybersecurity landscape.

Project Team: Charles A. Hulebak, Will Bobe, Alivia Coon, Edward Kim

Table of Contents

Background

Background

Stop, Shop, and Roll, Inc. (SSR) is a mega corporation formed from the merger of three large companies. Despite optimistic projections about IT synergies resulting from the merger, the blending of the IT departments has been difficult, symbolized by the hiring and firing of 3 separate CIOs. Successive cost cutting and consolidating measures implemented by these CIOs have left the Cybersecurity department dangerously unprepared for the current threat landscape.

This lack of preparation led to monday's disastrous Ransomware incident and related Data Breach. Luckily Stop, Shop, and Roll merely needs to Stop, Drop, and Roll by instituting (1) good incident response, and (2) a plan to mature cybersecurity capabilities.

Key Issues and Complicating Factors

Simmons made 12 observations that highlight a deep lack of cybersecurity maturity in SSR.

1. No IT Strategy
2. No Policy Enforcement
3. A disconnect between Compliance and Security.
4. IT Operations doesn’t conduct investigations
5. No vetting of Third Parties
6. No centralized asset repository
7. No formal incident management process
8. Too many passwords
9. No logs
10. No BCP.
11. Nowhere to report.
12. No staff, small budget.

The Problem and How to Solve it

SSR currently faces two problems:

1. How to respond to the Ransomware and Data Breach Incident; and
2. How to develop and mature SSR's Cybersecurity Capabilities.

Thankfully, many other companies have dealt with similar problems in the past, and various solutions exist. Namely, the Cybersecurity Program Management Framework (CPM).

Incident Response

The Threat

What are we dealing with?

Landscape

Enemy

Tools

The Threat: Landscape

Although the current incident was caused by Ransomware, merely focusing on a single threat will not prepare the company to deal with the multi-form, phased, and varied attacks which will hit vulnerable companies from every direction.

Malicious actors are legion, as are their tools of cyber-mischief.

The Threat: Enemy

Many adversaries exist in cyberspace. They may range from “script-kiddies” who use minor vulnerabilities to troll for fun, to “advanced-persistent-threats” posed by state actors who have nearly unlimited human and financial capital to penetrate your system, steal your data, and destroy your company.

The current ransomware attack may have come from a hacker who purchased the vector of attack online from a dark-net broker, or even from the Russian or Chinese government.

The Threat: Tools

Spyware, Ransomware, Phishing, Spear-Phishing, Cat-Phishing, Whaling, Trojans, Viruses, Insider-Espionage . . . just to name a few.

The tools and techniques malicious actors use to penetrate your system, steal your data, and destroy your integrity are varied.

According to most cybersecurity professionals, every major company either knows it has undergone a cybersecurity incident, or hasn’t discovered it yet.

The only defense, beyond reverting to the stone age, is preparation and having a good Incident Response Framework in place to mitigate the damage to continue business operations.

The Response

Putting out the fire.

Introduction

Your Team + RACI

Your Plan

The Framework (17 - 24)

The Timeline

The Budget

Conclusion

Intro: How to Respond

Like any good project, you will need to pick your **team**, and develop your **plan**. Once you have your team and your plan, you will need to **execute** as fast as possible to contain the threat.

Your Team

A Cross-Functional Incident Response Team will be essential to make sure you cover all your bases.

1. Info Security Staff (ISS): to handle investigation of the incident.
2. IT Staff: to help the ISS with specialized knowledge of apps/systems.
3. Legal Representative: legality of searches and contacting law enforcement.
4. Business Representative: to help ISS understand business implications.
5. Communication Representative: to speak for the company.
6. Incident responders: for specialized expertise to help ISS.
7. Breach notification providers: to comply with breach notification laws.

RACI: Who is responsible for what?

