A Roadmap for Ransomware Recovery Planning

> *"When you know that you're capable of dealing with whatever comes, you have the only security the world has to offer."*
>
> **Harry Browne**

Facing the Challenge of Ransomware Attacks

A $20+ billion consumer product goods distribution company worried that it wasn't ready to deal with ransomware. Company leadership had watched as one of its significant suppliers had been attacked and was able to stay in business only by paying a hefty ransom. Had that supplier been unable to recover, the company's supply chain and ability to serve its own customers would have been in jeopardy. At the same time, news coverage of other ransomware attacks disabling companies such as Colonial Pipeline made it all too clear that the company needed to take immediate steps to protect its operations and resources.

The company had warehouse distribution operations in nearly every state, a team of more than 19,000 employees, roughly 17,000 endpoints, redundant hosted east- and west-coast data centers, and made extensive use of cloud providers including AWS, Azure, and Salesforce. Its proactive approach to cybersecurity focused on detection and protection strategies through technology, policy, and employee training. Ransomware posed a quickly emerging threat, and the leadership knew the company needed to be ready.

Seeking a Proactive Approach

While the company had invested in and implemented detection and protection strategies, it didn't have a plan or resources to quickly recover from successful ransomware attacks. Although the need to prepare for ransomware recovery was urgent, there were no funds for it in the 2021 IT budget, and the company's IT resources were already allocated to active projects for the balance of the year.

Company leadership decided to begin planning for "worst-day" scenarios, such as a ransomware attack, a major network outage, or a production data center loss. With no desire to pay ransoms to criminals, the company chose to invest in rapid-recovery capabilities from ransomware attacks. Recognizing this would involve a complex multi-year planning and implementation effort, they prioritized immediate development of recovery capabilities for their most critical systems while the rest of the plan was created.

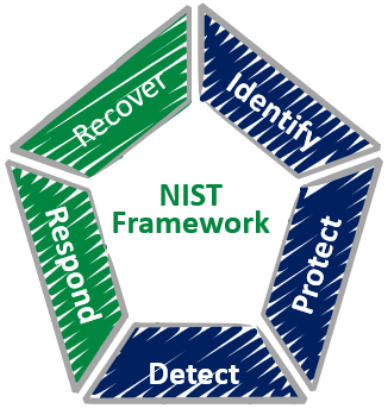
The company engaged BCS to assist with development of the program's scope, estimate the expenses, create a realistic timeline, and navigate the internal PMO methodology and corporate finance approval processes.

A Comprehensive Protection & Recovery Framework

The company's ransomware program was intended to complement -- and enhance -- existing disaster recovery/backup systems and processes. The program implemented included these four components:

1. NIST Cybersecurity Framework

The organization wanted to adhere to the NIST cybersecurity framework. Through significant investments, they had achieved some level of maturity with the framework's Identify, Protect, and Detect categories and would continue these efforts. However, the ransomware program design would include incremental 2021 funding to focus on the framework's Recover and Respond categories.



2. Simplified/Focused Program Design, Scope, and Deliverables

We quickly identified five highly focused projects with primary and secondary deliverables:

Primary Deliverables

These four elements were prioritized as must-have, near-term deliverables and accordingly received the majority of the funding commitments:

- **Immutable Data Vault Technology (IDV)/Backup Best Practices**

  As part of a goal to consolidate the number of backup technologies and leverage the latest immutable backup technology, the company had already made investments in Rubrik, had begun a proof-of-concept (POC) effort with this technology, and intended to make additional Rubrik investments as part of the program. The Rubrik POC became part of the initial program project, with movement of the most critical system backups to Rubrik as quickly as possible a key deliverable. Migration of less-critical business platform backups became part of a multi-year project effort.

- **Critical Systems/Business Process Rebuild Discovery & Documentation**

  In parallel with the IDV implementation, the company began a comprehensive analysis of all of its critical business systems, which involved more than 50 discrete applications that were grouped into five recovery tiers. These five recovery tiers reflected the organization's Recovery Time Objective (RTO) and Recovery Point Objectives (RPO). The RTO time frames ranged from near-real-time to best-effort, depending upon the tier. The analysis was further grouped by ranking more than 20 key business processes, along with the systems supporting these processes.

  We worked with application owners to perform and document a comprehensive business impact analysis for all supported applications. The primary deliverable was a detailed visual depiction of each application's infrastructure dependencies, with the complete sequential steps necessary to recover each application and restore the critical business processes the applications supported.

- **Isolated Recovery Environment (IRV)/Tabletop Testing**

  Another key deliverable involved implementing an air-gapped, offsite environment in which all critical applications could be rebuilt and the business processes they support reestablished as quickly as possible. The plan involved presenting executive management with multiple technology options and cost alternatives. The company opted to purchase entirely redundant disaster recovery hardware that would be powered off until needed, even though that represented the most expensive option. This deliverable included comprehensive tabletop and disaster recovery exercises to validate the IRV environment's effectiveness.

- **Critical Data Security Encryption**

  We identified critical data that was in immediate need of encryption and protection from data hostage situations. While the eventual plan would provide extensive protection of enterprise-wide data, this deliverable focused on quickly encrypting financial, supplier, and personal information data.

Secondary Deliverables

The program also funded three secondary deliverables:

- **Critical Systems Resiliency**

  As part of the program, we performed gap analysis, remediation, and testing of failover capability for critical business platforms. In addition to developing location circuit redundancy, this involved local file server cloud migration where appropriate.