Action / Responsible Party	Coordination	Logs (analysis and gather)	Forensics	Emergency Change Management	Technical Assurance	Monitoring and investigation	Law enforcement liaison	Media Messaging	International Messaging	Staff Messaging	Customer Messaging	Partner Messaging
CIO/CISO/CPO	A			I	I	I	I	I	AR	AR	I	AR
Director of Cybersecurity	R	I	I	A	A	I	I	C	C	C	C	C
IT Operations	I	I	I	R	R							
Enterprise Architecture	I			R	R							
Enterprise Risk Management	I	I	I	I	C							
Internal Audit	I					I						
Internal Investigations	I	AR	AR	C	I	AR	AR					
Forensic Services	I		R			R						
Law Department	I					C						
External Legal Counsel	I											

R = Responsible *= The person who performs the work. There must be one "R" on every row, no more and no less. "R" is the only letter that must appear in each row.*

A = Accountable *= The person ultimately accountable for the work or decision being made. Use this letter where appropriate, but not to excess – only when a key decision or task is at hand. There can be from zero to one "A's" in each row, but no more than one.*

C = Consulted *= Anyone who must be consulted with prior to a decision being made and/or the task being completed. There can be as many "C's" as are appropriate in each row.*

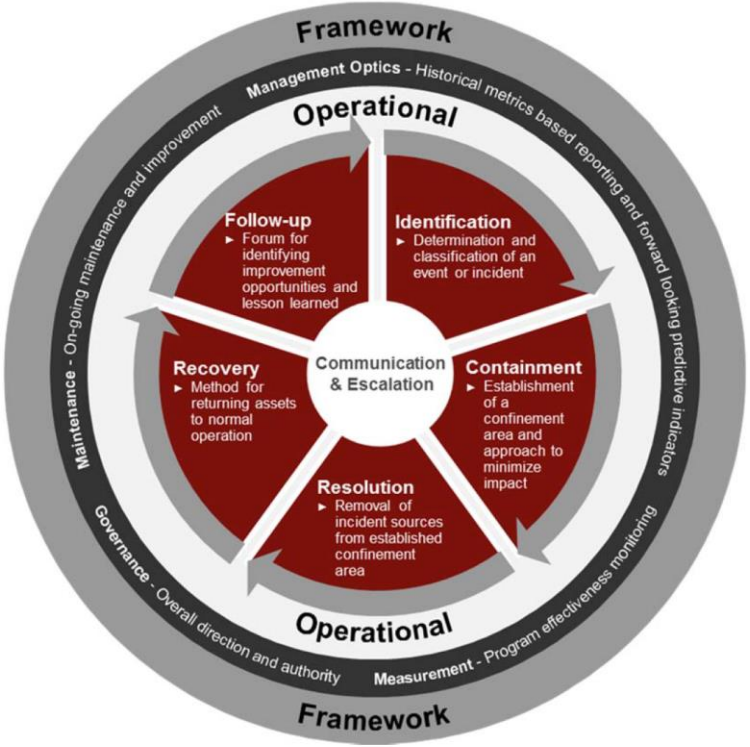
I = Informed *= Anyone who must be informed when a decision is made or work is completed. There can be as many "I's" as are appropriate in each row.*

https://www.healthprivacyforum.com/sites/healthprivacyforum/files/cybersecurity_incident_response_-_how_to_survive_an_attack.pdf

Your Plan: Incident Response Framework

A company must attempt to reduce chaos and formalize incident response procedures. Incident response typically follows a lifecycle, and is formalized as to provide effective and immediate response to minimize damage to a corporation. Typical steps include:

1. Identification,
2. Containment,
3. Resolution,
4. Recovery,
5. Follow-up



Understanding the Framework

The Framework is easy to understand:

1. The identification phase deals with determining that there is an incident.
2. The containment phase is in place to prevent further damage from occurring.
3. The resolution phase involves performing actions to eradicate the issue.
4. The recovery phase involves performing actions to return to normal operations.
5. The follow-up phase consists of lessons learned, including a summary of the incident and details of the other phases.

Identification

Identification: Where is the fire?

- Windows servers are reported to be impacted by the ransomware attack
- At least the C-suite computers are reported to be impacted by the ransomware attack
- There appears to be a data breach as reported by Special Agent Leonard

It is important at this stage to establish documentation. Documentation should continue throughout the IR process.

References:

https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Containment 1 of 3

Containment: Making sure the fire doesn't spread.

- Attempt to isolate the affected machines from the rest of the network
  - This will help prevent the spread of the ransomware
  - E.g., remove the affected machines from the network by pulling the ethernet cable
- Identify and patch any other potential vectors that are operating in the production environment
  - E.g., machines running the same software suite, improperly configured firewalls, routers and other devices

https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Containment 2 of 3

- Hire an external Information Security Team (IST)
  - Due to budget cuts, there is no dedicated Information Security Team in place with experience in investigating and responding to incidents.
- Assign Legal and Business representatives that are familiar with the business to guide the IST.
- Hire a Public Relations, and Breach Notification firms to handle the fallout from the Incident.

Containment 3 of 3

- Take a forensic image of any machines that will be reimaged or otherwise replaced
  - This will help maintain any evidence in an unaltered state which will be vitally important in the event of litigation
  - Should be performed by an external source
    - Cost between $5,000 and $15,000 for typical cases, but can cost up to $100,000 (https://www.vestigeltd.com/thought-leadership/digital-forensic-services-cost-guide-vestige-digital-investigations)

Containment should happen as fast as possible to prevent further damage. This is especially true of the isolation.

https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Resolution

Resolution: Putting out the fire.

Penetration of Systems

- Cleaning and re-imaging hard drives
- Hardening systems and network against attacks
  - Including thorough patching and removal of vulnerabilities

Dealing with Aftermath

- Ensure the Breach Notification Firm is in communication with the IST and has all necessary information in regards to the Breach.
- Hire a law firm to settle subsequent litigation matters.

https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Recovery

Recovery: Rebuilding the house.

Penetration of Systems

- Restoring previously affected machines to production
  - This phase requires testing, monitoring, and validation that the machines are clean and ready to be returned to production

Dealing with Aftermath

- Work with the PR firm to restore investor and consumer trust in the brand.

https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Follow-up

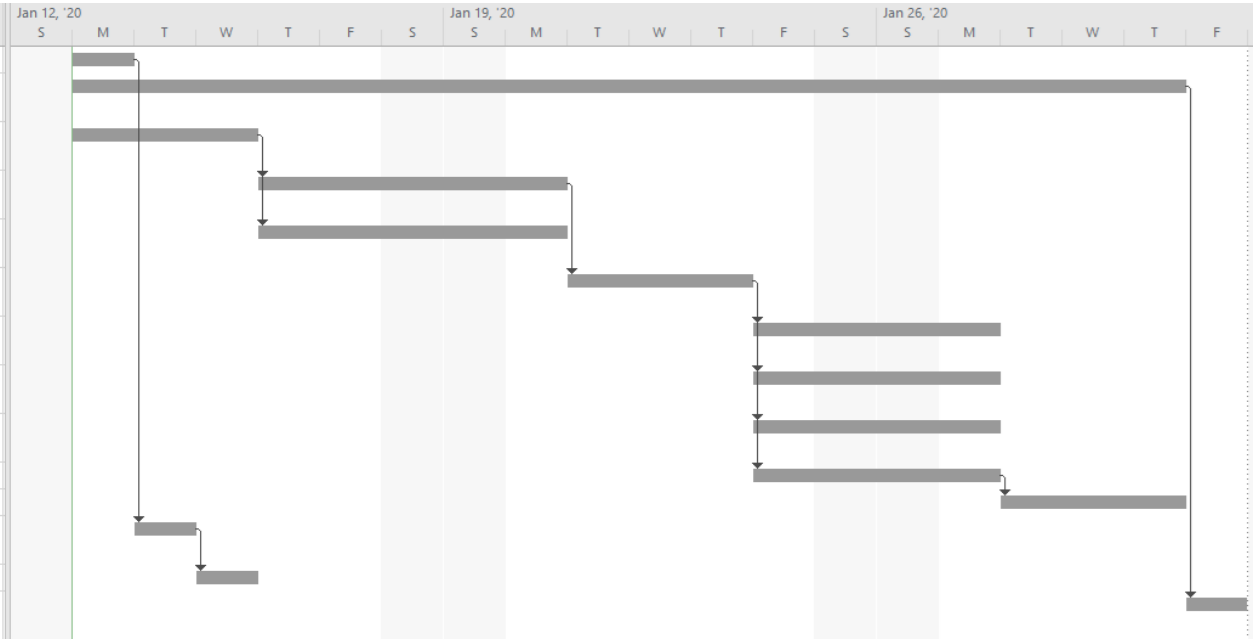
The follow-up phase: Making sure this doesn't happen again. The follow-up should have:

- When and by whom the incident was detected
- How widespread and impactful the incident was
- Steps taken to contain and eradicate the issue
- Steps taken for recovery
- Positive feedback
  - What went well?
- Negative feedback
  - What could have been done better?

https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

2 Week Timeline

Task Name
Assess Ransomware threat with stakeholders
Log all communication; changes to network, devices add/removal, software installation; initiate process, previously not enforced
Identify unique characteristics of the variant; Utilize a resource (i.e. ransomware.malwarehunterteam.com) to identify the variant
Identify all computers and servers infected by the ransomware; review files for access date and modification; take all systems offline until fully scanned
Review firewall logs and egress filtering to ensure that all impacted machines have been identified
Remove infected computers from the network to limit the impact and spread (isolate incident)
Isolate backup media, online media (policy should be in place before incident to ensure recovery without paying the ransom)
Review security measures that failed (i.e. antivirus), and provide samples to identify and protect intrusion
Review backup processes and identify data that cannot be recovered and potential impact to business
Forensic image of all systems subject to incident
Recover the data on the network and rebuild machines as required
Research alternative approaches to resolve ransomware impact; i.e. decrypt ransomware files, etc.
Consider (at a last resort) payment of the ransom
Post Incident review-What was found during the investigation and recommended changes/adjustments to network



https://www.sans.org/reading-room/whitepapers/ActiveDefense/ransomware-37317

Budget for this particular Incident

Following this ransomware attack, SSR will have to consider many financial factors, including the direct cost of the ransom payment, and indirect costs associated with downtime, reputation loss, liability, collateral damage, and data loss. Monetizing these factors, SSR could expect the following financial loss:

Type of Loss	**Cost of Loss**
Direct cost: ransom payment	10M
Indirect cost: enforced downtime	961M
Indirect cost: reputation loss	1.25B
Indirect cost: liability	1.25B
Indirect cost: collateral damage	135M
Indirect cost: data loss	270M
Total Loss	**3.877B**

Refer to Addendum A for calculations

https://digitalguardian.com/blog/whats-cost-data-breach-2019
https://www.sentinelone.com/blog/what-is-the-true-cost-of-a-ransomware-attack-6-factors-to-consider/

Conclusion to Incident Response

Creating an effective team of internal and external responders, and implementing the incident response framework will put out this particular fire. A quick and decisive response will mitigate damage to the company’s finances and public reputation. However, in order to better prepare for the inevitable next attack the company needs to improve its Cybersecurity Program.

Cybersecurity Program Improvement

Introduction

The basics.

Why do we care?

CPM Maturity Model

CPM Framework

Why do we care?

Experts have recently coined the term “cyber fatality” to describe corporations that have been put out-of-business by an especially devastating cyber attack. Just this monday, SSR suffered what may turn out to be a Merck-level incident, which ended up costing that company around 1.3 billion dollars.

There is nothing stopping the Ransomware hackers from attacking SSR again, a few weeks after we restore all the systems from backup. The only defense is to advance SSR’s cybersecurity capabilities to an acceptable level.