- **Cloud-based systems secure backup validation**

  We provided cloud-based application backup/recovery capabilities, contractual commitment review, and instructions for remediation actions.

- **Application Migration Completion**

  The program also funded the migration of on-premise applications that had not been moved to the east- and west-coast data centers.

3. Expedited Finance/PMO Delivery Methodologies/Processes

A key reason for the program's effectiveness was that company leadership assigned it the highest priority and communicated that priority throughout the enterprise, encouraging all groups to provide the support we needed. In addition, the Finance and PMO methodologies and processes were adjusted as needed to expedite program funding and project review/tollgate progression approvals.

Financial Summary

The program involved more than $25 million in multi-year funding and reflected heavy external contract resources due to fully allocated internal resources. The one-time cost for the five projects that made up the program is summarized as follows:

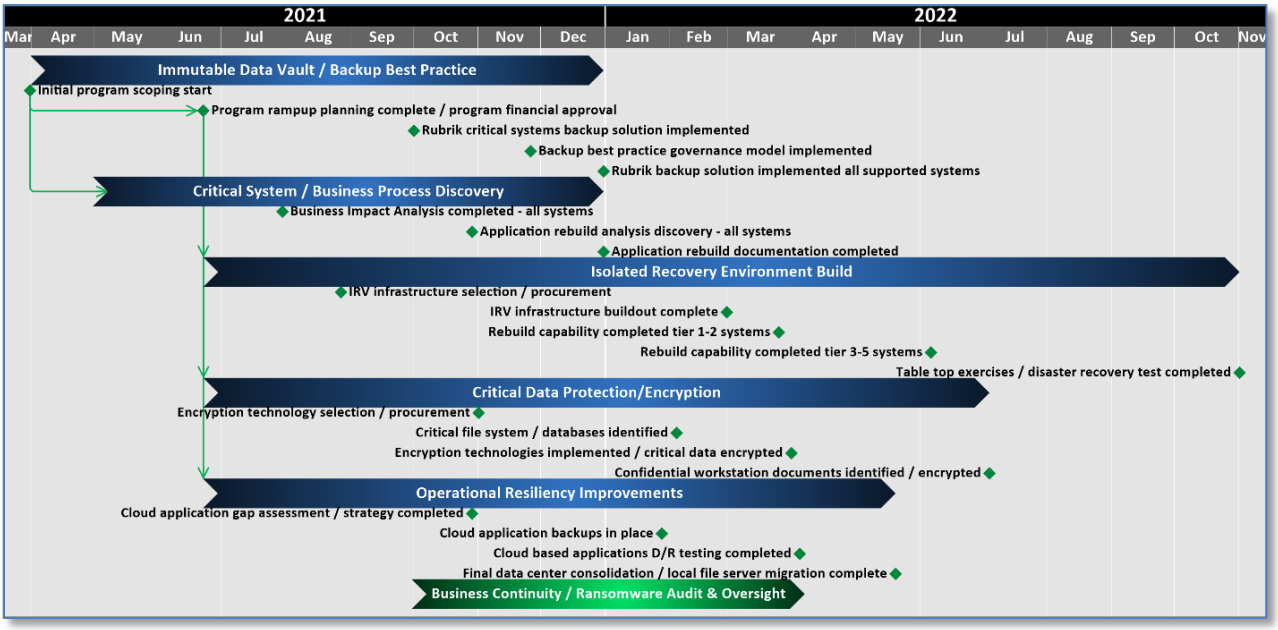
Hardware	$7,000,000
Software	$3,000,000
Consulting	$12,000,000
Internal Labor	$3,000,000
Total	**$25,000,000**

The estimated annualized recurring cost for the technologies and recovery capabilities delivered as part of the plan exceeds $4 million.

Project Timeline

The initial element of the project provided a brief ramp-up planning period for the remaining projects. It included near-term deliverables that would support phased ransomware recovery capabilities for critical systems as quickly as possible. Most of the project activity and associated workstreams used a waterfall methodology supported by the PMO, with Agile approaches for the deliverable. Wherever possible -- particularly for the program's primary deliverables -- we planned compressed timelines.

Below is a high-level multi-year project milestone roadmap.



4. **Business Continuity/Ransomware Program Audits & Oversight**

The ransomware program was designed as a technology initiative and planned and executed in parallel with a business-led business continuity (BC) project that included a capabilities gap analysis, remediation effort, and tabletop exercises involving IT and business unit participants. The BC project also involved an external audit of the IT ransomware, business BC project deliverables, penetration testing, and a review of cyber insurance and incident response plans.

The Benefits of Preparation

Faced with a challenging reality for all companies, this company's leadership opted to invest in comprehensive cybersecurity, rather than accept the inevitability of criminal payments for a successful ransomware attack or data hostage situation. The ultimate business benefits of their decision were to guarantee the company's financial survival and significantly improve the enterprise's operational resiliency.

Recommended Program Elements

A comprehensive ransomware recovery roadmap for a cybersecurity program should include the following components:

- Invest in the survival of the business, prepare for worst-day scenarios
- Adhere to the NIST security framework
- Focus on and prioritize recovery of systems that support critical business processes and protect key organizational data
- Leverage external cybersecurity resources when internal resources are not available or lack the necessary expertise