For more information on Merck cyber attack. See https://www.insurancejournal.com/news/national/2019/12/03/550039.htm

CPM Maturity Model

The CPM Maturity Model shows how developed a corporation's cyber defense capabilities are.

Currently we are at a 1. There are no logs, no dedicated cybersecurity department, and the IT Operations staff doesn't even conduct investigations.

As an online business giant, **we need to take this to a 5.**

Rating	Definition
1	**Initial** Basic, adhoc, 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).

Cybersecurity Program Management Framework

How do we take this to a 5?

All successful Cybersecurity Departments must be able to:

1. **Complicate** the attack
2. **Detect** the attack
3. **Respond** to the attack
4. **Educate** the workforce; and
5. **Govern** effectively.

Creating a Cybersecurity Department

One team, with one mission.

Initial Steps

Creating a Cybersecurity Dept.

Initial Steps

The first step will be to create and fund a dedicated Cybersecurity department (CSD). This CSD will plan, direct, and execute all cybersecurity tasks within SSR. Forming the CSD will clarify duties and responsibilities within SSR, and resolve many of the 12 Simmons observations. Namely, the CSD can create and implement IT strategy, Policy enforcement, conduct formal investigations, ensure all transactions are logged, and conduct the formal incident management process. Most importantly, every dollar allocated to the Cybersecurity Department won't be siphoned off to IT Help Desk or other services, but be dedicated to improving Cybersecurity.

Hint: Instead of starting from scratch, consider buying an existing cybersecurity firm.

Creating a Cybersecurity Department

- Bring the current skill set and capabilities together to develop the department
  - Move PCI team to new department
    - Realign PCI team's goals with security, rather than merely compliance
  - Move IT operations personnel that conduct monitoring and incident response to the new department
- Provide training (in-house or externally)
- Hire skilled experts

Using the NIST Framework

A clear framework for developing cybersecurity capabilities.

IPDRR

Identify

Protect

Detect

Respond

Recover

Long Term Plans

IPDRR

Leverage the NIST Cybersecurity Framework

- Identify
- Protect
- Detect
- Respond
- Recover

https://www.nist.gov/cyberframework/online-learning/five-functions

Identify

All of the organization's assets, policies, mission, etc., need to be identified, documented, and tracked, examples of what needs to be identified include:

- Assets for the organization (people, data, systems and devices, facilities)
  - Allows for centralization of asset repository and inventory
- Legal requirements (policies, agreements, regulations, legislation)
  - Establish accountability
    - Allows for appropriate policy enforcement
- Threats, vulnerabilities, risks
- Vendor security
  - Maintain vendor policies and review; vetting for security
- Reporting metrics
  - Have a workflow for reporting to executive management on security issues

Protect

An executable plan needs to be in place to protect all of the organization’s assets (personnel, data, systems, devices, etc.). Examples of protection:

- Security first versus compliance first
  - Security will result in compliance
- Safeguards to ensure delivery of critical services
  - Redundancy of systems, servers, connections, etc. to allow for normal operations to continue during incidents
- Credential and authentication management (e.g., Active Directory with appropriate Organizational Units, single sign on (SSO), and multifactor-authentication)
  - Integration across the enterprise
- Awareness training for personnel and partners

Detect

A well maintained detection scheme needs to be in place. This includes:

- Intrusion detection and prevention systems (e.g., Snort)
  - Snort is free, cost of personnel to configure and maintain
- Address logging and monitoring
  - Appropriate event logging and analysis (e.g., ELK stack)
    - Appropriate training for determining false positives and negatives in events and logging
    - Pricing for ELK stack running on the cloud up to around $106,000/year (https://cloud.elastic.co/pricing)
      - Possible to run ELK locally with reduced functionality, likely to cost more for engineers to maintain than it would for the cloud
  - Monitoring systems, personnel, facilities, etc.
    - Monitoring will be conducted by the new department, with dedicated personnel and systems

Respond

Effective and efficient event and incident response is key to a well-established cybersecurity program. This should include:

- Defined criteria for incident response
- Appropriate framework established, reviewed, and maintained for incident response
  - Framework should be repeatable
- Clear and appropriate assignment of roles for incident response team or teams
- Incidents mitigated and contained
- Review after action reports and follow-ups that results in appropriate modification to incident response plans

Recover

A plan for recovery after an incident is vital. This can be one of the most chaotic times, and without a clear path toward recovery, it will cost more time and money to do so. Recover should include:

- Plans for mitigation, including public relations
- Plans for processes, lessons learned, how activities will be restored to normal
- The plans should build resiliency and be a part of the enterprise Disaster Recovery Plan/Business Continuity Plan
  - Consider whether to have a cold, warm, or hot site (if any)
  - Well maintained backup and recovery plan and process
    - Including testing the process/time it takes to perform a full recovery

Long Term Plans

Long term plans include a methodical refinement of the plans laid out. Refinement should include:

- Reciprocal application, review, and modification of the plans
- Lessons learned
  - Pros and cons of the plan (i.e., what's working, what's not)
- A willingness to let go of parts of the plan that are not working and to try new ideas

To Be Continued

Timeline, Budget, Conclusion

Key Issues and Complicating Factors Revisit

Two Year Timeline

Budget

Conclusion

Key Issues and Complicating Factors Revisit

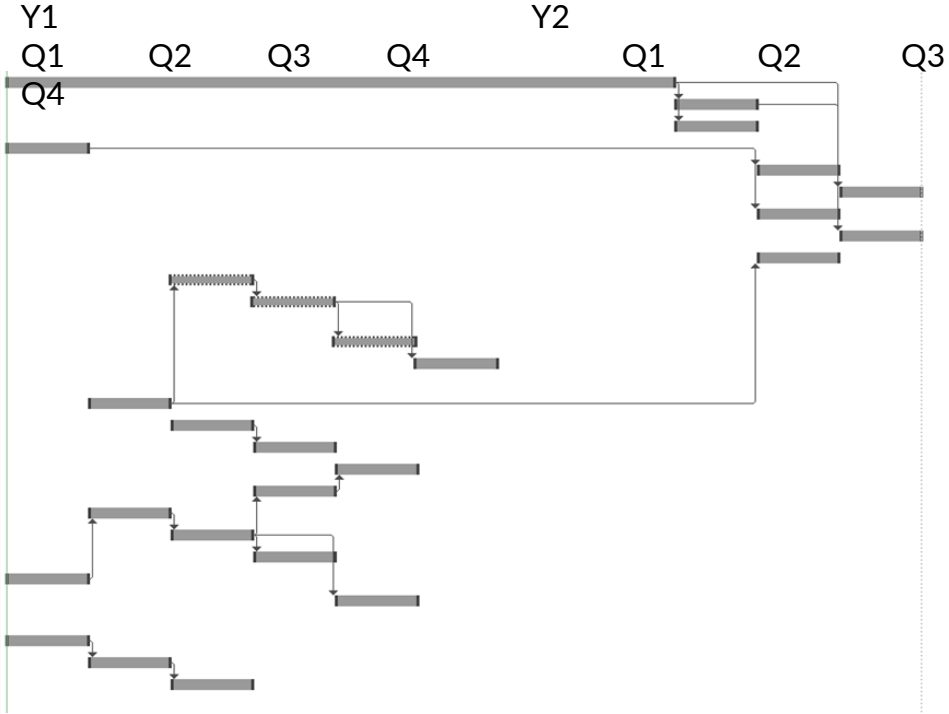
Through the implementation of the NIST framework, we have resolved all of the Simmons concerns.

1. IT Strategy
2. Policy Enforcement
3. Connecting Compliance and Security.
4. Formal investigations
5. Vetting of Third Parties
6. A centralized asset repository
7. A formal incident management process
8. A simple, multi-factor authentication system
9. Logs
10. A solid BCP.
11. A single place to report.
12. A cyber team with sufficient staff, and budgeting.

Two Year Timeline

This timeline represents the work that SSR will be doing in a 2 year timeframe. The duration of each task translates to a multi-phased plan for addressing key issues milestones and capability improvements delivered every quarter (approx every 3-5 months).

Identify	Organization's mission, objectives, stakeholders and activities
Identify	Software platforms and applications, device inventories, external resources
Identify	Legal requirements (policies, agreements, regulations, legislation)
Identify	Threats, vulnerabilities, risks
Identify	Assets for the organization (people, data, systems and devices, facilities)
Identify	Supply chain process
Identify	Vendor security
Identify	Reporting metrics
Protect	Safeguards to ensure delivery of critical services
Protect	Access management for physical and logical assets (locked doors, usergroups)
Protect	Credential and authentication management (e.g., Active Directory with appropriate Organizational Units, single sign on (SSO), and multifactor-authentication)
Protect	Integration across the enterprise
Protect	Protection for data at rest (encryption for databases and host systems, cryptographic hash functions for data integrity, etc.) and in transit (TLS, HTTPS, digital certificates, etc.)
Protect	Awareness training for personnel and partners
Detect	Intrusion detection and prevention systems (e.g., Snort)
Detect	Event logging and analysis
Detect	Continuous education on threats (e.g., monitoring the CVE database [https://cve.mitre.org/])
Detect	Monitoring systems, personnel, facilities, etc.
Respond	Defined criteria for incident response
Respond	Appropriate framework established, reviewed, and maintained for incident response
Respond	Clear and appropriate assignment of roles for incident response team or teams
Respond	Incidents mitigated and contained
Respond	Review after action reports and follow-ups that results in appropriate modification to incident response plans
Recover	Plans for mitigation, including public relations
Recover	Plans for processes, lessons learned, how activities will be restored to normal
Recover	The plans should build resiliency and be a part of the enterprise Disaster Recovery Plan/Business Continuity Plan



Budget: Quick Facts

Quick facts for SSR: 25 billion dollar company. 12.5 billion in revenue (time-revenue).

SSR should be spending: 400 million on IT (3.2% revenue). 40 million on IT Security (10% of IT Budget).

SSR is spending: Too little on Security.

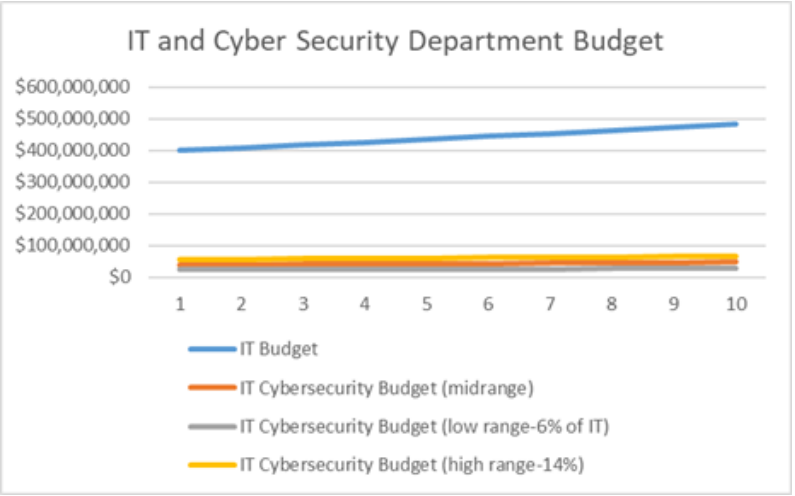
References:

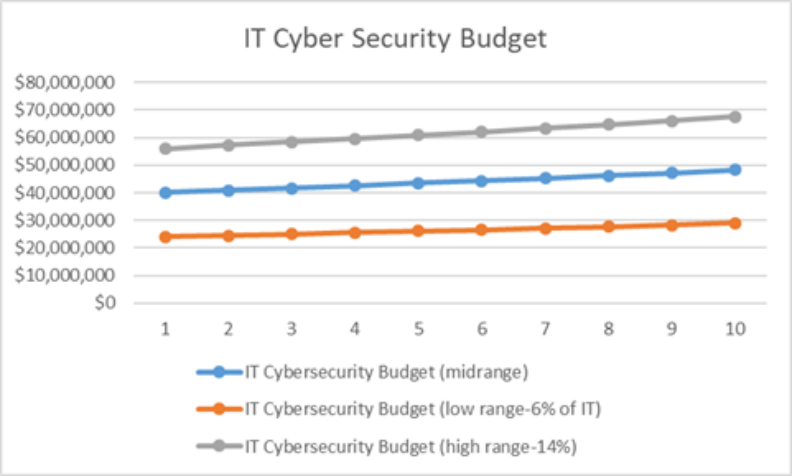
1. Time Revenue method to calculate company value: https://www.investopedia.com/terms/t/times-revenue-method.asp
2. Large companies (>2billion) spend 3.2% of revenue on IT: https://blog.techvera.com/company-it-spend
3. 6-14% of ITBudget is Security (10% selected): https://www.pionline.com/article/20190501/ONLINE/190509988/financial-services-firms-spend-6-to-14-of-it-budget-on-cybersecurity-survey
4. Example datapoint. Amazon spends 13.6 billion on IT: https://www.wsj.com/articles/amazon-alphabet-and-walmart-were-top-it-spenders-in-2018-11547754757
5. Consider purchasing Cybersecurity Firm: https://www.businessinsider.com/amazon-web-services-acquires-harvestai-2017-1
6. Cyber security for business – counting the costs and finding the value https://media.kaspersky.com/en/business-security/cybersecurity-for-business-counting-the-costs-finding-the-value.pdf

Budget Continued.

Creating a dedicated cybersecurity budget will only cost a fraction of the overall IT budget while providing sufficient security to SSR.

Low-end protection would only run about 6% of the IT Budget, while higher-end protection would run about 14% of the IT Budget.





Conclusion

Cybersecurity capabilities are a central pillar to business success in any large corporation. Developing cybersecurity capabilities within SSR will be an ongoing process. The initial foundations can be laid within a 2 year period, but there will need to be constant reassessment and improvement to combat new and emerging threats as time progresses. The new world of technology has given us an unprecedented capability to process information, communicate, and sell to people worldwide but this capability comes with risks. A good, clear-eyed, mature cybersecurity program can mitigate those risks.

Resources/Addendum A

- P. Kral, "Incident Handler's Handbook | SANS Institute", *Sans.org*, 2012. [Online]. Available: https://www.sans.org/white-papers/33901/.
- Information Systems Audit and Control Association (ISACA), *COBIT 5*. Rolling Meadows, IL: Information Systems Audit and Control Association (ISACA), 2013. [Online]. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoCDEA0.
- "Cost of a data breach 2022", *Ibm.com*, 2022. [Online]. Available: https://www.ibm.com/reports/data-breach.
- "What's the Cost of a Data Breach in 2019?", *Digital Guardian*, 2019. [Online]. Available: https://digitalguardian.com/blog/whats-cost-data-breach-2019.
- "Assessing Security and Privacy Controls in Information Systems and Organizations", *csrc.nist.gov*, 2022. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final#pubs-documentation.
- "Information Security Handbook: A Guide for Managers", *csrc.nist.gov*, 2006. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-100/final.
- Informative References Asset Management (ID.AM)”, ", *csrc.nist.gov*, 2006. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-100/final.
-
- "The Cost of Malicious Cyber Activity to the U.S. Economy", *whitehouse.gov*, 2018. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.
- "Cybersecurity Framework Manufacturing Draft", *csrc.nist.gov*, 2016. [Online]. Available: https://www.nist.gov/system/files/documents/2017/06/12/csf-manufacturing-profile-draft.pdf.
- "Framework for Improving Critical Infrastructure Security", *csrc.nist.gov*, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
- "Framework Resources*csrc.nist.gov*, 2022. [Online]. Available: https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx.