**CYBERSECURITY CAPSTONE SIMULATION**
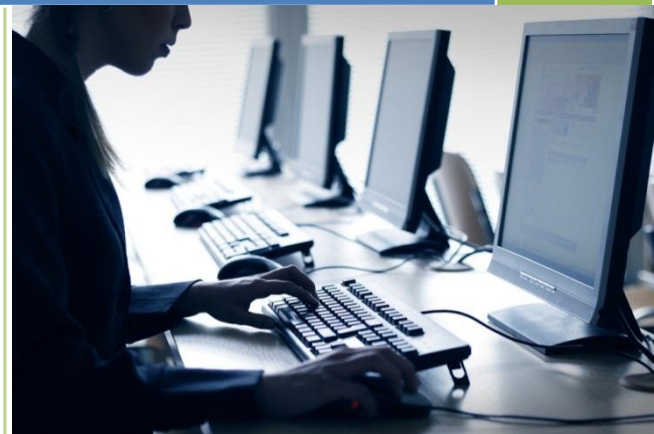
# Application Model Reference

**Student Edition**

University of Maryland University College

# Table of Contents

# Table of Figures

# List of Tables

# 1. Introduction

Welcome to the Cybersecurity Capstone Simulation (CCS).

## 1.1 About this Document

This reference is your guide to the CCS model. It details:

- The theoretical constructs of the model at the core of the CCS

- The calculation methods used

## 1.2 Prerequisites

This document is designed to help you, the student, understand the model that underlies the Cybersecurity Capstone Simulation, hereafter referred to as the CCS in this document.

Please use this reference in conjunction with the Student Manual. Reading the manual first is recommended.

## 1.3 CCS Documentation

The following documents accompany the CCS.

**Table 1: CCS Documentation**

| # | Document | Description |
|---|----------|-------------|
| 1. | Application Model Reference (this document) | A reference document that details the working of the application and the elements that go into its calculations. |
| 2. | Student Manual | A document that details the CCS structure, the task flows, best practices, and the student console user interface. |

# 2. Basics of the CCS Model

This section details the basics of the CCS model.

## 2.1 Reviewing Model Components

Let's briefly review the components of the CCS model.

**Table 2: Model Components**

| Component | Description |
|---|---|
| Decisions | You will make these every round; this will change how your systems behave. These are organized into groups called categories, which are then again clubbed into three supergroups: technical decision categories, policy decision categories, and other decision categories. |
| Events | Events triggered by the simulation that affect the teams and the virtual USA. They are defined to create certain outcomes in the CCS. |
| Indicators | Provide feedback to you on how your teams' systems and the virtual USA are doing in terms of cybersecurity and related aspects. Are generally measured as indices in the range of 0 to 200; some financial indicators like Budget are measured in dollars. |
| Outcomes | They are the results of the interaction between the events and the decisions; they affect the indicators in the CCS. |
| Round | One pass or turn of decision input, event impact, and outcome calculation. |

# 3. Decision Reference

This section details the contents of the decisions area of the CCS.

Decisions in the CCS are of two types:

**Numerical inputs:** Wherever a numerical input is required; e.g., *Spending on Kerberos servers* where you have to input a value between cost ranges specific to that decision.

**Dropdowns**: Whenever you have to make a single choice out of the options available; e.g., the decision *Encryption Strength* has options of:

- 32 bits

- 64 bits

- 128 bits

For this part, the reference we need to use is the ***decision to indicator mapping***, with sections 1.1 through 3.5 of this document.

Every decision impacts one or more indicators based on the option selected by the user or the input value entered in case of a numerical input. Associated with the variable is the degree of impact which lies in the range of -5 to 5. This relationship defines how the inputs entered by the user change the indicators in the model.

Additionally, the points below need to be taken into consideration:

- The dropdown options are not arranged in cost-ascending or cost-descending order; do not use order as an indication of cost. Refer the actual cost figures or check the in-simulation budget changes.

- The decision option providing the most security is not necessarily the most costly. It may be possible with some decisions to have diminishing returns of security vs. cost.

- You should not mechanically choose the last option because it is necessarily the "best"; you will need to think through the options. For example, a decision on frequency of patch updates would have "yearly" as the last option, but an option like "weekly" is actually more secure.

- Causal relationships and their degree of impact upon the indices in the CCS will sometimes be difficult for you to identify. This is because in the current practice of cybersecurity, decisions are sometimes made with some uncertainty (e.g., lack of perfect information and other factors).

- For example, you may find that the relationships in the simulation are not readily apparent among some events, decision controls, and the resulting outputs of a round.

The decision indicator tables start from the next page, organized by team.

### 3.1 Avisitel

**Table 3: Avisitel Decision Reference**

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Authentication | Kerberos servers spending | How much will you spend on Kerberos servers for authentication? | Minimum | 150,000 | 5,000 | • Technical Security Index<br>• Performance<br>• Downtime |
| | | | Maximum | 400,000 | 10,000 | |
| Authentication | Key distribution centers spending | How much will you spend on key distribution centers for authentication? | Minimum | 10,000 | 4,000 | • Technical Security Index<br>• Performance<br>• Downtime |
| | | | Maximum | 25,000 | 8,000 | |
| Backup | RAID levels | What's the RAID level of your server backup? | 0 | 5,000 | 10,000 | • Performance<br>• Compliance<br>• Downtime |
| | | | 1 | 10,000 | 15,000 | |
| | | | 5 | 15,000 | 17,500 | |
| | | | 6 | 17,500 | 20,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Backup | Remote backup spending | Choose the amount to spend on remote backup services. | Minimum | 10,000 | 40,000 | • Performance<br>• Downtime<br>• Compliance |
| | | | Maximum | 20,000 | 80,000 | |
| Data Encryption | Level of encryption | What is the average scale of encryption used across the organization? | No encryption | 10,000 | - | • Technical Security Index<br>• Productivity |
| | | | File | 20,000 | 5,000 | |
| | | | Folder | 30,000 | 14,000 | |
| | | | Drive | 35,000 | 25,000 | |
| Data Encryption | Encryption strength in bits | The strength of encryption you will use; the higher the bit strength, the stronger the encryption. | 32 bits | 10,000 | 10,000 | • Technical Security Index<br>• Performance |
| | | | 64 bits | 20,000 | 15,000 | |
| | | | 128 bits | 25,000 | 20,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Load Management | DDOS protection through delayed binding | Delay binding to protect against DDOS attacks. | Disable | - | - | • Technical Security Index<br>• Performance |
| | | | Enable | 30,000 | 25,000 | |
| Load Management | HTTP security through load balancing | Use load balancing to improve security. | Disable | - | - | • Technical Security Index<br>• Performance |
| | | | Enable | 60,000 | 20,000 | |
| Network Isolation | Isolate affected areas of the network as needed | Choose whether to isolate areas of the network affected by cyber or physical attacks. | Yes | 25,000 | 5,000 | • Contribution to National Security Index<br>• Network Load<br>• Customer Satisfaction<br>• Downtime<br>• Popular Sentiment |
| | | | No | - | - | |
| Network Isolation | Period of isolation in weeks | How long will you isolate affected areas of the network? | 1 | 10,000 | 100,000 | • Contribution to National Security Index<br>• Network Load<br>• Customer Satisfaction<br>• Downtime<br>• Popular Sentiment |
| | | | 2 | 20,000 | 200,000 | |
| | | | 3 | 30,000 | 300,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Patch Management | Frequency of patch management | Determine the frequency of rolling out updates to systems. | Critical updates only | 10,000 | 10,000 | • Productivity<br>• Performance<br>• Technical Security Index |
| | | | Critical and important updates | 20,000 | 20,000 | |
| | | | All updates | 40,000 | 40,000 | |
| Patch Management | Degree of patch testing prior to installation | How rigorously will you test patches before installing them? | Low | 10,000 | 5,000 | • Performance<br>• Technical Security Index |
| | | | Medium | 20,000 | 10,000 | |
| | | | High | 40,000 | 15,000 | |
| Patch Management | Trustworthiness of patch | Will you rely only on official patches, or are you willing to use unofficial or community workarounds? | Unofficial | 5,000 | 2,500 | • Downtime<br>• Performance |
| | | | Trusted | 10,000 | 5,000 | |
| | | | Official | 15,000 | 7,500 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Role Based Access Control | Degree of role-based access control | What is the degree of implementation of access control by employee role? | Low | 20,000 | 10,000 | • Technical Security Index<br>• Employee Morale |
| | | | Medium | 30,000 | 20,000 | |
| | | | High | 44,000 | 30,000 | |
| Virtualization OR Cloud Computing | Choose virtualization or cloud computing | Choose virtualization or cloud computing for your systems to improve security. | Virtualization | 10,000 | 5,000 | Technical Security Index |
| | | | Cloud computing | 50,000 | 10,000 | |
| If Virtualization Chosen | Degree of virtualization | To what degree will you implement virtualization? | Limited | 2,000 | 10,000 | Technical Security Index |
| | | | Significant | 7,000 | 20,000 | |
| | | | Full | 20,000 | 40,000 | |
| If Virtualization Chosen | Spending on underlying physical network | How much will you spend on the underlying physical network? | Minimum | 10,000 | - | Technical Security Index |
| | | | Maximum | 50,000 | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| If Virtualization Chosen | Degree of isolation of network | How isolated is the network under the virtualization schema? | Minor | 10,000 | 20,000 | • Performance • Technical Security Index |
| | | | Medium | 30,000 | 30,000 | |
| | | | Complete | 60,000 | 50,000 | |
| If Virtualization Chosen | Traffic monitoring on network | Choose the extent of traffic monitoring on the network. | Limited | 10,000 | 5,000 | • Performance • Technical Security Index |
| | | | Significant | 20,000 | 20,000 | |
| | | | Full | 30,000 | 30,000 | |
| If Cloud Computing Chosen | Cloud hosting model | Choose the cloud hosting model for your systems. Will you pay more for a more secure private infrastructure or share deployment with other companies for less cost? | Private | 22,000 | 12,571 | • Technical Security Index • Performance |
| | | | Hybrid | 16,500 | 8,250 | |
| | | | Public | 8,800 | 6,600 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| If Cloud Computing Chosen | Services offered by the cloud | At what level of engagement will you operate off the cloud? Will you stick with software, or will you go all the way to infrastructure? | Software as a service | 10,000 | 20,000 | • Technical Security Index<br>• Performance |
| | | | Platform as a service | 20,000 | 30,000 | |
| | | | Infrastructure as a service | 40,000 | 60,000 | |
| Firewall | Filtering strictness | How strict is the firewall configured to be? | Low | 5,000 | 5,000 | • Productivity<br>• Technical Security Index<br>• Performance |
| | | | Medium | 10,000 | 7,500 | |
| | | | Medium-high | 12,500 | 10,000 | |
| | | | High | 17,500 | 12,500 | |
| DNS Redundancy | DNS server redundancy | Enable DNS server redundancy to reduce downtime. | Yes | 10,000 | 15,000 | Downtime |
| | | | No | 5,000 | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| DNS Redundancy | Split DNS topology | Use a split DNS topology to reduce downtime. | Yes | 5,000 | 15,000 | Downtime |
| | | | No | 10,000 | - | |
| Database Security | Frequency of forcing password changes in days | How frequently does the database ask for a change of password? | 15 | 40,000 | 5,000 | • Productivity • Technical Security Index |
| | | | 30 | 30,000 | 5,000 | |
| | | | 60 | 20,000 | 5,000 | |
| | | | 90 | 10,000 | 5,000 | |
| Database Security | Degree of separation of roles for admin and operator roles | Choose to separate admin and operator roles for database systems. | None | 10,000 | - | • Productivity • Technical Security Index |
| | | | Limited | 20,000 | 250,000 | |
| | | | Complete | 30,000 | 350,000 | |
| Database Security | Control privileges | Are database control privileges restricted or distributed? | Restricted | 10,000 | 90,000 | • Productivity • Technical Security Index |
| | | | Distributed | 5,000 | 180,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Database Security | OS services and associated ports | Will you enable or disable database-related OS services and associated ports? | Disable | - | - | • Productivity<br>• Performance<br>• Technical Security Index |
| | | | Enable | - | - | |
| Database Security | Database honeypots | Will you employ database honeypots to trap and redirect attacks? | Disable | - | - | • Productivity<br>• Technical Security Index |
| | | | Enable | - | - | |
| IDPS | Type of intrusion detection system to install | Will you employ a network-based IDS, a host-based IDS, or both? | Network-based intrusion detection (NIDS) | 10,000 | 100,000 | Technical Security Index |
| | | | Host-based intrusion detection (HIDS) | 30,000 | 80,000 | |
| | | | Both | 36,000 | 160,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|----------|----------|-------------|---------|------------------|--------------------|--------------------|
| IDPS | Class of honeypot to deploy | Will you use a production honeypot or go for a research honeypot with better analytics? | Production honeypot | 20,000 | 90,000 | Technical Security Index |
| | | | Research honeypot | 10,000 | 70,000 | |
| IDPS | Strength of honeypot to deploy | How strong is the honeypot you deploy? | Pure honeypot | 10,000 | 90,000 | Technical Security Index |
| | | | Low interaction honeypot | 20,000 | 60,000 | |
| | | | High interaction honeypot | 30,000 | 90,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Hiring and Employee Policy | IT team size | What strength will you keep your IT teams at, in relation to the industry average? | Less than average | 10,000 | 600,000 | • Productivity<br>• Employee Morale<br>• Technical Security Index |
| | | | Average | 30,000 | 900,000 | |
| | | | More than average | 50,000 | 1,400,000 | |
| Hiring and Employee Policy | Full-time employees as a percentage of the workforce | Will you choose to bolster your IT team with temporary or part-time hires? | All | 8,800 | 4,224 | • Productivity<br>• Employee Morale<br>• Technical Security Index |
| | | | 0.9 | 16,500 | 3,960 | |
| | | | 0.8 | 22,000 | 5,867 | |
| Hiring and Employee Policy | Hiring by average experience in years | What's the average experience you're looking for when you hire for IT teams? | 3 | 8,800 | 12,941 | Internal Security Index |
| | | | 5 | 16,500 | 21,000 | |
| | | | 7 | 22,000 | 26,400 | |
| | | | 8 | 24,000 | 27,429 | |
| | | | 9 | 25,000 | 29,310 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Hiring and Employee Policy | Forced rotation of employees | Will you make employee rotation mandatory? | Disable | - | - | • Productivity<br>• Employee Morale<br>• Internal Security Index |
| | | | Enable | 25,000 | 45,000 | |
| Hiring and Employee Policy | Forced vacation for employees | Will you make employee vacations mandatory? | Disable | - | - | • Productivity<br>• Employee Morale<br>• Internal Security Index |
| | | | Enable | 75,000 | 85,000 | |
| Advisory Subscription and Federal Help | Degree of advisory referral | To what degree does your organization rely on security advisories from the federal government? | None | - | - | Technical Security Index |
| | | | Limited | 30,000 | 150,000 | |
| Advisory Subscription and Federal Help | Reliance on federal government support | To what degree will you rely on federal government support? | None | - | - | • Technical Security Index<br>• Reputation |
| | | | For critical issues only | 300,000 | 170,000 | |
| | | | Ongoing | 400,000 | 250,000 | |
| Training | Training by funding | What is the extent of funding for cybersecurity training? | Minimum | 1,000 | 50,000 | • Internal Security Index<br>• Productivity<br>• Employee Morale |
| | | | Maximum | 2,000 | 100,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Training Incentives | Average compensation bonus as a fraction of technical certification fees | How much will you reimburse employees for technical certification for security training? | 25% of fees | 5,000 | 20,000 | • Technical Security Index<br>• Productivity<br>• Employee Morale |
| | | | 50% of fees | 10,000 | 40,000 | |
| | | | 75% of fees | 15,000 | 60,000 | |
| | | | 100% of fees | 20,000 | 80,000 | |
| Training Incentives | Link training outcomes to promotion | Will you link training outcomes to promotion? | Yes | 10,000 | 10,000 | • Technical Security Index<br>• Productivity<br>• Employee Morale |
| | | | No | - | - | |
| Training Incentives | Link training outcomes to evaluation | Will you link training outcomes to evaluation? | Yes | 15,000 | 7,000 | • Technical Security Index<br>• Productivity<br>• Employee Morale |
| | | | No | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Training and Auditing | Focus on training area: network vulnerabilities | Choose whether to focus your security auditing efforts on network vulnerabilities, controls, encryption, and penetration. | Minimum | - | - | • Technical Security Index • Compliance |
| Training and Auditing | Focus on training area: network vulnerabilities | | Maximum | - | - | • Technical Security Index • Compliance |
| Training and Auditing | Focus on training area: controls | | Minimum | - | - | • Technical Security Index • Compliance |
| Training and Auditing | Focus on training area: controls | | Maximum | - | - | • Technical Security Index • Compliance |
| Training and Auditing | Focus on training area: encryption | | Minimum | - | - | • Technical Security Index • Compliance |
| Training and Auditing | Focus on training area: encryption | | Maximum | - | - | • Technical Security Index • Compliance |
| Training and Auditing | Focus on training area: penetration testing | | Minimum | - | - | • Technical Security Index • Compliance |
| Training and Auditing | Focus on training area: penetration testing | | Maximum | - | - | • Technical Security Index • Compliance |
| Training and Auditing | Frequency of physical audits of the equipment | How often will you run physical audits of system equipment? | Every three months | 10,000 | 20,000 | Technical Security Index |
| Training and Auditing | Frequency of physical audits of the equipment | | Every six months | 7,500 | 10,000 | Technical Security Index |
| Training and Auditing | Frequency of physical audits of the equipment | | Once a year | 5,000 | 5,000 | Technical Security Index |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Business Continuity Planning | Degree of IT data storage redundancy | How much redundancy will you build in for IT data storage? | Low | 5,000 | 5,000 | Disaster Readiness |
| | | | Medium | 10,000 | 10,000 | |
| | | | High | 15,000 | 20,000 | |
| Business Continuity Planning | Degree of IT network redundancy | How much redundancy will you build in for IT networks? | Low | 7,500 | 20,000 | Disaster Readiness |
| | | | Medium | 12,500 | 30,000 | |
| | | | High | 20,000 | 50,000 | |
| Business Continuity Planning | Levels of power backup redundancy | How much redundancy will you build in for power backup? | 1 | 5,000 | 25,000 | Disaster Readiness |
| | | | 2 | 10,000 | 45,000 | |
| | | | 3 | 15,000 | 67,500 | |
| Business Continuity Planning | Number of backup sites | How many backup sites will you maintain? | 1 | 5,000 | 75,000 | Disaster Readiness |
| | | | 2 | 10,000 | 150,000 | |
| | | | 3 | 15,000 | 200,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Business Continuity Planning | Number of redundant backup communication links | How many backup communication links will you maintain? | 1 | 5,000 | 10,000 | Disaster Readiness |
| | | | 2 | 10,000 | 17,500 | |
| | | | 3 | 15,000 | 25,000 | |
| Business Continuity Planning | Policy review frequency in months | How often will you review disaster recovery policy? | 3 | - | 100,000 | Disaster Readiness |
| | | | 6 | - | 75,000 | |
| | | | 9 | - | 50,000 | |
| | | | 12 | - | 25,000 | |
| Information Sharing | Degree of information sharing on attacks | To what extent does the organization share cybersecurity attack information publicly? | High - full disclosure | 8,800 | 1,760 | • Profitability<br>• Disaster Readiness |
| | | | Medium - non-sensitive disclosure | 16,500 | 4,125 | |
| | | | Low - no disclosure | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Sharing | Degree of non-crisis information sharing | To what extent does the organization share routine cybersecurity information publicly? | High - full disclosure | 16,500 | 3,536 | • Profitability<br>• Disaster Readiness |
| | | | Medium - non-sensitive disclosure | 8,800 | 1,760 | |
| | | | Low - no disclosure | - | - | |
| Public Relations | Spending on public relations | How much will you spend on public relations? | Minimum | 50,000 | 25,000 | Reputation |
| | | | Maximum | 100,000 | 100,000 | |
| Emergency Bypass Policy | Spending on emergency bypass policy | How much will you spend on emergency bypass policy? | Minimum | 5,000 | 1,000 | Disaster Readiness |
| | | | Maximum | 10,000 | 2,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Emergency Bypass Policy | Response to violations of typical separation of duties protocol | What is the response to violations of typical Separation of Duties protocol? | Not allowed | 25,000 | 12,500 | • Technical Security Index • Disaster Readiness |
| | | | Permitted with limitations | 15,000 | 20,000 | |
| | | | Allowed | 2,500 | 35,000 | |
| Emergency Bypass Policy | Violation penalties | What punitive actions will you use for violations of emergency bypass policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Information Sharing Policy | No. of people in groups to overlook and enforce internal information sharing | How many people will you put in groups to overlook and enforce information sharing? | 2 | 17,600 | 12,000 | • Productivity • Technical Security Index • Employee Morale |
| | | | 3 | 33,000 | 22,164 | |
| | | | 4 | 44,000 | 30,000 | |
| | | | 5 | 48,000 | 31,304 | |
| | | | 6 | 50,000 | 30,357 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Sharing Policy | Internal information sharing by role-based access control | How restrictive is the system for internal sharing of information? | Strictly need-to-know | 15,000 | 50,000 | • Productivity<br>• Technical Security Index<br>• Employee Morale |
| | | | Limited access | 10,000 | 35,000 | |
| | | | Open system | 1,000 | - | |
| Information Sharing Policy | Degree of external information sharing | How restrictive is the system for external sharing of information? | Strictly need-to-know | 15,000 | 50,000 | • Productivity<br>• Technical Security Index<br>• Customer Satisfaction<br>• Compliance |
| | | | Limited access | 10,000 | 35,000 | |
| | | | Open system | 1,000 | - | |
| Information Sharing Policy | Frequency of disclosure for InfraGard communication in days | How frequently will you share information for the InfraGard service of information sharing between private and public entities? | 7 days | 30,000 | 2,500 | • Contribution to National Security Index<br>• Profitability |
| | | | 14 days | 25,000 | 5,000 | |
| | | | 21 days | 12,500 | 7,500 | |
| | | | 28 days | 10,000 | 10,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Sharing Policy | Violation penalties | What punitive actions will you use for violations of information sharing policy? | Warnings | - | - | Employee Morale |
| | | | Fines | - | - | |
| | | | Suspensions | - | - | |
| | | | Termination | - | - | |
| Breach Notification Policy | Degree of openness of breach notification | How open is your organization about breaches that have happened to its systems? | All incidents | 24,000 | 50,000 | • Reputation<br>• Customer Satisfaction<br>• Contribution to National Security Index |
| | | | Critical and significant incidents | 22,000 | 35,000 | |
| | | | Only critical incidents | 16,500 | 20,000 | |
| | | | None of the incidents | 8,800 | 0 | |
| Breach Notification Policy | Investigative agencies to call in for major security breaches | Which investigative agencies will you approach for major security breaches? | Private investigators | 8,800 | 12,571 | • Reputation<br>• Employee Morale<br>• Contribution to National Security Index<br>• Downtime |
| | | | Forensic investigators | 16,500 | 24,750 | |
| | | | CERT | - | - | |
| | | | FBI/NSA | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|----------|----------|-------------|---------|------------------|--------------------|--------------------|
| Breach Notification Policy | Violation penalties | What punitive actions will you use for violations of breach notification policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Information Privacy Policy | Privacy program investment spending | How much will you spend on your organization's privacy program? | Minimum | 10,000 | 5,000 | • Employee Morale • Customer Satisfaction |
| | | | Maximum | 50,000 | 10,000 | |
| Information Privacy Policy | Appoint a dedicated privacy officer | Will you appoint a dedicated privacy officer? | Yes | 8,800 | 10,560 | • Employee Morale • Customer Satisfaction |
| | | | No | - | - | |
| Information Privacy Policy | Privacy training spending for employees | How much will you spend on training employees on privacy policies? | Minimum | 10,000 | 5,000 | • Employee Morale • Customer Satisfaction |
| | | | Maximum | 40,000 | 10,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Privacy Policy | Degree of information and record retention | What sort of information will you retain? | Critical information | 25,000 | 20,000 | • Performance<br>• Employee Morale |
| | | | Operational information | 15,000 | 75,000 | |
| | | | All information | 37,500 | 110,000 | |
| Information Privacy Policy | Violation penalties | What punitive actions will you use for violations of information privacy policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| General Access Policies | Degree of freedom given to employees regarding communications over the Internet | How free are your employees to communicate over the Internet? | Restricted | 12,500 | 50,000 | • Employee Morale<br>• Productivity |
| | | | Time-limited | 12,500 | 50,000 | |
| | | | Free | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| General Access Policies | Degree of freedom over browsing non-business sites | How free are your employees to browse non-business sites? | Restricted | 5,000 | 50,000 | • Employee Morale<br>• Productivity |
| | | | Time-limited | 10,000 | 50,000 | |
| | | | Free | - | - | |
| General Access Policies | Degree of logging of Internet access and other system actions and accesses | Choose the degree to which Internet access and other system actions and access are logged. | None | - | - | • Internal Security Index<br>• Employee Morale |
| | | | Limited actions | 10,000 | 20,000 | |
| | | | Critical system access only | 25,000 | 75,000 | |
| | | | All actions | 50,000 | 125,000 | |
| General Access Policies | Number of permitted login attempts | Choose the number of permitted login attempts. | 3 | - | - | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 5 | - | - | |
| | | | 7 | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| General Access Policies | Password validity in days | How long will passwords set be valid? | 15 | 20,000 | 30,000 | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 30 | 20,000 | 15,000 | |
| | | | 45 | 20,000 | 10,000 | |
| General Access Policies | Password length requirements | How many characters long should the password be? | 4 | 20,000 | 10,000 | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 6 | 30,000 | 10,000 | |
| | | | 8 | 45,000 | 10,000 | |
| General Access Policies | Non-use of prior passwords | How many prior passwords are set to be invalid for use? | 1 | - | - | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 3 | - | - | |
| | | | 6 | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| General Access Policies | Violation penalties | What punitive actions will you use for violations of general access policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Physical Security | Physically isolate rooms containing important infrastructure | Control the degree of physical access to servers. | Free access | 10,000 | - | Technical Security Index |
| | | | Limited access | 25,000 | 20,000 | |
| | | | Restricted access | 30,000 | 15,000 | |
| Physical Security | Restricting physical access through role based access control | Control the degree of physical access to servers through role-based access control. | Free access | 5,000 | - | • Productivity<br>• Disaster Readiness<br>• Technical Security Index |
| | | | Limited access | 12,500 | 2,000 | |
| | | | Restricted access | 15,000 | 15,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Physical Security | Degree of access given to visitors | Control the degree and quality of access for visitors. | Free access | 10,000 | - | • Productivity<br>• Technical Security Index |
| | | | Limited access | 20,000 | 10,000 | |
| | | | Accompanied free access | 30,000 | 150,000 | |
| | | | Accompanied limited access | 40,000 | 250,000 | |
| | | | Restricted access | 50,000 | 300,000 | |
| Physical Security | Violation penalties | What punitive actions will you use for violations of physical security policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Remote Access Policy | Degree of remote access by employee grade | For which employee grades is remote access available? | Executive management only | 10,000 | 2,500 | • Technical Security Index<br>• Productivity |
| | | | Upper management | 15,000 | 7,500 | |
| | | | Middle management | 20,000 | 25,000 | |
| | | | All professional staff members | 35,000 | 100,000 | |
| Remote Access Policy | Access privileges permitted | What are the maximum remote access privileges allowed? | Low - read only | 10,000 | 5,000 | • Technical Security Index<br>• Productivity |
| | | | Medium - read/write | 15,000 | 5,000 | |
| | | | High - read/write/delete | 20,000 | 10,000 | |
| | | | Very high - administrator level | 35,000 | 10,000 | |
| Remote Access Policy | Violation penalties | What punitive actions will you use for violations of remote access policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Authorized Software Policy | Type of software permitted for use by employees | How lenient are you in terms of software usage? | Freeware | - | - | • Employee Morale<br>• Technical Security Index |
| | | | Games | 20,000 | 30,000 | |
| | | | Open-source | - | - | |
| | | | Approved software | 100,000 | 150,000 | |
| Authorized Software Policy | Software evaluation frequency in months | How frequently will you evaluate systems for presence of unauthorized software? | 6 | 25,000 | 85,000 | • Productivity<br>• Technical Security Index |
| | | | 12 | 35,000 | 50,000 | |
| | | | 18 | 45,000 | 40,000 | |
| Authorized Software Policy | Violation penalties | What punitive actions will you use for violations of authorized software policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Systems Development Testing | Intensity of quality assurance testing | How intense is your quality assurance testing? | Low | 40,000 | 50,000 | • Employee Morale<br>• Technical Security Index |
| | | | Medium | 60,000 | 150,000 | |
| | | | High | 90,000 | 300,000 | |
| Systems Development Testing | Degree of reliance on external vendor | Choose the degree of reliance on external vendors for systems development testing. | Usability and other minor testing | 10,000 | 50,000 | • Productivity<br>• Technical Security Index |
| | | | Supplementary testing | 20,000 | 100,000 | |
| | | | Comprehensive testing | 30,000 | 200,000 | |
| Antivirus Policy | Quality of antivirus solution used | Choose the quality of the antivirus solution used across the organization. | Baseline | 30,000 | 50,000 | • Performance<br>• Productivity<br>• Technical Security Index |
| | | | Strong | 50,000 | 100,000 | |
| | | | State-of-the-art | 70,000 | 180,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Antivirus Policy | Frequency of scans | How frequently does the antivirus scan run? | Multiple times per day | 24,000 | 28,800 | • Productivity<br>• Technical Security Index |
| | | | Once daily | 22,000 | 3,846 | |
| | | | Once per week | 16,500 | 15,000 | |
| | | | Once per month | 8,800 | 8,800 | |
| Antivirus Policy | Frequency of patch updates | How frequently will you update your antivirus solution with patches? | Always once released | 22,000 | 66,000 | • Productivity<br>• Technical Security Index |
| | | | Only for major and critical updates | 16,500 | 39,286 | |
| | | | Only for critical updates | 8,800 | 18,857 | |
| Insurance Policy | Degree of insurance used against a cyberattack | How high will you prioritize insurance against a cyberattack? | Low | 8,800 | 88,000 | • Disaster Readiness<br>• Compliance |
| | | | Medium | 16,500 | 32,000 | |
| | | | High | 22,000 | 330,000 | |

### 3.2 DTL Power

**Table 4: DTL Power Decision Reference**

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Authentication | Kerberos servers spending | How much will you spend on Kerberos servers for authentication? | Minimum | 150,000 | 5,000 | • Technical Security Index<br>• Performance<br>• Downtime |
| | | | Maximum | 400,000 | 10,000 | |
| Authentication | Key distribution centers spending | How much will you spend on key distribution centers for authentication? | Minimum | 10,000 | 4,000 | • Technical Security Index<br>• Performance<br>• Downtime |
| | | | Maximum | 25,000 | 8,000 | |
| Backup | RAID levels | What's the RAID level of your server backup? | 0 | 5,000 | 10,000 | • Performance<br>• Compliance<br>• Downtime |
| | | | 1 | 10,000 | 15,000 | |
| | | | 5 | 15,000 | 17,500 | |
| | | | 6 | 17,500 | 20,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Backup | Remote backup spending | Choose the amount to spend on remote backup services. | Minimum | 10,000 | 40,000 | • Performance<br>• Downtime<br>• Compliance |
| | | | Maximum | 20,000 | 80,000 | |
| Data Encryption | Level of encryption | What is the average scale of encryption used across the organization? | No encryption | 10,000 | - | • Technical Security Index<br>• Productivity |
| | | | File | 20,000 | 5,000 | |
| | | | Folder | 30,000 | 14,000 | |
| | | | Drive | 35,000 | 25,000 | |
| Data Encryption | Encryption strength in bits | The strength of encryption you will use; the higher the bit strength, the stronger the encryption. | 32 bits | 10,000 | 10,000 | • Technical Security Index<br>• Performance |
| | | | 64 bits | 20,000 | 15,000 | |
| | | | 128 bits | 25,000 | 20,000 | |
| Load Management | DDOS protection through delayed binding | Delay binding to protect against DDOS attacks. | Disable | - | - | • Technical Security Index<br>• Performance |
| | | | Enable | 30,000 | 25,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Load Management | HTTP security through load balancing | Use load balancing to improve security. | Disable | - | - | • Technical Security Index<br>• Performance |
| | | | Enable | 60,000 | 20,000 | |
| Network Isolation | Isolate affected areas of the network as needed | Choose whether to isolate areas of the network affected by cyber or physical attacks. | Yes | 25,000 | 5,000 | • Contribution to National Security Index<br>• Network Load<br>• Customer Satisfaction<br>• Downtime<br>• Popular Sentiment |
| | | | No | - | - | |
| Network Isolation | Period of isolation in weeks | How long will you isolate affected areas of the network? | 1 | 10,000 | 100,000 | • Contribution to National Security Index<br>• Network Load<br>• Customer Satisfaction<br>• Downtime<br>• Popular Sentiment |
| | | | 2 | 20,000 | 200,000 | |
| | | | 3 | 30,000 | 300,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Patch Management | Frequency of patch management | Determine the frequency of rolling out updates to systems. | Critical updates only | 10,000 | 10,000 | • Productivity • Performance • Technical Security Index |
| | | | Critical and important updates | 20,000 | 20,000 | |
| | | | All updates | 40,000 | 40,000 | |
| Patch Management | Degree of patch testing prior to installation | How rigorously will you test patches before installing them? | Low | 10,000 | 5,000 | • Performance • Technical Security Index |
| | | | Medium | 20,000 | 10,000 | |
| | | | High | 40,000 | 15,000 | |
| Patch Management | Trustworthiness of patch | Will you rely only on official patches, or are you willing to use unofficial or community workarounds? | Unofficial | 5,000 | 2,500 | • Downtime • Performance |
| | | | Trusted | 10,000 | 5,000 | |
| | | | Official | 15,000 | 7,500 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Role Based Access Control | Degree of role-based access control | What is the degree of implementation of access control by employee role? | Low | 20,000 | 10,000 | • Technical Security Index • Employee Morale |
| | | | Medium | 30,000 | 20,000 | |
| | | | High | 44,000 | 30,000 | |
| Virtualization OR Cloud Computing | Choose virtualization or cloud computing | Choose virtualization or cloud computing for your systems to improve security. | Virtualization | 10,000 | 5,000 | Technical Security Index |
| | | | Cloud computing | 50,000 | 10,000 | |
| If Virtualization Chosen | Degree of virtualization | To what degree will you implement virtualization? | Limited | 2,000 | 10,000 | Technical Security Index |
| | | | Significant | 7,000 | 20,000 | |
| | | | Full | 20,000 | 40,000 | |
| If Virtualization Chosen | Spending on underlying physical network | How much will you spend on the underlying physical network? | Minimum | 10,000 | - | Technical Security Index |
| | | | Maximum | 50,000 | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| If Virtualization Chosen | Degree of isolation of network | How isolated is the network under the virtualization schema? | Minor | 10,000 | 20,000 | • Performance<br>• Technical Security Index |
| | | | Medium | 30,000 | 30,000 | |
| | | | Complete | 60,000 | 50,000 | |
| If Virtualization Chosen | Traffic monitoring on network | Choose the extent of traffic monitoring on the network. | Limited | 10,000 | 5,000 | • Performance<br>• Technical Security Index |
| | | | Significant | 20,000 | 20,000 | |
| | | | Full | 30,000 | 30,000 | |
| If Cloud Computing Chosen | Cloud hosting model | Choose the cloud hosting model for your systems. Will you pay more for a more secure private infrastructure or share deployment with other companies for less cost? | Private | 22,000 | 12,571 | • Technical Security Index<br>• Performance |
| | | | Hybrid | 16,500 | 8,250 | |
| | | | Public | 8,800 | 6,600 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| If Cloud Computing Chosen | Services offered by the cloud | At what level of engagement will you operate off the cloud? Will you stick with software, or will you go all the way to infrastructure? | Software as a service | 10,000 | 20,000 | • Technical Security Index<br>• Performance |
| | | | Platform as a service | 20,000 | 30,000 | |
| | | | Infrastructure as a service | 40,000 | 60,000 | |
| Firewall | Filtering strictness | How strict is the firewall configured to be? | Low | 5,000 | 5,000 | • Productivity<br>• Technical Security Index<br>• Performance |
| | | | Medium | 10,000 | 7,500 | |
| | | | Medium-high | 12,500 | 10,000 | |
| | | | High | 17,500 | 12,500 | |
| DNS Redundancy | DNS server redundancy | Enable DNS server redundancy to reduce downtime. | Yes | 10,000 | 15,000 | Downtime |
| | | | No | 5,000 | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| DNS Redundancy | Split DNS topology | Use a split DNS topology to reduce downtime. | Yes | 5,000 | 15,000 | Downtime |
| | | | No | 10,000 | - | |
| Database Security | Frequency of forcing password changes in days | How frequently does the database ask for a change of password? | 15 | 40,000 | 5,000 | • Productivity<br>• Technical Security Index |
| | | | 30 | 30,000 | 5,000 | |
| | | | 60 | 20,000 | 5,000 | |
| | | | 90 | 10,000 | 5,000 | |
| Database Security | Degree of separation of roles for admin and operator roles | Choose to separate admin and operator roles for database systems. | None | 10,000 | - | • Productivity<br>• Technical Security Index |
| | | | Limited | 20,000 | 250,000 | |
| | | | Complete | 30,000 | 350,000 | |
| Database Security | Control privileges | Are database control privileges restricted or distributed? | Restricted | 10,000 | 90,000 | • Productivity<br>• Technical Security Index |
| | | | Distributed | 5,000 | 180,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Database Security | OS services and associated ports | Will you enable or disable database-related OS services and associated ports? | Disable | - | - | • Productivity<br>• Performance<br>• Technical Security Index |
| | | | Enable | - | - | |
| Database Security | Database honeypots | Will you employ database honeypots to trap and redirect attacks? | Disable | - | - | • Productivity<br>• Technical Security Index |
| | | | Enable | - | - | |
| IDPS | Type of intrusion detection system to install | Will you employ a network-based IDS, a host-based IDS, or both? | Network-based intrusion detection (NIDS) | 10,000 | 100,000 | Technical Security Index |
| | | | Host-based intrusion detection (HIDS) | 30,000 | 80,000 | |
| | | | Both | 36,000 | 160,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|----------|----------|-------------|---------|------------------|--------------------|--------------------|
| IDPS | Class of honeypot to deploy | Will you use a production honeypot or go for a research honeypot with better analytics? | Production honeypot | 20,000 | 90,000 | Technical Security Index |
| | | | Research honeypot | 10,000 | 70,000 | |
| IDPS | Strength of honeypot to deploy | How strong is the honeypot you deploy? | Pure honeypot | 10,000 | 90,000 | Technical Security Index |
| | | | Low interaction honeypot | 20,000 | 60,000 | |
| | | | High interaction honeypot | 30,000 | 90,000 | |
| Hiring and Employee Policy | IT team size | What strength will you keep your IT teams at, in relation to the industry average? | Less than average | 10,000 | 600,000 | • Productivity<br>• Employee Morale<br>• Technical Security Index |
| | | | Average | 30,000 | 900,000 | |
| | | | More than average | 50,000 | 1,400,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Hiring and Employee Policy | Full-time employees as a percentage of the workforce | Will you choose to bolster your IT team with temporary or part-time hires? | All | 8,800 | 4,224 | • Productivity<br>• Employee Morale<br>• Technical Security Index |
| | | | 0.9 | 16,500 | 3,960 | |
| | | | 0.8 | 22,000 | 5,867 | |
| Hiring and Employee Policy | Hiring by average experience in years | What's the average experience you're looking for when you hire for IT teams? | 3 | 8,800 | 12,941 | Internal Security Index |
| | | | 5 | 16,500 | 21,000 | |
| | | | 7 | 22,000 | 26,400 | |
| | | | 8 | 24,000 | 27,429 | |
| | | | 9 | 25,000 | 29,310 | |
| Hiring and Employee Policy | Forced rotation of employees | Will you make employee rotation mandatory? | Disable | - | - | • Productivity<br>• Employee Morale<br>• Internal Security Index |
| | | | Enable | 25,000 | 45,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Hiring and Employee Policy | Forced vacation for employees | Will you make employee vacations mandatory? | Disable | - | - | • Productivity<br>• Employee Morale<br>• Internal Security Index |
| | | | Enable | 75,000 | 85,000 | |
| Advisory Subscription and Federal Help | Degree of advisory referral | To what degree does your organization rely on security advisories from the federal government? | None | - | - | Technical Security Index |
| | | | Limited | 30,000 | 150,000 | |
| Advisory Subscription and Federal Help | Reliance on federal government support | To what degree will you rely on federal government support? | None | - | - | • Technical Security Index<br>• Reputation |
| | | | For critical issues only | 300,000 | 170,000 | |
| | | | Ongoing | 400,000 | 250,000 | |
| Training | Training by funding | What is the extent of funding for cybersecurity training? | Minimum | 1,000 | 50,000 | • Internal Security Index<br>• Productivity<br>• Employee Morale |
| | | | Maximum | 2,000 | 100,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Training Incentives | Average compensation bonus as a fraction of technical certification fees | How much will you reimburse employees for technical certification for security training? | 25% of fees | 5,000 | 20,000 | • Technical Security Index<br>• Productivity<br>• Employee Morale |
| | | | 50% of fees | 10,000 | 40,000 | |
| | | | 75% of fees | 15,000 | 60,000 | |
| | | | 100% of fees | 20,000 | 80,000 | |
| Training Incentives | Link training outcomes to promotion | Will you link training outcomes to promotion? | Yes | 10,000 | 10,000 | • Technical Security Index<br>• Productivity<br>• Employee Morale |
| | | | No | - | - | |
| Training Incentives | Link training outcomes to evaluation | Will you link training outcomes to evaluation? | Yes | 15,000 | 7,000 | • Technical Security Index<br>• Productivity<br>• Employee Morale |
| | | | No | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|----------|----------|-------------|---------|------------------|--------------------|--------------------|
| Training and Auditing | Focus on training area: network vulnerabilities | Choose whether to focus your security auditing efforts on network vulnerabilities, controls, encryption, and penetration. | Minimum | - | - | • Technical Security Index<br>• Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Focus on training area: controls | | Minimum | - | - | • Technical Security Index<br>• Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Focus on training area: encryption | | Minimum | - | - | • Technical Security Index<br>• Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Focus on training area: penetration testing | | Minimum | - | - | • Technical Security Index<br>• Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Frequency of physical audits of the equipment | How often will you run physical audits of system equipment? | Every three months | 10,000 | 20,000 | Technical Security Index |
| | | | Every six months | 7,500 | 10,000 | |
| | | | Once a year | 5,000 | 5,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Business Continuity Planning | Degree of IT data storage redundancy | How much redundancy will you build in for IT data storage? | Low | 5,000 | 5,000 | Disaster Readiness |
| | | | Medium | 10,000 | 10,000 | |
| | | | High | 15,000 | 20,000 | |
| Business Continuity Planning | Degree of IT network redundancy | How much redundancy will you build in for IT networks? | Low | 7,500 | 20,000 | Disaster Readiness |
| | | | Medium | 12,500 | 30,000 | |
| | | | High | 20,000 | 50,000 | |
| Business Continuity Planning | Levels of power backup redundancy | How much redundancy will you build in for power backup? | 1 | 5,000 | 25,000 | Disaster Readiness |
| | | | 2 | 10,000 | 45,000 | |
| | | | 3 | 15,000 | 67,500 | |
| Business Continuity Planning | Number of backup sites | How many backup sites will you maintain? | 1 | 5,000 | 75,000 | Disaster Readiness |
| | | | 2 | 10,000 | 150,000 | |
| | | | 3 | 15,000 | 200,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Business Continuity Planning | Number of redundant backup communication links | How many backup communication links will you maintain? | 1 | 5,000 | 10,000 | Disaster Readiness |
| | | | 2 | 10,000 | 17,500 | |
| | | | 3 | 15,000 | 25,000 | |
| Business Continuity Planning | Policy review frequency in months | How often will you review disaster recovery policy? | 3 | - | 100,000 | Disaster Readiness |
| | | | 6 | - | 75,000 | |
| | | | 9 | - | 50,000 | |
| | | | 12 | - | 25,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Sharing | Degree of information sharing on attacks | To what extent does the organization share cybersecurity attack information publicly? | High - full disclosure | 16,500 | 3,300 | • Profitability<br>• Disaster Readiness |
| | | | Medium - non-sensitive disclosure | 8,800 | 2,200 | |
| | | | Low - no disclosure | - | - | |
| Information Sharing | Degree of non-crisis information sharing | To what extent does the organization share routine cybersecurity information publicly? | High - full disclosure | 16,500 | 3,536 | • Profitability<br>• Disaster Readiness |
| | | | Medium - non-sensitive disclosure | 8,800 | 1,760 | |
| | | | Low - no disclosure | - | - | |
| Public Relations | Spending on public relations | How much will you spend on public relations? | Minimum | 50,000 | 25,000 | Reputation |
| | | | Maximum | 100,000 | 100,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Emergency Bypass Policy | Spending on emergency bypass policy | How much will you spend on emergency bypass policy? | Minimum | 5,000 | 1,000 | Disaster Readiness |
| | | | Maximum | 10,000 | 2,000 | |
| Emergency Bypass Policy | Response to violations of typical separation of duties protocol | What is the response to violations of typical Separation of Duties protocol? | Not allowed | 25,000 | 12,500 | • Technical Security Index<br>• Disaster Readiness |
| | | | Permitted with limitations | 15,000 | 20,000 | |
| | | | Allowed | 2,500 | 35,000 | |
| Emergency Bypass Policy | Violation penalties | What punitive actions will you use for violations of emergency bypass policy? | Focus on warnings | | | - | Employee Morale |
| | | | Focus on fines | | | - | |
| | | | Focus on suspensions | | | - | |
| | | | Focus on termination | | | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Sharing Policy | No. of people in groups to overlook and enforce internal information sharing | How many people will you put in groups to overlook and enforce information sharing? | 2 | 17,600 | 12,000 | • Productivity<br>• Technical Security Index<br>• Employee Morale |
| | | | 3 | 33,000 | 22,164 | |
| | | | 4 | 44,000 | 30,000 | |
| | | | 5 | 48,000 | 31,304 | |
| | | | 6 | 50,000 | 30,357 | |
| Information Sharing Policy | Internal information sharing by role-based access control | How restrictive is the system for internal sharing of information? | Strictly need-to-know | 15,000 | 50,000 | • Productivity<br>• Technical Security Index<br>• Employee Morale |
| | | | Limited access | 10,000 | 35,000 | |
| | | | Open system | 1,000 | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Sharing Policy | Degree of external information sharing | How restrictive is the system for external sharing of information? | Strictly need-to-know | 15,000 | 50,000 | • Productivity<br>• Technical Security Index<br>• Customer Satisfaction<br>• Compliance |
| | | | Limited access | 10,000 | 35,000 | |
| | | | Open system | 1,000 | - | |
| Information Sharing Policy | Frequency of disclosure for InfraGard communication in days | How frequently will you share information for the InfraGard service of information sharing between private and public entities? | 7 days | 24,000 | 2,000 | • Contribution to National Security Index<br>• Profitability |
| | | | 14 days | 22,000 | 4,400 | |
| | | | 21 days | 16,500 | 9,900 | |
| | | | 28 days | 8,800 | 8,800 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Sharing Policy | Violation penalties | What punitive actions will you use for violations of information sharing policy? | Warnings | - | - | Employee Morale |
| | | | Fines | - | - | |
| | | | Suspensions | - | - | |
| | | | Termination | - | - | |
| Breach Notification Policy | Degree of openness of breach notification | How open is your organization about breaches that have happened to its systems? | All incidents | 24,000 | 50,000 | • Reputation<br>• Customer Satisfaction<br>• Contribution to National Security Index |
| | | | Critical and significant incidents | 22,000 | 35,000 | |
| | | | Only critical incidents | 16,500 | 20,000 | |
| | | | None of the incidents | 8,800 | 0 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Breach Notification Policy | Investigative agencies to call in for major security breaches | Which investigative agencies will you approach for major security breaches? | Private investigators | 8,800 | 12,571 | • Reputation<br>• Employee Morale<br>• Contribution to National Security Index<br>• Downtime |
| | | | Forensic investigators | 16,500 | 24,750 | |
| | | | CERT | - | - | |
| | | | FBI/NSA | - | - | |
| Breach Notification Policy | Violation penalties | What punitive actions will you use for violations of breach notification policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Information Privacy Policy | Privacy program investment spending | How much will you spend on your organization's privacy program? | Minimum | 10,000 | 5,000 | • Employee Morale<br>• Customer Satisfaction |
| | | | Maximum | 50,000 | 10,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Privacy Policy | Appoint a dedicated privacy officer | Will you appoint a dedicated privacy officer? | Yes | 8,800 | 10,560 | • Employee Morale<br>• Customer Satisfaction |
| | | | No | - | - | |
| Information Privacy Policy | Privacy training spending for employees | How much will you spend on training employees on privacy policies? | Minimum | 10,000 | 5,000 | • Employee Morale<br>• Customer Satisfaction |
| | | | Maximum | 40,000 | 10,000 | |
| Information Privacy Policy | Degree of information and record retention | What sort of information will you retain? | Critical information | 25,000 | 20,000 | • Performance<br>• Employee Morale |
| | | | Operational information | 15,000 | 75,000 | |
| | | | All information | 37,500 | 110,000 | |
| Information Privacy Policy | Violation penalties | What punitive actions will you use for violations of information privacy policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| General Access Policies | Degree of freedom given to employees regarding communications over the Internet | How free are your employees to communicate over the Internet? | Restricted | 12,500 | 50,000 | • Employee Morale<br>• Productivity |
| | | | Time-limited | 12,500 | 50,000 | |
| | | | Free | - | - | |
| General Access Policies | Degree of freedom over browsing non-business sites | How free are your employees to browse non-business sites? | Restricted | 5,000 | 50,000 | • Employee Morale<br>• Productivity |
| | | | Time-limited | 10,000 | 50,000 | |
| | | | Free | - | - | |
| General Access Policies | Degree of logging of Internet access and other system actions and accesses | Choose the degree to which Internet access and other system actions and access are logged. | None | - | - | • Internal Security Index<br>• Employee Morale |
| | | | Limited actions | 10,000 | 20,000 | |
| | | | Critical system access only | 25,000 | 75,000 | |
| | | | All actions | 50,000 | 125,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| General Access Policies | Number of permitted login attempts | Choose the number of permitted login attempts. | 3 | - | - | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 5 | - | - | |
| | | | 7 | - | - | |
| General Access Policies | Password validity in days | How long will passwords set be valid? | 15 | 20,000 | 30,000 | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 30 | 20,000 | 15,000 | |
| | | | 45 | 20,000 | 10,000 | |
| General Access Policies | Password length requirements | How many characters long should the password be? | 4 | 20,000 | 10,000 | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 6 | 30,000 | 10,000 | |
| | | | 8 | 45,000 | 10,000 | |
| General Access Policies | Non-use of prior passwords | How many prior passwords are set to be invalid for use? | 1 | - | - | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 3 | - | - | |
| | | | 6 | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| General Access Policies | Violation penalties | What punitive actions will you use for violations of general access policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Physical Security | Physically isolate rooms containing important infrastructure | Control the degree of physical access to servers. | Free access | 10,000 | - | Technical Security Index |
| | | | Limited access | 25,000 | 20,000 | |
| | | | Restricted access | 30,000 | 15,000 | |
| Physical Security | Restricting physical access through role based access control | Control the degree of physical access to servers through role-based access control. | Free access | 5,000 | - | • Productivity<br>• Disaster Readiness<br>• Technical Security Index |
| | | | Limited access | 12,500 | 2,000 | |
| | | | Restricted access | 15,000 | 15,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Physical Security | Degree of access given to visitors | Control the degree and quality of access for visitors. | Free access | 10,000 | - | • Productivity<br>• Technical Security Index |
| | | | Limited access | 20,000 | 10,000 | |
| | | | Accompanied free access | 30,000 | 150,000 | |
| | | | Accompanied limited access | 40,000 | 250,000 | |
| | | | Restricted access | 50,000 | 300,000 | |
| Physical Security | Violation penalties | What punitive actions will you use for violations of physical security policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Remote Access Policy | Degree of remote access by employee grade | For which employee grades is remote access available? | Executive management only | 10,000 | 2,500 | • Technical Security Index<br>• Productivity |
| | | | Upper management | 15,000 | 7,500 | |
| | | | Middle management | 20,000 | 25,000 | |
| | | | All professional staff members | 35,000 | 100,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Remote Access Policy | Access privileges permitted | What are the maximum remote access privileges allowed? | Low - read only | 10,000 | 5,000 | • Technical Security Index<br>• Productivity |
| | | | Medium - read/write | 15,000 | 5,000 | |
| | | | High - read/write/delete | 20,000 | 10,000 | |
| | | | Very high - administrator level | 35,000 | 10,000 | |
| Remote Access Policy | Violation penalties | What punitive actions will you use for violations of remote access policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Authorized Software Policy | Type of software permitted for use by employees | How lenient are you in terms of software usage? | Freeware | - | - | • Employee Morale<br>• Technical Security Index |
| | | | Games | 20,000 | 30,000 | |
| | | | Open-source | - | - | |
| | | | Approved software | 100,000 | 150,000 | |
| Authorized Software Policy | Software evaluation frequency in months | How frequently will you evaluate systems for presence of unauthorized software? | 6 | 25,000 | 85,000 | • Productivity<br>• Technical Security Index |
| | | | 12 | 35,000 | 50,000 | |
| | | | 18 | 45,000 | 40,000 | |
| Authorized Software Policy | Violation penalties | What punitive actions will you use for violations of authorized software policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Systems Development Testing | Intensity of quality assurance testing | How intense is your quality assurance testing? | Low | 40,000 | 50,000 | • Employee Morale<br>• Technical Security Index |
| | | | Medium | 60,000 | 150,000 | |
| | | | High | 90,000 | 300,000 | |
| Systems Development Testing | Degree of reliance on external vendor | Choose the degree of reliance on external vendors for systems development testing. | Usability and other minor testing | 10,000 | 50,000 | • Productivity<br>• Technical Security Index |
| | | | Supplementary testing | 20,000 | 100,000 | |
| | | | Comprehensive testing | 30,000 | 200,000 | |
| Antivirus Policy | Quality of antivirus solution used | Choose the quality of the antivirus solution used across the organization. | Baseline | 30,000 | 50,000 | • Performance<br>• Productivity<br>• Technical Security Index |
| | | | Strong | 50,000 | 100,000 | |
| | | | State-of-the-art | 70,000 | 180,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Antivirus Policy | Frequency of scans | How frequently does the antivirus scan run? | Multiple times per day | 24,000 | 28,800 | • Productivity<br>• Technical Security Index |
| | | | Once daily | 22,000 | 33,846 | |
| | | | Once per week | 16,500 | 15,000 | |
| | | | Once per month | 8,800 | 8,800 | |
| Antivirus Policy | Frequency of patch updates | How frequently will you update your antivirus solution with patches? | Always once released | 22,000 | 66,000 | • Productivity<br>• Technical Security Index |
| | | | Only for major and critical updates | 16,500 | 39,286 | |
| | | | Only for critical updates | 8,800 | 18,857 | |
| SCADA Vulnerability Analysis | SCADA vulnerability analysis spending | How much will you spend on SCADA vulnerability analysis? | Minimum | 100,000 | 10,000 | Technical Security Index |
| | | | Maximum | 250,000 | 20,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| SCADA Vulnerability Analysis | Standards review and update spending | How much will you spend on standards review and updating? | Minimum | 250,000 | 15,000 | • Performance<br>• Productivity<br>• Technical Security Index |
| | | | Maximum | 450,000 | 35,000 | |
| SCADA Vulnerability Analysis | Policy analysis spending | Choose your spending on SCADA vulnerability policy analysis. | Minimum | 100,000 | 15,000 | • Performance<br>• Productivity<br>• Technical Security Index |
| | | | Maximum | 200,000 | 50,000 | |
| SCADA Vulnerability Analysis | Physical SVA test spending | Determine your spending on physical SVA testing. | Minimum | 100,000 | 25,000 | • Performance<br>• Productivity<br>• Technical Security Index |
| | | | Maximum | 200,000 | 75,000 | |
| SCADA Vulnerability Analysis | Risk analysis spending | Choose how much you spend to bring in risk analysis experts. | Minimum | 125,000 | 25,000 | Technical Security Index |
| | | | Maximum | 500,000 | 50,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| SCADA Training | Network security spending | Determine your spending on network security. | Minimum | 100,000 | 10,000 | • Productivity<br>• Technical Security Index |
| | | | Maximum | 200,000 | 30,000 | |
| SCADA Training | SCADA security spending | Choose your spending on SCADA security. | Minimum | 100,000 | 10,000 | • Productivity<br>• Technical Security Index |
| | | | Maximum | 200,000 | 30,000 | |
| SCADA Training | Spending on training against social engineering | Determine your spending on training against social engineering. | Minimum | 100,000 | 15,000 | • Productivity<br>• Technical Security Index |
| | | | Maximum | 200,000 | 50,000 | |
| SCADA Security | Degree of interconnection with other networks | Choose the degree of interconnection with other networks. | Isolated | 5,000 | 250,000 | • Performance<br>• Technical Security Index |
| | | | Limited | 25,000 | 100,000 | |
| | | | High | 65,000 | 50,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| SCADA Security | Firewall sensitivity | Set the sensitivity of the firewalls in the SCADA setup. | Low | 10,000 | 20,000 | • Performance<br>• Technical Security Index |
| | | | Medium | 30,000 | 24,000 | |
| | | | Medium-high | 40,000 | 30,000 | |
| | | | High | 60,000 | 36,000 | |
| SCADA Security | Re-configure the registry of some equipment to make instructions temporarily unavailable | Re-configure the registry of SCADA equipment to make instructions temporarily unavailable, which acts as a buffer against intrusion. | Yes | 25,000 | 2,000 | • Performance<br>• Technical Security Index |
| | | | No | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| SCADA Security | SCADA security patch frequency | How frequently are SCADA security patches applied? | Quarterly | 300,000 | 1,500,000 | • Performance<br>• Productivity<br>• Technical Security Index |
| | | | Biannually | 200,000 | 1,000,000 | |
| | | | Annually | 125,000 | 700,000 | |
| | | | Bienially | 100,000 | 600,000 | |
| SCADA Security | SCADA access mechanism | How will you implement SCADA backdoor access? | Weak - direct backdoor access | 10,000 | 10,000 | • Performance<br>• Productivity<br>• Technical Security Index |
| | | | Stronger - callback mechanism | 25,000 | 20,000 | |
| SCADA Security | Continuous incident monitoring | Choose whether to enable or disable continuous incident monitoring. | Enable | 80,000 | 200,000 | Technical Security Index |
| | | | Disable | 2,000 | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|----------|----------|-------------|---------|------------------|--------------------|--------------------|
| SCADA Security | Remote access point privileges | Choose whether to enable or disable remote access privileges. | Enable | 50,000 | 50,000 | • Performance<br>• Productivity<br>• Technical Security Index |
| | | | Disable | 1,000 | - | |
| SCADA Policy Interventions | Risk management policy | How lenient is your policy on risk management? | Highly risk adverse | 100,000 | 100,000 | • Performance<br>• Productivity<br>• Technical Security Index |
| | | | Moderately risk adverse | 75,000 | 70,000 | |
| | | | Availability inclined | 20,000 | 50,000 | |
| SCADA Policy Interventions | Frequency of system backups in months | How frequently will you backup SCADA systems? | 2 | 15,000 | 20,000 | • Technical Security Index<br>• Compliance |
| | | | 3 | 15,000 | 17,500 | |
| | | | 4 | 15,000 | 14,000 | |
| | | | 6 | 15,000 | 10,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Insurance Policy | Degree of insurance used against a cyberattack | How high will you prioritize insurance against a cyberattack? | Low | 8,800 | 88,000 | • Disaster Readiness<br>• Compliance |
| | | | Medium | 16,500 | 132,000 | |
| | | | High | 22,000 | 33,000 | |

### 3.3 Federal Government

**Table 5: Federal Government Decision Reference**

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Authentication | Kerberos servers spending | How much will you spend on Kerberos servers for authentication? | Minimum | 3,750,000 | 125,000 | • Technical Security Index<br>• Performance<br>• Downtime |
| | | | Maximum | 10,000,000 | 250,000 | |
| Authentication | Key distribution centers spending | How much will you spend on key distribution centers for authentication? | Minimum | 250,000 | 100,000 | • Technical Security Index<br>• Performance<br>• Downtime |
| | | | Maximum | 625,000 | 200,000 | |
| Backup | RAID levels | What's the RAID level of your server backup? | 0 | 125,000 | 250,000 | • Performance<br>• Compliance<br>• Downtime |
| | | | 1 | 250,000 | 375,000 | |
| | | | 5 | 375,000 | 437,500 | |
| | | | 6 | 437,500 | 500,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|----------|----------|-------------|---------|------------------|--------------------|---------------------|
| Backup | Remote backup spending | Choose the amount to spend on remote backup services. | Minimum | 250,000 | 1,000,000 | • Performance<br>• Downtime<br>• Compliance |
| | | | Maximum | 500,000 | 2,000,000 | |
| Data Encryption | Level of encryption | What is the average scale of encryption used across the organization? | No encryption | 250,000 | - | • Technical Security Index<br>• Productivity |
| | | | File | 500,000 | 125,000 | |
| | | | Folder | 750,000 | 350,000 | |
| | | | Drive | 875,000 | 625,000 | |
| Data Encryption | Encryption strength in bits | The strength of encryption you will use; the higher the bit strength, the stronger the encryption. | 32 bits | 250,000 | 250,000 | • Technical Security Index<br>• Performance |
| | | | 64 bits | 500,000 | 375,000 | |
| | | | 128 bits | 625,000 | 500,000 | |
| Load Management | DDOS protection through delayed binding | Delay binding to protect against DDOS attacks. | Disable | - | - | • Technical Security Index<br>• Performance |
| | | | Enable | 750,000 | 625,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Load Management | HTTP security through load balancing | Use load balancing to improve security. | Disable | - | - | • Technical Security Index<br>• Performance |
| | | | Enable | 1,500,000 | 500,000 | |
| Patch Management | Frequency of patch management | Determine the frequency of rolling out updates to systems. | Critical updates only | 250,000 | 250,000 | • Productivity<br>• Performance<br>• Technical Security Index |
| | | | Critical and important updates | 500,000 | 500,000 | |
| | | | All updates | 1,000,000 | 1,000,000 | |
| Patch Management | Degree of patch testing prior to installation | How rigorously will you test patches before installing them? | Low | 250,000 | 125,000 | • Performance<br>• Technical Security Index |
| | | | Medium | 500,000 | 250,000 | |
| | | | High | 1,000,000 | 375,000 | |
| Patch Management | Trustworthiness of patch | Will you rely only on official patches, or are you willing to use unofficial or community workarounds? | Unofficial | 125,000 | 62,500 | • Downtime<br>• Performance |
| | | | Trusted | 250,000 | 125,000 | |
| | | | Official | 375,000 | 187,500 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Role Based Access Control | Degree of role-based access control | What is the degree of implementation of access control by employee role? | Low | 500,000 | 250,000 | • Technical Security Index<br>• Employee Morale |
| | | | Medium | 750,000 | 500,000 | |
| | | | High | 1,100,000 | 750,000 | |
| Virtualization OR Cloud Computing | Choose virtualization or cloud computing | Choose virtualization or cloud computing for your systems to improve security. | Virtualization | 250,000 | 125,000 | Technical Security Index |
| | | | Cloud computing | 1,250,000 | 250,000 | |
| If Virtualization Chosen | Degree of virtualization | To what degree will you implement virtualization? | Limited | 50,000 | 250,000 | Technical Security Index |
| | | | Significant | 175,000 | 500,000 | |
| | | | Full | 500,000 | 1,000,000 | |
| If Virtualization Chosen | Spending on underlying physical network | How much will you spend on the underlying physical network? | Minimum | 250,000 | - | Technical Security Index |
| | | | Maximum | 1,250,000 | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| If Virtualization Chosen | Degree of isolation of network | How isolated is the network under the virtualization schema? | Minor | 250,000 | 500,000 | • Performance • Technical Security Index |
| | | | Medium | 750,000 | 750,000 | |
| | | | Complete | 1,500,000 | 1,250,000 | |
| If Virtualization Chosen | Traffic monitoring on network | Choose the extent of traffic monitoring on the network. | Limited | 250,000 | 125,000 | • Performance • Technical Security Index |
| | | | Significant | 500,000 | 500,000 | |
| | | | Full | 750,000 | 750,000 | |
| If Cloud Computing Chosen | Cloud hosting model | Choose the cloud hosting model for your systems. Will you pay more for a more secure private infrastructure or share deployment with other companies for less cost? | Private | 438,000 | 250,286 | • Technical Security Index • Performance |
| | | | Hybrid | 340,000 | 170,000 | |
| | | | Public | 200,000 | 150,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| If Cloud Computing Chosen | Services offered by the cloud | At what level of engagement will you operate off the cloud? Will you stick with software, or will you go all the way to infrastructure? | Software as a service | 250,000 | 500,000 | • Technical Security Index<br>• Performance |
| | | | Platform as a service | 500,000 | 750,000 | |
| | | | Infrastructure as a service | 1,000,000 | 1,500,000 | |
| Firewall | Filtering strictness | How strict is the firewall configured to be? | Low | 125,000 | 125,000 | • Productivity<br>• Technical Security Index<br>• Performance |
| | | | Medium | 250,000 | 187,500 | |
| | | | Medium-high | 312,500 | 250,000 | |
| | | | High | 437,500 | 312,500 | |
| DNS Redundancy | DNS server redundancy | Enable DNS server redundancy to reduce downtime. | Yes | 250,000 | 375,000 | Downtime |
| | | | No | 125,000 | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| DNS Redundancy | Split DNS topology | Use a split DNS topology to reduce downtime. | Yes | 125,000 | 375,000 | Downtime |
| | | | No | 250,000 | - | |
| Database Security | Frequency of forcing password changes in days | How frequently does the database ask for a change of password? | 15 | 1,000,000 | 125,000 | • Productivity<br>• Technical Security Index |
| | | | 30 | 750,000 | 125,000 | |
| | | | 60 | 500,000 | 125,000 | |
| | | | 90 | 250,000 | 125,000 | |
| Database Security | Degree of separation of roles for admin and operator roles | Choose to separate admin and operator roles for database systems. | None | 250,000 | - | • Productivity<br>• Technical Security Index |
| | | | Limited | 500,000 | 6,250,000 | |
| | | | Complete | 750,000 | 8,750,000 | |
| Database Security | Control privileges | Are database control privileges restricted or distributed? | Restricted | 250,000 | 2,250,000 | • Productivity<br>• Technical Security Index |
| | | | Distributed | 125,000 | 4,500,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Database Security | OS services and associated ports | Will you enable or disable database-related OS services and associated ports? | Disable | - | - | • Productivity<br>• Performance<br>• Technical Security Index |
|  |  |  | Enable | - | - |  |
| Database Security | Database honeypots | Will you employ database honeypots to trap and redirect attacks? | Disable | - | - | • Productivity<br>• Technical Security Index |
|  |  |  | Enable | - | - |  |
| IDPS | Type of intrusion detection system to install | Will you employ a network-based IDS, a host-based IDS, or both? | Network-based intrusion detection (NIDS) | 250,000 | 2,500,000 | Technical Security Index |
|  |  |  | Host-based intrusion detection (HIDS) | 750,000 | 2,000,000 |  |
|  |  |  | Both | 900,000 | 4,000,000 |  |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| IDPS | Class of honeypot to deploy | Will you use a production honeypot or go for a research honeypot with better analytics? | Production honeypot | 500,000 | 2,250,000 | Technical Security Index |
| | | | Research honeypot | 250,000 | 1,750,000 | |
| IDPS | Strength of honeypot to deploy | How strong is the honeypot you deploy? | Pure honeypot | 250,000 | 2,250,000 | Technical Security Index |
| | | | Low interaction honeypot | 500,000 | 1,500,000 | |
| | | | High interaction honeypot | 750,000 | 2,250,000 | |
| Hiring and Employee Policy | IT team size | What strength will you keep your IT teams at, in relation to the industry average? | Less than average | 250,000 | 15,000,000 | • Productivity • Employee Morale • Technical Security Index |
| | | | Average | 750,000 | 22,500,000 | |
| | | | More than average | 1,250,000 | 35,000,000 | |
| Hiring and Employee Policy | Full-time employees as a percentage of the workforce | Will you choose to bolster your IT team with temporary or part-time hires? | All | 200,000 | 96,000 | • Productivity • Employee Morale • Technical Security Index |
| | | | 0.9 | 340,000 | 81,600 | |
| | | | 0.8 | 438,000 | 116,800 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Hiring and Employee Policy | Hiring by average experience in years | What's the average experience you're looking for when you hire for IT teams? | 3 | 200,000 | 294,118 | Internal Security Index |
| | | | 5 | 340,000 | 432,727 | |
| | | | 7 | 438,000 | 525,600 | |
| | | | 8 | 600,000 | 685,714 | |
| | | | 9 | 625,000 | 732,759 | |
| Hiring and Employee Policy | Spending on background check of DSS or other vendors | How much will you spend on background checks on DSS or other vendors? | Minimum | 10,000 | 625,000 | Internal Security Index |
| | | | Maximum | 20,000 | 1,250,000 | |
| Hiring and Employee Policy | Forced rotation of employees | Will you make employee rotation mandatory? | Disable | - | - | • Productivity<br>• Employee Morale<br>• Internal Security Index |
| | | | Enable | 625,000 | 1,125,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Hiring and Employee Policy | Forced vacation for employees | Will you make employee vacations mandatory? | Disable | - | - | • Productivity<br>• Employee Morale<br>• Internal Security Index |
| | | | Enable | 1,875,000 | 2,125,000 | |
| Training | Training by funding | What is the extent of funding for cybersecurity training? | Minimum | 25,000 | 1,250,000 | • Internal Security Index<br>• Productivity<br>• Employee Morale |
| | | | Maximum | 50,000 | 2,500,000 | |
| Training Incentives | Average compensation bonus as a fraction of technical certification fees | How much will you reimburse employees for technical certification for security training? | 25% of fees | 125,000 | 500,000 | • Technical Security Index<br>• Productivity<br>• Employee Morale |
| | | | 50% of fees | 250,000 | 1,000,000 | |
| | | | 75% of fees | 375,000 | 1,500,000 | |
| | | | 100% of fees | 500,000 | 2,000,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Training Incentives | Link training outcomes to promotion | Will you link training outcomes to promotion? | Yes | 250,000 | 250,000 | • Technical Security Index • Productivity • Employee Morale |
| | | | No | - | - | |
| Training Incentives | Link training outcomes to evaluation | Will you link training outcomes to evaluation? | Yes | 375,000 | 175,000 | • Technical Security Index • Productivity • Employee Morale |
| | | | No | - | - | |
| Training and Auditing | Focus on training area: network vulnerabilities | Choose whether to focus your security auditing efforts on network vulnerabilities, controls, encryption, and penetration. | Minimum | - | - | • Technical Security Index • Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Focus on training area: controls | | Minimum | - | - | • Technical Security Index • Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Focus on training area: encryption | | Minimum | - | - | • Technical Security Index • Compliance |
| | | | Maximum | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Training and Auditing | Focus on training area: penetration testing | | Minimum | - | - | • Technical Security Index<br>• Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Frequency of physical audits of the equipment | How often will you run physical audits of system equipment? | Every three months | 250,000 | 500,000 | Technical Security Index |
| | | | Every six months | 187,500 | 250,000 | |
| | | | Once a year | 125,000 | 125,000 | |
| Business Continuity Planning | Degree of IT data storage redundancy | How much redundancy will you build in for IT data storage? | Low | 125,000 | 125,000 | Disaster Readiness |
| | | | Medium | 250,000 | 250,000 | |
| | | | High | 375,000 | 500,000 | |
| Business Continuity Planning | Degree of IT network redundancy | How much redundancy will you build in for IT networks? | Low | 187,500 | 500,000 | Disaster Readiness |
| | | | Medium | 312,500 | 750,000 | |
| | | | High | 500,000 | 1,250,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Business Continuity Planning | Levels of power backup redundancy | How much redundancy will you build in for power backup? | 1 | 125,000 | 625,000 | Disaster Readiness |
| | | | 2 | 250,000 | 1,125,000 | |
| | | | 3 | 375,000 | 1,687,500 | |
| Business Continuity Planning | Number of backup sites | How many backup sites will you maintain? | 1 | 125,000 | 1,875,000 | Disaster Readiness |
| | | | 2 | 250,000 | 3,750,000 | |
| | | | 3 | 375,000 | 5,000,000 | |
| Business Continuity Planning | Number of redundant backup communication links | How many backup communication links will you maintain? | 1 | 125,000 | 250,000 | Disaster Readiness |
| | | | 2 | 250,000 | 437,500 | |
| | | | 3 | 375,000 | 625,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Business Continuity Planning | Policy review frequency in months | How often will you review disaster recovery policy? | 3 | - | 2,500,000 | Disaster Readiness |
| | | | 6 | - | 1,875,000 | |
| | | | 9 | - | 1,250,000 | |
| | | | 12 | - | 625,000 | |
| Information Sharing | Degree of information sharing on attacks | To what extent does the organization share cybersecurity attack information publicly? | High - full disclosure | 200,000 | 40,000 | • Profitability<br>• Disaster Readiness |
| | | | Medium - non-sensitive disclosure | 340,000 | 85,000 | |
| | | | Low - no disclosure | - | - | |
| Information Sharing | Degree of non-crisis information sharing | To what extent does the organization share routine cybersecurity information publicly? | High - full disclosure | 340,000 | 72,857 | • Profitability<br>• Disaster Readiness |
| | | | Medium - non-sensitive disclosure | 200,000 | 40,000 | |
| | | | Low - no disclosure | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Public Relations | Spending on public relations | How much will you spend on public relations? | Minimum | 1,250,000 | 625,000 | Reputation |
| | | | Maximum | 2,500,000 | 2,500,000 | |
| Emergency Bypass Policy | Spending on emergency bypass policy | How much will you spend on emergency bypass policy? | Minimum | 125,000 | 25,000 | Disaster Readiness |
| | | | Maximum | 250,000 | 50,000 | |
| Emergency Bypass Policy | Response to violations of typical separation of duties protocol | What is the response to violations of typical Separation of Duties protocol? | Not allowed | 625,000 | 312,500 | • Technical Security Index • Disaster Readiness |
| | | | Permitted with limitations | 375,000 | 500,000 | |
| | | | Allowed | 62,500 | 875,000 | |
| Emergency Bypass Policy | Violation penalties | What punitive actions will you use for violations of emergency bypass policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Sharing Policy | No. of people in groups to overlook and enforce internal information sharing | How many people will you put in groups to overlook and enforce information sharing? | 2 | 400,000 | 272,727 | • Productivity<br>• Technical Security Index<br>• Employee Morale |
| | | | 3 | 680,000 | 456,716 | |
| | | | 4 | 876,000 | 597,273 | |
| | | | 5 | 1,200,000 | 782,609 | |
| | | | 6 | 1,250,000 | 758,929 | |
| Information Sharing Policy | Internal information sharing by role-based access control | How restrictive is the system for internal sharing of information? | Strictly need-to-know | 375,000 | 1,250,000 | • Productivity<br>• Technical Security Index<br>• Employee Morale |
| | | | Limited access | 250,000 | 875,000 | |
| | | | Open system | 25,000 | - | |
| Information Sharing Policy | Degree of external information sharing | How restrictive is the system for external sharing of information? | Strictly need-to-know | 375,000 | 1,250,000 | • Productivity<br>• Technical Security Index<br>• Customer Satisfaction<br>• Compliance |
| | | | Limited access | 250,000 | 875,000 | |
| | | | Open system | 25,000 | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Sharing Policy | Frequency of disclosure for InfraGard communication in days | How frequently will you share information for the InfraGard service of information sharing between private and public entities? | 7 days | 600,000 | 50,000 | • Contribution to National Security Index<br>• Profitability |
| | | | 14 days | 438,000 | 87,600 | |
| | | | 21 days | 340,000 | 204,000 | |
| | | | 28 days | 200,000 | 200,000 | |
| Information Sharing Policy | Violation penalties | What punitive actions will you use for violations of information sharing policy? | Warnings | - | - | Employee Morale |
| | | | Fines | - | - | |
| | | | Suspensions | - | - | |
| | | | Termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Breach Notification Policy | Degree of openness of breach notification | How open is your organization about breaches that have happened to its systems? | All incidents | 600,000 | 1,250,000 | • Reputation<br>• Customer Satisfaction<br>• Contribution to National Security Index |
| | | | Critical and significant incidents | 438,000 | 875,000 | |
| | | | Only critical incidents | 340,000 | 500,000 | |
| | | | None of the incidents | 200,000 | 0 | |
| Breach Notification Policy | Investigative agencies to call in for major security breaches | Which investigative agencies will you approach for major security breaches? | Private investigators | 200,000 | 285,714 | • Reputation<br>• Employee Morale<br>• Contribution to National Security Index<br>• Downtime |
| | | | Forensic investigators | 340,000 | 510,000 | |
| | | | CERT | - | - | |
| | | | FBI/NSA | - | - | |
| Breach Notification Policy | Violation penalties | What punitive actions will you use for violations of breach notification policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Privacy Policy | Privacy program investment spending | How much will you spend on your organization's privacy program? | Minimum | 250,000 | 125,000 | • Employee Morale <br> • Customer Satisfaction |
| | | | Maximum | 1,250,000 | 250,000 | |
| Information Privacy Policy | Appoint a dedicated privacy officer | Will you appoint a dedicated privacy officer? | Yes | 200,000 | 240,000 | • Employee Morale <br> • Customer Satisfaction |
| | | | No | - | - | |
| Information Privacy Policy | Privacy training spending for employees | How much will you spend on training employees on privacy policies? | Minimum | 250,000 | 125,000 | • Employee Morale <br> • Customer Satisfaction |
| | | | Maximum | 1,000,000 | 250,000 | |
| Information Privacy Policy | Degree of information and record retention | What sort of information will you retain? | Critical information | 625,000 | 500,000 | • Performance <br> • Employee Morale |
| | | | Operational information | 375,000 | 1,875,000 | |
| | | | All information | 937,500 | 2,750,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Privacy Policy | Violation penalties | What punitive actions will you use for violations of information privacy policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| General Access Policies | Degree of freedom given to employees regarding communications over the Internet | How free are your employees to communicate over the Internet? | Restricted | 312,500 | 1,250,000 | • Employee Morale • Productivity |
| | | | Time-limited | 312,500 | 1,250,000 | |
| | | | Free | - | - | |
| General Access Policies | Degree of freedom over browsing non-business sites | How free are your employees to browse non-business sites? | Restricted | 125,000 | 1,250,000 | • Employee Morale • Productivity |
| | | | Time-limited | 250,000 | 1,250,000 | |
| | | | Free | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| General Access Policies | Degree of logging of Internet access and other system actions and accesses | Choose the degree to which Internet access and other system actions and access are logged. | None | - | - | • Internal Security Index<br>• Employee Morale |
| | | | Limited actions | 250,000 | 500,000 | |
| | | | Critical system access only | 625,000 | 1,875,000 | |
| | | | All actions | 1,250,000 | 3,125,000 | |
| General Access Policies | Number of permitted login attempts | Choose the number of permitted login attempts. | 3 | - | - | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 5 | - | - | |
| | | | 7 | - | - | |
| General Access Policies | Password validity in days | How long will passwords set be valid? | 15 | 500,000 | 750,000 | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 30 | 500,000 | 375,000 | |
| | | | 45 | 500,000 | 250,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| General Access Policies | Password length requirements | How many characters long should the password be? | 4 | 500,000 | 250,000 | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 6 | 750,000 | 250,000 | |
| | | | 8 | 1,125,000 | 250,000 | |
| General Access Policies | Non-use of prior passwords | How many prior passwords are set to be invalid for use? | 1 | - | - | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 3 | - | - | |
| | | | 6 | - | - | |
| General Access Policies | Violation penalties | What punitive actions will you use for violations of general access policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Physical Security | Physically isolate rooms containing important infrastructure | Control the degree of physical access to servers. | Free access | 250,000 | - | Technical Security Index |
| | | | Limited access | 625,000 | 500,000 | |
| | | | Restricted access | 750,000 | 375,000 | |
| Physical Security | Restricting physical access through role based access control | Control the degree of physical access to servers through role-based access control. | Free access | 125,000 | - | • Productivity<br>• Disaster Readiness<br>• Technical Security Index |
| | | | Limited access | 312,500 | 50,000 | |
| | | | Restricted access | 375,000 | 375,000 | |
| Physical Security | Degree of access given to visitors | Control the degree and quality of access for visitors. | Free access | 250,000 | - | • Productivity<br>• Technical Security Index |
| | | | Limited access | 500,000 | 250,000 | |
| | | | Accompanied free access | 750,000 | 3,750,000 | |
| | | | Accompanied limited access | 1,000,000 | 6,250,000 | |
| | | | Restricted access | 1,250,000 | 7,500,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Physical Security | Violation penalties | What punitive actions will you use for violations of physical security policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Remote Access Policy | Degree of remote access by employee grade | For which employee grades is remote access available? | Executive management only | 250,000 | 62,500 | • Technical Security Index<br>• Productivity |
| | | | Upper management | 375,000 | 187,500 | |
| | | | Middle management | 500,000 | 625,000 | |
| | | | All professional staff members | 875,000 | 2,500,000 | |
| Remote Access Policy | Access privileges permitted | What are the maximum remote access privileges allowed? | Low - read only | 250,000 | 125,000 | • Technical Security Index<br>• Productivity |
| | | | Medium - read/write | 375,000 | 125,000 | |
| | | | High - read/write/delete | 500,000 | 250,000 | |
| | | | Very high - administrator level | 875,000 | 250,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Remote Access Policy | Violation penalties | What punitive actions will you use for violations of remote access policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Authorized Software Policy | Type of software permitted for use by employees | How lenient are you in terms of software usage? | Freeware | - | - | • Employee Morale<br>• Technical Security Index |
| | | | Games | 500,000 | 750,000 | |
| | | | Open-source | - | - | |
| | | | Approved software | 2,500,000 | 3,750,000 | |
| Authorized Software Policy | Software evaluation frequency in months | How frequently will you evaluate systems for presence of unauthorized software? | 6 | 625,000 | 2,125,000 | • Productivity<br>• Technical Security Index |
| | | | 12 | 875,000 | 1,250,000 | |
| | | | 18 | 1,125,000 | 1,000,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Authorized Software Policy | Violation penalties | What punitive actions will you use for violations of authorized software policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Systems Development Testing | Intensity of quality assurance testing | How intense is your quality assurance testing? | Low | 1,000,000 | 1,250,000 | • Employee Morale<br>• Technical Security Index |
| | | | Medium | 1,500,000 | 3,750,000 | |
| | | | High | 2,250,000 | 7,500,000 | |
| Systems Development Testing | Degree of reliance on external vendor | Choose the degree of reliance on external vendors for systems development testing. | Usability and other minor testing | 250,000 | 1,250,000 | • Productivity<br>• Technical Security Index |
| | | | Supplementary testing | 500,000 | 2,500,000 | |
| | | | Comprehensive testing | 750,000 | 5,000,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Antivirus Policy | Quality of antivirus solution used | Choose the quality of the antivirus solution used across the organization. | Baseline | 750,000 | 1,250,000 | • Performance<br>• Productivity<br>• Technical Security Index |
| | | | Strong | 1,250,000 | 2,500,000 | |
| | | | State-of-the-art | 1,750,000 | 4,500,000 | |
| Antivirus Policy | Frequency of scans | How frequently does the antivirus scan run? | Multiple times per day | 600,000 | 720,000 | • Productivity<br>• Technical Security Index |
| | | | Once daily | 438,000 | 673,846 | |
| | | | Once per week | 340,000 | 309,091 | |
| | | | Once per month | 200,000 | 200,000 | |
| Antivirus Policy | Frequency of patch updates | How frequently will you update your antivirus solution with patches? | Always once released | 438,000 | 1,314,000 | • Productivity<br>• Technical Security Index |
| | | | Only for major and critical updates | 340,000 | 809,524 | |
| | | | Only for critical updates | 200,000 | 428,571 | |
| CERT Controls | CERT funding | Choose the spending on CERT. | Minimum | 1,250,000 | 125,000 | Contribution to National Security Index |
| | | | Maximum | 3,000,000 | 250,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| CERT Controls | Frequency of automated advisories in days | How frequent is the issuance of automated advisories from CERT? | 4 | 625,000 | 1,875,000 | Contribution to National Security Index |
| | | | 5 | 500,000 | 1,500,000 | |
| | | | 6 | 375,000 | 1,125,000 | |
| | | | 8 | 250,000 | 875,000 | |
| | | | 10 | 125,000 | 625,000 | |
| CERT Controls | Experience of CERT responders in years | Choose the average experience of the CERT responder. | 2 | 125,000 | 2,500,000 | Contribution to National Security Index |
| | | | 4 | 250,000 | 3,000,000 | |
| | | | 6 | 375,000 | 3,375,000 | |
| | | | 8 | 500,000 | 3,750,000 | |
| | | | 10 | 625,000 | 4,375,000 | |
| CERT Controls | Training allocation funding | Choose the spending on CERT training. | Minimum | 1,250,000 | 1,000,000 | Contribution to National Security Index |
| | | | Maximum | 3,000,000 | 3,000,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| CERT Controls | Vulnerability database maintenance funding | Choose the spending on vulnerability database maintenance. | Minimum | 500,000 | 250,000 | Contribution to National Security Index |
| | | | Maximum | 1,500,000 | 500,000 | |
| Other Responders | Funding for FBI responder maintenance | Choose the funding for FBI responder maintenance. | Minimum | 1,250,000 | 3,000,000 | Contribution to National Security Index |
| | | | Maximum | 2,500,000 | 5,000,000 | |
| Other Responders | Funding for training FBI agents on cybersecurity issues | Choose the funding for FBI agent training on cybersecurity. | Minimum | 1,250,000 | 500,000 | Contribution to National Security Index |
| | | | Maximum | 3,000,000 | 1,250,000 | |
| Other Responders | Cybersecurity school education programs spending | Specify the funding for cybersecurity school education programs. | Minimum | 2,000,000 | 2,000,000 | Contribution to National Security Index |
| | | | Maximum | 3,500,000 | 4,000,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Other Responders | US Secret Service investment for financial crimes | Specify the funding for Secret Service investment against financial crimes. | Minimum | 1,000,000 | 1,000,000 | Contribution to National Security Index |
| | | | Maximum | 2,000,000 | 2,500,000 | |
| ISACs | Funding for the ISAC | Choose the funding for the ISAC. | Minimum | 1,250,000 | 1,000,000 | Contribution to National Security Index |
| | | | Maximum | 2,000,000 | 3,000,000 | |
| ISACs | Training and certification programs funding | Choose the funding for training and certification programs for the ISACs. | Minimum | 1,200,000 | 1,500,000 | Contribution to National Security Index |
| | | | Maximum | 3,250,000 | 3,000,000 | |
| Research Funding | Cybersecurity research funding | Specify the funding for cybersecurity research. | Minimum | 2,000,000 | 1,000,000 | Contribution to National Security Index |
| | | | Maximum | 25,000,000 | 17,500,000 | |
| Research Funding | Specific technology labs funding | Specify the funding for specific technology. | Minimum | 2,000,000 | 333,333 | Contribution to National Security Index |
| | | | Maximum | 25,000,000 | 5,000,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Research Funding | University program funding | Specify the funding for cybersecurity programs in universities. | Minimum | 2,000,000 | 400,000 | Contribution to National Security Index |
| | | | Maximum | 25,000,000 | 2,500,000 | |
| Research Funding | Funding centers of excellence in information assurance research | Specify the funding for centers of excellence in information assurance research. | Minimum | 2,000,000 | 1,000,000 | Contribution to National Security Index |
| | | | Maximum | 5,000,000 | 3,000,000 | |
| Advisories | NSA security configuration guide creation spending | Choose the funding for creating NSA security configuration guides. | Minimum | 25,000 | 250,000 | Contribution to National Security Index |
| | | | Maximum | 1,000,000 | 750,000 | |
| Advisories | NIST library funding | Choose the funding for the NIST library. | Minimum | 500,000 | 300,000 | Contribution to National Security Index |
| | | | Maximum | 1,000,000 | 500,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Supply Tools | Degree of support offered to private companies | What is the degree of support offered to private companies for cybersecurity issues? | Low | 125,000 | 15,000,000 | Contribution to National Security Index |
| | | | Medium | 250,000 | 35,000,000 | |
| | | | High | 375,000 | 75,000,000 | |
| Supply Tools | Nature of support offered to private companies | How strong are the cybersecurity tools offered to private companies? | Low-level security tools | 125,000 | 1,875,000 | Contribution to National Security Index |
| | | | Sophisticated security tools | 250,000 | 3,750,000 | |
| | | | Internally developed tools | 375,000 | 3,750,000 | |
| External Collaboration | Degree of collaboration with allies and Interpol | Choose the degree of collaboration with allies and Interpol. | Low | 125,000 | 15,000,000 | • Contribution to National Security Index<br>• International Policy Burden |
| | | | Medium | 250,000 | 35,000,000 | |
| | | | High | 375,000 | 80,000,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Federal Gov. Information Classification | Strictness of cybersecurity information classification | Choose the strictness of cybersecurity information classification. | Unclassified | 125,000 | - | • Contribution to National Security Index<br>• International Policy Burden |
| | | | Classified | 250,000 | 15,000,000 | |
| | | | Secret | 375,000 | 30,000,000 | |
| | | | Top secret | 500,000 | - | |
| | | | Top secret/SCI | 625,000 | - | |

### 3.4 Hytema

**Table 6: Hytema Decision Reference**

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Authentication | Kerberos servers spending | How much will you spend on Kerberos servers for authentication? | Minimum | 150,000 | 5,000 | • Technical Security Index<br>• Performance<br>• Downtime |
| | | | Maximum | 400,000 | 10,000 | |
| Authentication | Key distribution centers spending | How much will you spend on key distribution centers for authentication? | Minimum | 10,000 | 4,000 | • Technical Security Index<br>• Performance<br>• Downtime |
| | | | Maximum | 25,000 | 8,000 | |
| Backup | RAID levels | What's the RAID level of your server backup? | 0 | 5,000 | 10,000 | • Performance<br>• Compliance<br>• Downtime |
| | | | 1 | 10,000 | 15,000 | |
| | | | 5 | 15,000 | 17,500 | |
| | | | 6 | 17,500 | 20,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Backup | Remote backup spending | Choose the amount to spend on remote backup services. | Minimum | 10,000 | 40,000 | • Performance<br>• Downtime<br>• Compliance |
| | | | Maximum | 20,000 | 80,000 | |
| Data Encryption | Level of encryption | What is the average scale of encryption used across the organization? | No encryption | 10,000 | - | • Technical Security Index<br>• Productivity |
| | | | File | 20,000 | 5,000 | |
| | | | Folder | 30,000 | 14,000 | |
| | | | Drive | 35,000 | 25,000 | |
| Data Encryption | Encryption strength in bits | The strength of encryption you will use; the higher the bit strength, the stronger the encryption. | 32 bits | 10,000 | 10,000 | • Technical Security Index<br>• Performance |
| | | | 64 bits | 20,000 | 15,000 | |
| | | | 128 bits | 25,000 | 20,000 | |
| Load Management | DDOS protection through delayed binding | Delay binding to protect against DDOS attacks. | Disable | - | - | • Technical Security Index<br>• Performance |
| | | | Enable | 30,000 | 25,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Load Management | HTTP security through load balancing | Use load balancing to improve security. | Disable | - | - | • Technical Security Index<br>• Performance |
| | | | Enable | 60,000 | 20,000 | |
| Patch Management | Frequency of patch management | Determine the frequency of rolling out updates to systems. | Critical updates only | 10,000 | 10,000 | • Productivity<br>• Performance<br>• Technical Security Index |
| | | | Critical and important updates | 20,000 | 20,000 | |
| | | | All updates | 40,000 | 40,000 | |
| Patch Management | Degree of patch testing prior to installation | How rigorously will you test patches before installing them? | Low | 10,000 | 5,000 | • Performance<br>• Technical Security Index |
| | | | Medium | 20,000 | 10,000 | |
| | | | High | 40,000 | 15,000 | |
| Patch Management | Trustworthiness of patch | Will you rely only on official patches, or are you willing to use unofficial or community workarounds? | Unofficial | 5,000 | 2,500 | • Downtime<br>• Performance |
| | | | Trusted | 10,000 | 5,000 | |
| | | | Official | 15,000 | 7,500 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Role Based Access Control | Degree of role-based access control | What is the degree of implementation of access control by employee role? | Low | 20,000 | 10,000 | • Technical Security Index<br>• Employee Morale |
| | | | Medium | 30,000 | 20,000 | |
| | | | High | 44,000 | 30,000 | |
| Virtualization OR Cloud Computing | Choose virtualization or cloud computing | Choose virtualization or cloud computing for your systems to improve security. | Virtualization | 10,000 | 5,000 | Technical Security Index |
| | | | Cloud computing | 50,000 | 10,000 | |
| If Virtualization Chosen | Degree of virtualization | To what degree will you implement virtualization? | Limited | 2,000 | 10,000 | Technical Security Index |
| | | | Significant | 7,000 | 20,000 | |
| | | | Full | 20,000 | 40,000 | |
| If Virtualization Chosen | Spending on underlying physical network | How much will you spend on the underlying physical network? | Minimum | 10,000 | - | Technical Security Index |
| | | | Maximum | 50,000 | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| If Virtualization Chosen | Degree of isolation of network | How isolated is the network under the virtualization schema? | Minor | 10,000 | 20,000 | • Performance<br>• Technical Security Index |
| | | | Medium | 30,000 | 30,000 | |
| | | | Complete | 60,000 | 50,000 | |
| If Virtualization Chosen | Traffic monitoring on network | Choose the extent of traffic monitoring on the network. | Limited | 10,000 | 5,000 | • Performance<br>• Technical Security Index |
| | | | Significant | 20,000 | 20,000 | |
| | | | Full | 30,000 | 30,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|----------|----------|-------------|---------|------------------|--------------------|--------------------|
| If Cloud Computing Chosen | Cloud hosting model | Choose the cloud hosting model for your systems. Will you pay more for a more secure private infrastructure or share deployment with other companies for less cost? | Private | 22,000 | 12,571 | • Technical Security Index<br>• Performance |
| | | | Hybrid | 16,500 | 8,250 | |
| | | | Public | 8,800 | 6,600 | |
| If Cloud Computing Chosen | Services offered by the cloud | At what level of engagement will you operate off the cloud? Will you stick with software, or will you go all the way to infrastructure? | Software as a service | 10,000 | 20,000 | • Technical Security Index<br>• Performance |
| | | | Platform as a service | 20,000 | 30,000 | |
| | | | Infrastructure as a service | 40,000 | 60,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Firewall | Filtering strictness | How strict is the firewall configured to be? | Low | 5,000 | 5,000 | • Productivity<br>• Technical Security Index<br>• Performance |
| | | | Medium | 10,000 | 7,500 | |
| | | | Medium-high | 12,500 | 10,000 | |
| | | | High | 17,500 | 12,500 | |
| DNS Redundancy | DNS server redundancy | Enable DNS server redundancy to reduce downtime. | Yes | 10,000 | 15,000 | Downtime |
| | | | No | 5,000 | - | |
| DNS Redundancy | Split DNS topology | Use a split DNS topology to reduce downtime. | Yes | 5,000 | 15,000 | Downtime |
| | | | No | 10,000 | - | |
| Database Security | Frequency of forcing password changes in days | How frequently does the database ask for a change of password? | 15 | 40,000 | 5,000 | • Productivity<br>• Technical Security Index |
| | | | 30 | 30,000 | 5,000 | |
| | | | 60 | 20,000 | 5,000 | |
| | | | 90 | 10,000 | 5,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Database Security | Degree of separation of roles for admin and operator roles | Choose to separate admin and operator roles for database systems. | None | 10,000 | - | • Productivity<br>• Technical Security Index |
| | | | Limited | 20,000 | 250,000 | |
| | | | Complete | 30,000 | 350,000 | |
| Database Security | Control privileges | Are database control privileges restricted or distributed? | Restricted | 10,000 | 90,000 | • Productivity<br>• Technical Security Index |
| | | | Distributed | 5,000 | 180,000 | |
| Database Security | OS services and associated ports | Will you enable or disable database-related OS services and associated ports? | Disable | - | - | • Productivity<br>• Performance<br>• Technical Security Index |
| | | | Enable | - | - | |
| Database Security | Database honeypots | Will you employ database honeypots to trap and redirect attacks? | Disable | - | - | • Productivity<br>• Technical Security Index |
| | | | Enable | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| IDPS | Type of intrusion detection system to install | Will you employ a network-based IDS, a host-based IDS, or both? | Network-based intrusion detection (NIDS) | 10,000 | 100,000 | Technical Security Index |
| | | | Host-based intrusion detection (HIDS) | 30,000 | 80,000 | |
| | | | Both | 36,000 | 160,000 | |
| IDPS | Class of honeypot to deploy | Will you use a production honeypot or go for a research honeypot with better analytics? | Production honeypot | 20,000 | 90,000 | Technical Security Index |
| | | | Research honeypot | 10,000 | 70,000 | |
| IDPS | Strength of honeypot to deploy | How strong is the honeypot you deploy? | Pure honeypot | 10,000 | 90,000 | Technical Security Index |
| | | | Low interaction honeypot | 20,000 | 60,000 | |
| | | | High interaction honeypot | 30,000 | 90,000 | |
| Hiring and Employee Policy | IT team size | What strength will you keep your IT teams at, in relation to the industry average? | Less than average | 10,000 | 600,000 | • Productivity<br>• Employee Morale<br>• Technical Security Index |
| | | | Average | 30,000 | 900,000 | |
| | | | More than average | 50,000 | 1,400,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|----------|----------|-------------|---------|------------------|--------------------|---------------------|
| Hiring and Employee Policy | Full-time employees as a percentage of the workforce | Will you choose to bolster your IT team with temporary or part-time hires? | All | 8,800 | 4,224 | • Productivity<br>• Employee Morale<br>• Technical Security Index |
| | | | 0.9 | 16,500 | 3,960 | |
| | | | 0.8 | 22,000 | 5,867 | |
| Hiring and Employee Policy | Hiring by average experience in years | What's the average experience you're looking for when you hire for IT teams? | 3 | 8,800 | 12,941 | Internal Security Index |
| | | | 5 | 16,500 | 21,000 | |
| | | | 7 | 22,000 | 26,400 | |
| | | | 8 | 24,000 | 27,429 | |
| | | | 9 | 25,000 | 29,310 | |
| Hiring and Employee Policy | Forced rotation of employees | Will you make employee rotation mandatory? | Disable | - | - | • Productivity<br>• Employee Morale<br>• Internal Security Index |
| | | | Enable | 25,000 | 45,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Hiring and Employee Policy | Forced vacation for employees | Will you make employee vacations mandatory? | Disable | - | - | • Productivity<br>• Employee Morale<br>• Internal Security Index |
| | | | Enable | 75,000 | 85,000 | |
| Advisory Subscription and Federal Help | Degree of advisory referral | To what degree does your organization rely on security advisories from the federal government? | None | - | - | Technical Security Index |
| | | | Limited | 30,000 | 150,000 | |
| Advisory Subscription and Federal Help | Reliance on federal government support | To what degree will you rely on federal government support? | None | - | - | • Technical Security Index<br>• Reputation |
| | | | For critical issues only | 300,000 | 170,000 | |
| | | | Ongoing | 400,000 | 250,000 | |
| Training | Training by funding | What is the extent of funding for cybersecurity training? | Minimum | 1,000 | 50,000 | • Internal Security Index<br>• Productivity<br>• Employee Morale |
| | | | Maximum | 2,000 | 100,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|----------|----------|-------------|---------|------------------|--------------------|--------------------|
| Training Incentives | Average compensation bonus as a fraction of technical certification fees | How much will you reimburse employees for technical certification for security training? | 25% of fees | 5,000 | 20,000 | • Technical Security Index<br>• Productivity<br>• Employee Morale |
| | | | 50% of fees | 10,000 | 40,000 | |
| | | | 75% of fees | 15,000 | 60,000 | |
| | | | 100% of fees | 20,000 | 80,000 | |
| Training Incentives | Link training outcomes to promotion | Will you link training outcomes to promotion? | Yes | 10,000 | 10,000 | • Technical Security Index<br>• Productivity<br>• Employee Morale |
| | | | No | - | - | |
| Training Incentives | Link training outcomes to evaluation | Will you link training outcomes to evaluation? | Yes | 15,000 | 7,000 | • Technical Security Index<br>• Productivity<br>• Employee Morale |
| | | | No | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Training and Auditing | Focus on training area: network vulnerabilities | Choose whether to focus your security auditing efforts on network vulnerabilities, controls, encryption, and penetration. | Minimum | - | - | • Technical Security Index <br> • Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Focus on training area: controls | | Minimum | - | - | • Technical Security Index <br> • Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Focus on training area: encryption | | Minimum | - | - | • Technical Security Index <br> • Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Focus on training area: penetration testing | | Minimum | - | - | • Technical Security Index <br> • Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Frequency of physical audits of the equipment | How often will you run physical audits of system equipment? | Every three months | 10,000 | 20,000 | Technical Security Index |
| | | | Every six months | 7,500 | 10,000 | |
| | | | Once a year | 5,000 | 5,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Business Continuity Planning | Degree of IT data storage redundancy | How much redundancy will you build in for IT data storage? | Low | 5,000 | 5,000 | Disaster Readiness |
|  |  |  | Medium | 10,000 | 10,000 |  |
|  |  |  | High | 15,000 | 20,000 |  |
| Business Continuity Planning | Degree of IT network redundancy | How much redundancy will you build in for IT networks? | Low | 7,500 | 20,000 | Disaster Readiness |
|  |  |  | Medium | 12,500 | 30,000 |  |
|  |  |  | High | 20,000 | 50,000 |  |
| Business Continuity Planning | Levels of power backup redundancy | How much redundancy will you build in for power backup? | 1 | 5,000 | 25,000 | Disaster Readiness |
|  |  |  | 2 | 10,000 | 45,000 |  |
|  |  |  | 3 | 15,000 | 67,500 |  |
| Business Continuity Planning | Number of backup sites | How many backup sites will you maintain? | 1 | 5,000 | 75,000 | Disaster Readiness |
|  |  |  | 2 | 10,000 | 150,000 |  |
|  |  |  | 3 | 15,000 | 200,000 |  |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Business Continuity Planning | Number of redundant backup communication links | How many backup communication links will you maintain? | 1 | 5,000 | 10,000 | Disaster Readiness |
| | | | 2 | 10,000 | 17,500 | |
| | | | 3 | 15,000 | 25,000 | |
| Business Continuity Planning | Policy review frequency in months | How often will you review disaster recovery policy? | 3 | - | 100,000 | Disaster Readiness |
| | | | 6 | - | 75,000 | |
| | | | 9 | - | 50,000 | |
| | | | 12 | - | 25,000 | |
| Information Sharing | Degree of information sharing on attacks | To what extent does the organization share cybersecurity attack information publicly? | High - full disclosure | 16,500 | 3,300 | • Profitability • Disaster Readiness |
| | | | Medium - non-sensitive disclosure | 8,800 | 2,200 | |
| | | | Low - no disclosure | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|----------|----------|-------------|---------|------------------|--------------------|--------------------|
| Information Sharing | Degree of non-crisis information sharing | To what extent does the organization share routine cybersecurity information publicly? | High - full disclosure | 16,500 | 3,536 | • Profitability • Disaster Readiness |
| | | | Medium - non-sensitive disclosure | 8,800 | 1,760 | |
| | | | Low - no disclosure | - | - | |
| Public Relations | Spending on public relations | How much will you spend on public relations? | Minimum | 50,000 | 25,000 | Reputation |
| | | | Maximum | 100,000 | 100,000 | |
| Emergency Bypass Policy | Spending on emergency bypass policy | How much will you spend on emergency bypass policy? | Minimum | 5,000 | 1,000 | Disaster Readiness |
| | | | Maximum | 10,000 | 2,000 | |
| Emergency Bypass Policy | Response to violations of typical separation of duties protocol | What is the response to violations of typical Separation of Duties protocol? | Not allowed | 25,000 | 12,500 | • Technical Security Index • Disaster Readiness |
| | | | Permitted with limitations | 15,000 | 20,000 | |
| | | | Allowed | 2,500 | 35,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Emergency Bypass Policy | Violation penalties | What punitive actions will you use for violations of emergency bypass policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Information Sharing Policy | No. of people in groups to overlook and enforce internal information sharing | How many people will you put in groups to overlook and enforce information sharing? | 2 | 17,600 | 12,000 | • Productivity<br>• Technical Security Index<br>• Employee Morale |
| | | | 3 | 33,000 | 22,164 | |
| | | | 4 | 44,000 | 30,000 | |
| | | | 5 | 48,000 | 31,304 | |
| | | | 6 | 50,000 | 30,357 | |
| Information Sharing Policy | Internal information sharing by role-based access control | How restrictive is the system for internal sharing of information? | Strictly need-to-know | 15,000 | 50,000 | • Productivity<br>• Technical Security Index<br>• Employee Morale |
| | | | Limited access | 10,000 | 35,000 | |
| | | | Open system | 1,000 | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Sharing Policy | Degree of external information sharing | How restrictive is the system for external sharing of information? | Strictly need-to-know | 15,000 | 50,000 | • Productivity<br>• Technical Security Index<br>• Customer Satisfaction<br>• Compliance |
| | | | Limited access | 10,000 | 35,000 | |
| | | | Open system | 1,000 | - | |
| Information Sharing Policy | Frequency of disclosure for InfraGard communication in days | How frequently will you share information for the InfraGard service of information sharing between private and public entities? | 7 days | 30,000 | 2,500 | • Contribution to National Security Index<br>• Profitability |
| | | | 14 days | 25,000 | 5,000 | |
| | | | 21 days | 12,500 | 7,500 | |
| | | | 28 days | 10,000 | 10,000 | |
| Information Sharing Policy | Violation penalties | What punitive actions will you use for violations of information sharing policy? | Warnings | - | - | Employee Morale |
| | | | Fines | - | - | |
| | | | Suspensions | - | - | |
| | | | Termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Breach Notification Policy | Degree of openness of breach notification | How open is your organization about breaches that have happened to its systems? | All incidents | 24,000 | 50,000 | • Reputation<br>• Customer Satisfaction<br>• Contribution to National Security Index |
| | | | Critical and significant incidents | 22,000 | 35,000 | |
| | | | Only critical incidents | 16,500 | 20,000 | |
| | | | None of the incidents | 8,800 | 0 | |
| Breach Notification Policy | Investigative agencies to call in for major security breaches | Which investigative agencies will you approach for major security breaches? | Private investigators | 8,800 | 12,571 | • Reputation<br>• Employee Morale<br>• Contribution to National Security Index<br>• Downtime |
| | | | Forensic investigators | 16,500 | 24,750 | |
| | | | CERT | - | - | |
| | | | FBI/NSA | - | - | |
| Breach Notification Policy | Violation penalties | What punitive actions will you use for violations of breach notification policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Privacy Policy | Privacy program investment spending | How much will you spend on your organization's privacy program? | Minimum | 10,000 | 5,000 | • Employee Morale<br>• Customer Satisfaction |
| | | | Maximum | 50,000 | 10,000 | |
| Information Privacy Policy | Appoint a dedicated privacy officer | Will you appoint a dedicated privacy officer? | Yes | 8,800 | 10,560 | • Employee Morale<br>• Customer Satisfaction |
| | | | No | - | - | |
| Information Privacy Policy | Privacy training spending for employees | How much will you spend on training employees on privacy policies? | Minimum | 10,000 | 5,000 | • Employee Morale<br>• Customer Satisfaction |
| | | | Maximum | 40,000 | 10,000 | |
| Information Privacy Policy | Degree of information and record retention | What sort of information will you retain? | Critical information | 25,000 | 20,000 | • Performance<br>• Employee Morale |
| | | | Operational information | 15,000 | 75,000 | |
| | | | All information | 37,500 | 110,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Privacy Policy | Violation penalties | What punitive actions will you use for violations of information privacy policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| General Access Policies | Degree of freedom given to employees regarding communications over the Internet | How free are your employees to communicate over the Internet? | Restricted | 12,500 | 50,000 | • Employee Morale • Productivity |
| | | | Time-limited | 12,500 | 50,000 | |
| | | | Free | - | - | |
| General Access Policies | Degree of freedom over browsing non-business sites | How free are your employees to browse non-business sites? | Restricted | 5,000 | 50,000 | • Employee Morale • Productivity |
| | | | Time-limited | 10,000 | 50,000 | |
| | | | Free | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| General Access Policies | Degree of logging of Internet access and other system actions and accesses | Choose the degree to which Internet access and other system actions and access are logged. | None | - | - | • Internal Security Index • Employee Morale |
| | | | Limited actions | 10,000 | 20,000 | |
| | | | Critical system access only | 25,000 | 75,000 | |
| | | | All actions | 50,000 | 125,000 | |
| General Access Policies | Number of permitted login attempts | Choose the number of permitted login attempts. | 3 | - | - | • Employee Morale • Productivity • Technical Security Index |
| | | | 5 | - | - | |
| | | | 7 | - | - | |
| General Access Policies | Password validity in days | How long will passwords set be valid? | 15 | 20,000 | 30,000 | • Employee Morale • Productivity • Technical Security Index |
| | | | 30 | 20,000 | 15,000 | |
| | | | 45 | 20,000 | 10,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| General Access Policies | Password length requirements | How many characters long should the password be? | 4 | 20,000 | 10,000 | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 6 | 30,000 | 10,000 | |
| | | | 8 | 45,000 | 10,000 | |
| General Access Policies | Non-use of prior passwords | How many prior passwords are set to be invalid for use? | 1 | - | - | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 3 | - | - | |
| | | | 6 | - | - | |
| General Access Policies | Violation penalties | What punitive actions will you use for violations of general access policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Physical Security | Physically isolate rooms containing important infrastructure | Control the degree of physical access to servers. | Free access | 10,000 | - | Technical Security Index |
| | | | Limited access | 25,000 | 20,000 | |
| | | | Restricted access | 30,000 | 15,000 | |
| Physical Security | Restricting physical access through role based access control | Control the degree of physical access to servers through role-based access control. | Free access | 5,000 | - | • Productivity<br>• Disaster Readiness<br>• Technical Security Index |
| | | | Limited access | 12,500 | 2,000 | |
| | | | Restricted access | 15,000 | 15,000 | |
| Physical Security | Degree of access given to visitors | Control the degree and quality of access for visitors. | Free access | 10,000 | - | • Productivity<br>• Technical Security Index |
| | | | Limited access | 20,000 | 10,000 | |
| | | | Accompanied free access | 30,000 | 150,000 | |
| | | | Accompanied limited access | 40,000 | 250,000 | |
| | | | Restricted access | 50,000 | 300,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Physical Security | Violation penalties | What punitive actions will you use for violations of physical security policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Remote Access Policy | Degree of remote access by employee grade | For which employee grades is remote access available? | Executive management only | 10,000 | 2,500 | • Technical Security Index<br>• Productivity |
| | | | Upper management | 15,000 | 7,500 | |
| | | | Middle management | 20,000 | 25,000 | |
| | | | All professional staff members | 35,000 | 100,000 | |
| Remote Access Policy | Access privileges permitted | What are the maximum remote access privileges allowed? | Low - read only | 10,000 | 5,000 | • Technical Security Index<br>• Productivity |
| | | | Medium - read/write | 15,000 | 5,000 | |
| | | | High - read/write/delete | 20,000 | 10,000 | |
| | | | Very high - administrator level | 35,000 | 10,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Remote Access Policy | Violation penalties | What punitive actions will you use for violations of remote access policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Authorized Software Policy | Type of software permitted for use by employees | How lenient are you in terms of software usage? | Freeware | - | - | • Employee Morale<br>• Technical Security Index |
| | | | Games | 20,000 | 30,000 | |
| | | | Open-source | - | - | |
| | | | Approved software | 100,000 | 150,000 | |
| Authorized Software Policy | Software evaluation frequency in months | How frequently will you evaluate systems for presence of unauthorized software? | 6 | 25,000 | 85,000 | • Productivity<br>• Technical Security Index |
| | | | 12 | 35,000 | 50,000 | |
| | | | 18 | 45,000 | 40,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Authorized Software Policy | Violation penalties | What punitive actions will you use for violations of authorized software policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Systems Development Testing | Intensity of quality assurance testing | How intense is your quality assurance testing? | Low | 40,000 | 50,000 | • Employee Morale<br>• Technical Security Index |
| | | | Medium | 60,000 | 150,000 | |
| | | | High | 90,000 | 300,000 | |
| Systems Development Testing | Degree of reliance on external vendor | Choose the degree of reliance on external vendors for systems development testing. | Usability and other minor testing | 10,000 | 50,000 | • Productivity<br>• Technical Security Index |
| | | | Supplementary testing | 20,000 | 100,000 | |
| | | | Comprehensive testing | 30,000 | 200,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Antivirus Policy | Quality of antivirus solution used | Choose the quality of the antivirus solution used across the organization. | Baseline | 30,000 | 50,000 | • Performance<br>• Productivity<br>• Technical Security Index |
| | | | Strong | 50,000 | 100,000 | |
| | | | State-of-the-art | 70,000 | 180,000 | |
| Antivirus Policy | Frequency of scans | How frequently does the antivirus scan run? | Multiple times per day | 24,000 | 28,800 | • Productivity<br>• Technical Security Index |
| | | | Once daily | 22,000 | 33,846 | |
| | | | Once per week | 16,500 | 15,000 | |
| | | | Once per month | 8,800 | 8,800 | |
| Antivirus Policy | Frequency of patch updates | How frequently will you update your antivirus solution with patches? | Always once released | 22,000 | 66,000 | • Productivity<br>• Technical Security Index |
| | | | Only for major and critical updates | 16,500 | 39,286 | |
| | | | Only for critical updates | 8,800 | 18,857 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Insurance Policy | Degree of insurance used against a cyberattack | How high will you prioritize insurance against a cyberattack? | Low | 8,800 | 88,000 | • Disaster Readiness <br> • Compliance |
| | | | Medium | 16,500 | 132,000 | |
| | | | High | 22,000 | 330,000 | |

### 3.5 Mistral Bank

**Table 7: Mistral Bank Decision Reference**

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Authentication | Kerberos servers spending | How much will you spend on Kerberos servers for authentication? | Minimum | 150,000 | 5,000 | • Technical Security Index<br>• Performance<br>• Downtime |
| | | | Maximum | 400,000 | 10,000 | |
| Authentication | Key distribution centers spending | How much will you spend on key distribution centers for authentication? | Minimum | 10,000 | 4,000 | • Technical Security Index<br>• Performance<br>• Downtime |
| | | | Maximum | 25,000 | 8,000 | |
| Backup | RAID levels | What's the RAID level of your server backup? | 0 | 5,000 | 10,000 | • Performance<br>• Compliance<br>• Downtime |
| | | | 1 | 10,000 | 15,000 | |
| | | | 5 | 15,000 | 17,500 | |
| | | | 6 | 17,500 | 20,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Backup | Hot site maintenance spending | Choose your spending on maintaining sites that can serve as full functional sites in case of failure. | Minimum | 200,000 | 25,000 | Downtime |
| | | | Maximum | 400,000 | 125,000 | |
| Backup | Remote backup spending | Choose the amount to spend on remote backup services. | Minimum | 10,000 | 40,000 | • Performance<br>• Downtime<br>• Compliance |
| | | | Maximum | 20,000 | 80,000 | |
| Data Encryption | Level of encryption | What is the average scale of encryption used across the organization? | No encryption | 10,000 | - | • Technical Security Index<br>• Productivity |
| | | | File | 20,000 | 5,000 | |
| | | | Folder | 30,000 | 14,000 | |
| | | | Drive | 35,000 | 25,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Data Encryption | Encryption strength in bits | The strength of encryption you will use; the higher the bit strength, the stronger the encryption. | 32 bits | 10,000 | 10,000 | • Technical Security Index<br>• Performance |
| | | | 64 bits | 20,000 | 15,000 | |
| | | | 128 bits | 25,000 | 20,000 | |
| Load Management | DDOS protection through delayed binding | Delay binding to protect against DDOS attacks. | Disable | - | - | • Technical Security Index<br>• Performance |
| | | | Enable | 30,000 | 25,000 | |
| Load Management | HTTP security through load balancing | Use load balancing to improve security. | Disable | - | - | • Technical Security Index<br>• Performance |
| | | | Enable | 60,000 | 20,000 | |
| Patch Management | Frequency of patch management | Determine the frequency of rolling out updates to systems. | Critical updates only | 10,000 | 10,000 | • Productivity<br>• Performance<br>• Technical Security Index |
| | | | Critical and important updates | 20,000 | 20,000 | |
| | | | All updates | 40,000 | 40,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Patch Management | Degree of patch testing prior to installation | How rigorously will you test patches before installing them? | Low | 10,000 | 5,000 | • Performance<br>• Technical Security Index |
| | | | Medium | 20,000 | 10,000 | |
| | | | High | 40,000 | 15,000 | |
| Patch Management | Trustworthiness of patch | Will you rely only on official patches, or are you willing to use unofficial or community workarounds? | Unofficial | 5,000 | 2,500 | • Downtime<br>• Performance |
| | | | Trusted | 10,000 | 5,000 | |
| | | | Official | 15,000 | 7,500 | |
| Role Based Access Control | Degree of role-based access control | What is the degree of implementation of access control by employee role? | Low | 20,000 | 10,000 | • Technical Security Index<br>• Employee Morale |
| | | | Medium | 30,000 | 20,000 | |
| | | | High | 44,000 | 30,000 | |
| Virtualization OR Cloud Computing | Choose virtualization or cloud computing | Choose virtualization or cloud computing for your systems to improve security. | Virtualization | 10,000 | 5,000 | Technical Security Index |
| | | | Cloud computing | 50,000 | 10,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| If Virtualization Chosen | Degree of virtualization | To what degree will you implement virtualization? | Limited | 2,000 | 10,000 | Technical Security Index |
| | | | Significant | 7,000 | 20,000 | |
| | | | Full | 20,000 | 40,000 | |
| If Virtualization Chosen | Spending on underlying physical network | How much will you spend on the underlying physical network? | Minimum | 10,000 | - | Technical Security Index |
| | | | Maximum | 50,000 | - | |
| If Virtualization Chosen | Degree of isolation of network | How isolated is the network under the virtualization schema? | Minor | 10,000 | 20,000 | • Performance<br>• Technical Security Index |
| | | | Medium | 30,000 | 30,000 | |
| | | | Complete | 60,000 | 50,000 | |
| If Virtualization Chosen | Traffic monitoring on network | Choose the extent of traffic monitoring on the network. | Limited | 10,000 | 5,000 | • Performance<br>• Technical Security Index |
| | | | Significant | 20,000 | 20,000 | |
| | | | Full | 30,000 | 30,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| If Cloud Computing Chosen | Cloud hosting model | Choose the cloud hosting model for your systems. Will you pay more for a more secure private infrastructure or share deployment with other companies for less cost? | Private | 22,000 | 12,571 | • Technical Security Index<br>• Performance |
| | | | Hybrid | 16,500 | 8,250 | |
| | | | Public | 8,800 | 6,600 | |
| If Cloud Computing Chosen | Services offered by the cloud | At what level of engagement will you operate off the cloud? Will you stick with software, or will you go all the way to infrastructure? | Software as a service | 10,000 | 20,000 | • Technical Security Index<br>• Performance |
| | | | Platform as a service | 20,000 | 30,000 | |
| | | | Infrastructure as a service | 40,000 | 60,000 | |
| Firewall | Filtering strictness | How strict is the firewall configured to be? | Low | 5,000 | 5,000 | • Productivity<br>• Technical Security Index<br>• Performance |
| | | | Medium | 10,000 | 7,500 | |
| | | | Medium-high | 12,500 | 10,000 | |
| | | | High | 17,500 | 12,500 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| DNS Redundancy | DNS server redundancy | Enable DNS server redundancy to reduce downtime. | Yes | 10,000 | 15,000 | Downtime |
| | | | No | 5,000 | - | |
| DNS Redundancy | Split DNS topology | Use a split DNS topology to reduce downtime. | Yes | 5,000 | 15,000 | Downtime |
| | | | No | 10,000 | - | |
| Database Security | Frequency of forcing password changes in days | How frequently does the database ask for a change of password? | 15 | 40,000 | 5,000 | • Productivity • Technical Security Index |
| | | | 30 | 30,000 | 5,000 | |
| | | | 60 | 20,000 | 5,000 | |
| | | | 90 | 10,000 | 5,000 | |
| Database Security | Degree of separation of roles for admin and operator roles | Choose to separate admin and operator roles for database systems. | None | 10,000 | - | • Productivity • Technical Security Index |
| | | | Limited | 20,000 | 250,000 | |
| | | | Complete | 30,000 | 350,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|----------|----------|-------------|---------|------------------|--------------------|--------------------| 
| Database Security | Control privileges | Are database control privileges restricted or distributed? | Restricted | 10,000 | 90,000 | • Productivity<br>• Technical Security Index |
| | | | Distributed | 5,000 | 180,000 | |
| Database Security | OS services and associated ports | Will you enable or disable database-related OS services and associated ports? | Disable | - | - | • Productivity<br>• Performance<br>• Technical Security Index |
| | | | Enable | - | - | |
| Database Security | Database honeypots | Will you employ database honeypots to trap and redirect attacks? | Disable | - | - | • Productivity<br>• Technical Security Index |
| | | | Enable | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| IDPS | Type of intrusion detection system to install | Will you employ a network-based IDS, a host-based IDS, or both? | Network-based intrusion detection (NIDS) | 10,000 | 100,000 | Technical Security Index |
| | | | Host-based intrusion detection (HIDS) | 30,000 | 80,000 | |
| | | | Both | 36,000 | 160,000 | |
| IDPS | Class of honeypot to deploy | Will you use a production honeypot or go for a research honeypot with better analytics? | Production honeypot | 20,000 | 90,000 | Technical Security Index |
| | | | Research honeypot | 10,000 | 70,000 | |
| IDPS | Strength of honeypot to deploy | How strong is the honeypot you deploy? | Pure honeypot | 10,000 | 90,000 | Technical Security Index |
| | | | Low interaction honeypot | 20,000 | 60,000 | |
| | | | High interaction honeypot | 30,000 | 90,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Hiring and Employee Policy | IT team size | What strength will you keep your IT teams at, in relation to the industry average? | Less than average | 10,000 | 600,000 | • Productivity<br>• Employee Morale<br>• Technical Security Index |
| | | | Average | 30,000 | 900,000 | |
| | | | More than average | 50,000 | 1,400,000 | |
| Hiring and Employee Policy | Full-time employees as a percentage of the workforce | Will you choose to bolster your IT team with temporary or part-time hires? | All | 8,800 | 4,224 | • Productivity<br>• Employee Morale<br>• Technical Security Index |
| | | | 0.9 | 16,500 | 3,960 | |
| | | | 0.8 | 22,000 | 5,867 | |
| Hiring and Employee Policy | Hiring by average experience in years | What's the average experience you're looking for when you hire for IT teams? | 3 | 8,800 | 12,941 | Internal Security Index |
| | | | 5 | 16,500 | 21,000 | |
| | | | 7 | 22,000 | 26,400 | |
| | | | 8 | 24,000 | 27,429 | |
| | | | 9 | 25,000 | 29,310 | |
| Hiring and Employee Policy | Spending on background check of vendors | How much will you spend on background checks on vendors? | Minimum | 1,000 | 10,000 | • Internal Security Index<br>• Compliance |
| | | | Maximum | 2,000 | 20,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Hiring and Employee Policy | Forced rotation of employees | Will you make employee rotation mandatory? | Disable | - | - | • Productivity<br>• Employee Morale<br>• Internal Security Index |
| | | | Enable | 25,000 | 45,000 | |
| Hiring and Employee Policy | Forced vacation for employees | Will you make employee vacations mandatory? | Disable | - | - | • Productivity<br>• Employee Morale<br>• Internal Security Index |
| | | | Enable | 75,000 | 85,000 | |
| Advisory Subscription and Federal Help | Degree of advisory referral | To what degree does your organization rely on security advisories from the federal government? | None | - | - | Technical Security Index |
| | | | Limited | 30,000 | 150,000 | |
| Advisory Subscription and Federal Help | Reliance on federal government support | To what degree will you rely on federal government support? | None | - | - | • Technical Security Index<br>• Reputation |
| | | | For critical issues only | 300,000 | 170,000 | |
| | | | Ongoing | 400,000 | 250,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Training | Training by funding | What is the extent of funding for cybersecurity training? | Minimum | 1,000 | 50,000 | • Internal Security Index<br>• Productivity<br>• Employee Morale |
| | | | Maximum | 2,000 | 100,000 | |
| Training | Focus on phishing training by target | Choose the focus of phishing training: customers, employees, and both. | Customers only | - | - | Customer Satisfaction |
| | | | Employees only | - | - | |
| | | | Customers and employees | - | - | |
| Training | Focus on phishing training on credit card fraud | Choose the focus of phishing training: customers, employees, and both. | Customers only | 5,000 | 25,000 | Customer Satisfaction |
| | | | Employees only | 7,500 | 100,000 | |
| | | | Customers and employees | 12,000 | 125,000 | |
| Training | Investment training for the fraud investigation team | How much will you invest in training for the fraud investigation team? | Minimum | 3,000 | 75,000 | Customer Satisfaction |
| | | | Maximum | 7,500 | 125,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|----------|----------|-------------|---------|------------------|--------------------|---------------------|
| Training Incentives | Average compensation bonus as a fraction of technical certification fees | How much will you reimburse employees for technical certification for security training? | 25% of fees | 5,000 | 20,000 | • Technical Security Index <br> • Productivity <br> • Employee Morale |
| | | | 50% of fees | 10,000 | 40,000 | |
| | | | 75% of fees | 15,000 | 60,000 | |
| | | | 100% of fees | 20,000 | 80,000 | |
| Training Incentives | Link training outcomes to promotion | Will you link training outcomes to promotion? | Yes | 10,000 | 10,000 | • Technical Security Index <br> • Productivity <br> • Employee Morale |
| | | | No | - | - | |
| Training Incentives | Link training outcomes to evaluation | Will you link training outcomes to evaluation? | Yes | 15,000 | 7,000 | • Technical Security Index <br> • Productivity <br> • Employee Morale |
| | | | No | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|----------|----------|-------------|---------|------------------|--------------------|--------------------|
| Training and Auditing | Focus on training area: network vulnerabilities | Choose whether to focus your security auditing efforts on network vulnerabilities, controls, encryption, and penetration. | Minimum | - | - | • Technical Security Index • Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Focus on training area: controls | | Minimum | - | - | • Technical Security Index • Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Focus on training area: encryption | | Minimum | - | - | • Technical Security Index • Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Focus on training area: penetration testing | | Minimum | - | - | • Technical Security Index • Compliance |
| | | | Maximum | - | - | |
| Training and Auditing | Frequency of physical audits of the equipment | How often will you run physical audits of system equipment? | Every three months | 10,000 | 20,000 | Technical Security Index |
| | | | Every six months | 7,500 | 10,000 | |
| | | | Once a year | 5,000 | 5,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Business Continuity Planning | Degree of IT data storage redundancy | How much redundancy will you build in for IT data storage? | Low | 5,000 | 5,000 | Disaster Readiness |
| | | | Medium | 10,000 | 10,000 | |
| | | | High | 15,000 | 20,000 | |
| Business Continuity Planning | Degree of IT network redundancy | How much redundancy will you build in for IT networks? | Low | 7,500 | 20,000 | Disaster Readiness |
| | | | Medium | 12,500 | 30,000 | |
| | | | High | 20,000 | 50,000 | |
| Business Continuity Planning | Levels of power backup redundancy | How much redundancy will you build in for power backup? | 1 | 5,000 | 25,000 | Disaster Readiness |
| | | | 2 | 10,000 | 45,000 | |
| | | | 3 | 15,000 | 67,500 | |
| Business Continuity Planning | Number of backup sites | How many backup sites will you maintain? | 1 | 5,000 | 75,000 | Disaster Readiness |
| | | | 2 | 10,000 | 150,000 | |
| | | | 3 | 15,000 | 200,000 | |
| Business Continuity Planning | Number of redundant backup communication links | How many backup communication links will you maintain? | 1 | 5,000 | 10,000 | Disaster Readiness |
| | | | 2 | 10,000 | 17,500 | |
| | | | 3 | 15,000 | 25,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Business Continuity Planning | Policy review frequency in months | How often will you review disaster recovery policy? | 3 | - | 100,000 | Disaster Readiness |
| | | | 6 | - | 75,000 | |
| | | | 9 | - | 50,000 | |
| | | | 12 | - | 25,000 | |
| Information Sharing | Degree of information sharing on attacks | To what extent does the organization share cybersecurity attack information publicly? | High - full disclosure | 16,500 | 3,300 | • Profitability • Disaster Readiness |
| | | | Medium - non-sensitive disclosure | 8,800 | 2,200 | |
| | | | Low - no disclosure | - | - | |
| Information Sharing | Degree of non-crisis information sharing | To what extent does the organization share routine cybersecurity information publicly? | High - full disclosure | 16,500 | 3,536 | • Profitability • Disaster Readiness |
| | | | Medium - non-sensitive disclosure | 8,800 | 1,760 | |
| | | | Low - no disclosure | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Public Relations | Spending on public relations | How much will you spend on public relations? | Minimum | 50,000 | 25,000 | Reputation |
| | | | Maximum | 100,000 | 100,000 | |
| Emergency Bypass Policy | Spending on emergency bypass policy | How much will you spend on emergency bypass policy? | Minimum | 5,000 | 1,000 | Disaster Readiness |
| | | | Maximum | 10,000 | 2,000 | |
| Emergency Bypass Policy | Response to violations of typical separation of duties protocol | What is the response to violations of typical Separation of Duties protocol? | Not allowed | 25,000 | 12,500 | • Technical Security Index • Disaster Readiness |
| | | | Permitted with limitations | 15,000 | 20,000 | |
| | | | Allowed | 2,500 | 35,000 | |
| Emergency Bypass Policy | Violation penalties | What punitive actions will you use for violations of emergency bypass policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Sharing Policy | No. of people in groups to overlook and enforce internal information sharing | How many people will you put in groups to overlook and enforce information sharing? | 2 | 17,600 | 12,000 | • Productivity<br>• Technical Security Index<br>• Employee Morale |
| | | | 3 | 33,000 | 22,164 | |
| | | | 4 | 44,000 | 30,000 | |
| | | | 5 | 48,000 | 31,304 | |
| | | | 6 | 50,000 | 30,357 | |
| Information Sharing Policy | Internal information sharing by role-based access control | How restrictive is the system for internal sharing of information? | Strictly need-to-know | 15,000 | 50,000 | • Productivity<br>• Technical Security Index<br>• Employee Morale |
| | | | Limited access | 10,000 | 35,000 | |
| | | | Open system | 1,000 | - | |
| Information Sharing Policy | Degree of external information sharing | How restrictive is the system for external sharing of information? | Strictly need-to-know | 15,000 | 50,000 | • Productivity<br>• Technical Security Index<br>• Customer Satisfaction<br>• Compliance |
| | | | Limited access | 10,000 | 35,000 | |
| | | | Open system | 1,000 | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Sharing Policy | Frequency of disclosure for InfraGard communication in days | How frequently will you share information for the InfraGard service of information sharing between private and public entities? | 7 days | 30,000 | 2,500 | • Contribution to National Security Index<br>• Profitability |
| | | | 14 days | 25,000 | 5,000 | |
| | | | 21 days | 12,500 | 7,500 | |
| | | | 28 days | 10,000 | 10,000 | |
| Information Sharing Policy | Violation penalties | What punitive actions will you use for violations of information sharing policy? | Warnings | - | - | Employee Morale |
| | | | Fines | - | - | |
| | | | Suspensions | - | - | |
| | | | Termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Breach Notification Policy | Degree of openness of breach notification | How open is your organization about breaches that have happened to its systems? | All incidents | 24,000 | 13,200 | • Reputation<br>• Customer Satisfaction<br>• Contribution to National Security Index |
| | | | Critical and significant incidents | 22,000 | 11,000 | |
| | | | Only critical incidents | 16,500 | 10,667 | |
| | | | None of the incidents | 8,800 | 8,800 | |
| Breach Notification Policy | Investigative agencies to call in for major security breaches | Which investigative agencies will you approach for major security breaches? | Private investigators | 8,800 | 12,571 | • Reputation<br>• Employee Morale<br>• Contribution to National Security Index<br>• Downtime |
| | | | Forensic investigators | 16,500 | 24,750 | |
| | | | CERT | - | - | |
| | | | FBI/NSA | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Breach Notification Policy | Violation penalties | What punitive actions will you use for violations of breach notification policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Information Privacy Policy | Privacy program investment spending | How much will you spend on your organization's privacy program? | Minimum | 10,000 | 5,000 | • Employee Morale<br>• Customer Satisfaction |
| | | | Maximum | 50,000 | 10,000 | |
| Information Privacy Policy | Appoint a dedicated privacy officer | Will you appoint a dedicated privacy officer? | Yes | 8,800 | 10,560 | • Employee Morale<br>• Customer Satisfaction |
| | | | No | - | - | |
| Information Privacy Policy | Privacy training spending for employees | How much will you spend on training employees on privacy policies? | Minimum | 10,000 | 5,000 | • Employee Morale<br>• Customer Satisfaction |
| | | | Maximum | 40,000 | 10,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Information Privacy Policy | Degree of information and record retention | What sort of information will you retain? | Critical information | 25,000 | 20,000 | • Performance<br>• Employee Morale |
| | | | Operational information | 15,000 | 75,000 | |
| | | | All information | 37,500 | 110,000 | |
| Information Privacy Policy | Violation penalties | What punitive actions will you use for violations of information privacy policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| General Access Policies | Degree of freedom given to employees regarding communications over the Internet | How free are your employees to communicate over the Internet? | Restricted | 12,500 | 50,000 | • Employee Morale<br>• Productivity |
| | | | Time-limited | 12,500 | 50,000 | |
| | | | Free | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| General Access Policies | Degree of freedom over browsing non-business sites | How free are your employees to browse non-business sites? | Restricted | 5,000 | 50,000 | • Employee Morale<br>• Productivity |
| | | | Time-limited | 10,000 | 50,000 | |
| | | | Free | - | - | |
| General Access Policies | Degree of logging of Internet access and other system actions and accesses | Choose the degree to which Internet access and other system actions and access are logged. | None | - | - | • Internal Security Index<br>• Employee Morale |
| | | | Limited actions | 10,000 | 20,000 | |
| | | | Critical system access only | 25,000 | 75,000 | |
| | | | All actions | 50,000 | 125,000 | |
| General Access Policies | Number of permitted login attempts | Choose the number of permitted login attempts. | 3 | - | - | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 5 | - | - | |
| | | | 7 | - | - | |
| General Access Policies | Password validity in days | How long will passwords set be valid? | 15 | 20,000 | 30,000 | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 30 | 20,000 | 15,000 | |
| | | | 45 | 20,000 | 10,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| General Access Policies | Password length requirements | How many characters long should the password be? | 4 | 20,000 | 10,000 | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 6 | 30,000 | 10,000 | |
| | | | 8 | 45,000 | 10,000 | |
| General Access Policies | Non-use of prior passwords | How many prior passwords are set to be invalid for use? | 1 | - | - | • Employee Morale<br>• Productivity<br>• Technical Security Index |
| | | | 3 | - | - | |
| | | | 6 | - | - | |
| General Access Policies | Violation penalties | What punitive actions will you use for violations of general access policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Physical Security | Physically isolate rooms containing important infrastructure | Control the degree of physical access to servers. | Free access | 10,000 | - | Technical Security Index |
| | | | Limited access | 25,000 | 20,000 | |
| | | | Restricted access | 30,000 | 15,000 | |
| Physical Security | Restricting physical access through role based access control | Control the degree of physical access to servers through role-based access control. | Free access | 5,000 | - | • Productivity<br>• Disaster Readiness<br>• Technical Security Index |
| | | | Limited access | 12,500 | 2,000 | |
| | | | Restricted access | 15,000 | 15,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Physical Security | Degree of access given to visitors | Control the degree and quality of access for visitors. | Free access | 10,000 | - | • Productivity<br>• Technical Security Index |
| | | | Limited access | 20,000 | 10,000 | |
| | | | Accompanied free access | 30,000 | 150,000 | |
| | | | Accompanied limited access | 40,000 | 250,000 | |
| | | | Restricted access | 50,000 | 300,000 | |
| Physical Security | Violation penalties | What punitive actions will you use for violations of physical security policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Remote Access Policy | Degree of remote access by employee grade | For which employee grades is remote access available? | Executive management only | 10,000 | 2,500 | • Technical Security Index<br>• Productivity |
| | | | Upper management | 15,000 | 7,500 | |
| | | | Middle management | 20,000 | 25,000 | |
| | | | All professional staff members | 35,000 | 100,000 | |
| Remote Access Policy | Access privileges permitted | What are the maximum remote access privileges allowed? | Low - read only | 10,000 | 5,000 | • Technical Security Index<br>• Productivity |
| | | | Medium - read/write | 15,000 | 5,000 | |
| | | | High - read/write/delete | 20,000 | 10,000 | |
| | | | Very high - administrator level | 35,000 | 10,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Remote Access Policy | Violation penalties | What punitive actions will you use for violations of remote access policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Authorized Software Policy | Type of software permitted for use by employees | How lenient are you in terms of software usage? | Freeware | - | - | • Employee Morale<br>• Technical Security Index |
| | | | Games | 20,000 | 30,000 | |
| | | | Open-source | - | - | |
| | | | Approved software | 100,000 | 150,000 | |
| Authorized Software Policy | Software evaluation frequency in months | How frequently will you evaluate systems for presence of unauthorized software? | 6 | 25,000 | 85,000 | • Productivity<br>• Technical Security Index |
| | | | 12 | 35,000 | 50,000 | |
| | | | 18 | 45,000 | 40,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Authorized Software Policy | Violation penalties | What punitive actions will you use for violations of authorized software policy? | Focus on warnings | - | - | Employee Morale |
| | | | Focus on fines | - | - | |
| | | | Focus on suspensions | - | - | |
| | | | Focus on termination | - | - | |
| Systems Development Testing | Intensity of quality assurance testing | How intense is your quality assurance testing? | Low | 40,000 | 50,000 | • Employee Morale • Technical Security Index |
| | | | Medium | 60,000 | 150,000 | |
| | | | High | 90,000 | 300,000 | |
| Systems Development Testing | Degree of reliance on external vendor | Choose the degree of reliance on external vendors for systems development testing. | Usability and other minor testing | 10,000 | 50,000 | • Productivity • Technical Security Index |
| | | | Supplementary testing | 20,000 | 100,000 | |
| | | | Comprehensive testing | 30,000 | 200,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Antivirus Policy | Quality of antivirus solution used | Choose the quality of the antivirus solution used across the organization. | Baseline | 30,000 | 50,000 | • Performance<br>• Productivity<br>• Technical Security Index |
| | | | Strong | 50,000 | 100,000 | |
| | | | State-of-the-art | 70,000 | 180,000 | |
| Antivirus Policy | Frequency of scans | How frequently does the antivirus scan run? | Multiple times per day | 24,000 | 28,800 | • Productivity<br>• Technical Security Index |
| | | | Once daily | 22,000 | 33,846 | |
| | | | Once per week | 16,500 | 15,000 | |
| | | | Once per month | 8,800 | 8,800 | |
| Antivirus Policy | Frequency of patch updates | How frequently will you update your antivirus solution with patches? | Always once released | 24,000 | 72,000 | • Productivity<br>• Technical Security Index |
| | | | Only for major and critical updates | 22,000 | 52,381 | |
| | | | Only for critical updates | 16,500 | 35,357 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| SOX and GLBA | Degree of control in identity provisioning | Choose the degree of control in identity provisioning. | None | - | - | • Technical Security Index<br>• Compliance |
| | | | Limited | 15,000 | 14,000 | |
| | | | Complete | 30,000 | 18,000 | |
| SOX and GLBA | Degree of customer-end SSO implementation | Choose the degree of customer-end SSO implementation. | None | - | - | • Customer Satisfaction<br>• Performance<br>• Technical Security Index |
| | | | Limited | 25,000 | 70,000 | |
| | | | Complete | 50,000 | 90,000 | |
| SOX and GLBA | SOX training and compliance spending | Choose the spending on SOX training and compliance. | Minimum | 200,000 | 75,000 | • Technical Security Index<br>• Compliance |
| | | | Maximum | 400,000 | 150,000 | |
| SOX and GLBA | Quality of third-party service providers for credit card and check processing | Choose the quality grade of third-party service providers for credit card and check processing. | Grade B | 17,600 | 3,520 | • Technical Security Index<br>• Compliance<br>• Customer Satisfaction |
| | | | Grade B+ | 33,000 | 7,920 | |
| | | | Grade A | 44,000 | 14,667 | |
| | | | Grade A+ | 48,000 | 16,000 | |

| Category | Decision | Explanation | Options | Capital Cost ($) | Operating Cost ($) | Indicators Affected |
|---|---|---|---|---|---|---|
| Financial Security Measures | Frequency of credit card usage security alerts | How frequently are credit card usage security alerts issued? | Low | 50,000 | 15,000 | Customer Satisfaction |
| | | | Medium | 75,000 | 25,000 | |
| | | | High | 90,000 | 35,000 | |
| Financial Security Measures | Mode of reception | What is the mode of reception for credit card usage security alerts? | E-mail | 25,000 | 10,000 | Customer Satisfaction |
| | | | SMS | 75,000 | 12,000 | |
| | | | Phone call | 150,000 | 15,000 | |
| Financial Security Measures | Security questions rigor | How rigorous are the security questions requirements? | Low | 5,000 | 20,000 | Customer Satisfaction |
| | | | Medium | 7,500 | 27,500 | |
| | | | High | 10,000 | 32,500 | |
| Financial Security Measures | Account lockout procedure rigor | How rigorous is the account lockout procedure? | Low | 5,000 | 10,000 | Customer Satisfaction |
| | | | Medium | 10,000 | 12,000 | |
| | | | High | 15,000 | 15,000 | |
| Insurance Policy | Degree of insurance used against a cyberattack | How high will you prioritize insurance against a cyberattack? | Low | 8,800 | 88,000 | • Disaster Readiness • Compliance |
| | | | Medium | 16,500 | 132,000 | |
| | | | High | 22,000 | 330,000 | |

# 4. Indicator Reference

The indicators are either indices or numeric values. Indices will be kept in the range of 0 to 200. Indices are best for teams when they are high in value (> 100) and vice versa. However, the Downtime and Disaster Damage indices are an exception, with higher values being detrimental to performance.

Financial indicators like Budget and Revenues will be numeric values in dollars. The table below details the different indicators used and how they relate to each other.

**Table 8: Indicator Reference**

| Indicator | Description |
|---|---|
| Budget (Budget Allocated) | This is the budget allocated to a particular team. The budget is used up based on the decisions the user chooses. Budget is measured in dollars. |
| Compliance Index | This is a measure of compliance attained by a particular team with respect to various security policies applicable to that team. Compliance is measured as an index on a scale of 200. |
| Contribution to National Security Index | This indicator is the measure of the effect on National Security Index by a particular team's decisions, derived from the team's Security Index. The Contribution to National Security Index of all the teams is averaged to arrive at a single National Security Index. |
| Customer Satisfaction Index | This is a measure of how satisfied the customers of a particular team are. Customer satisfaction is measured as an index which is on a scale of 200. |
| Disaster Damage Index | Whenever there is a disaster at a national level we measure the damage caused to the organization using this indicator. Disaster Damage is an index measured on a scale of 200. |

| Indicator | Description |
|---|---|
| Disaster Readiness Index | This indicator explains the readiness of a particular team in controlling the effects of a disaster. This indicator is measured as an index on a scale of 200. |
| Downtime Index | This indicator is the annual downtime percentage, relating to the particular service the organization offers. This indicator is measured as an index on a scale of 200. |
| Economic Health Index | This indicator is a national level indicator of the economic status of the U.S. This indicator is measured as an index on a scale of 200. |
| Employee Morale Index | This indicator explains the level of employee morale in the organization. This indicator is measured as an index on a scale of 200. |
| Insurance Payout Index | This is the insurance payout to the organization when downtime occurs, measured in dollars. A fraction of this is added to the budget for the next round. |
| Internal Security Index | This indicator explains the state of a company's security index from the internal policy aspect. This indicator is measured as an index on a scale of 200. |
| International Policy Burden Index | This is the 'policy burden' the U.S. incurs when it co-operates with other countries on cybersecurity. |
| National Security Index | This indicator tells us the degree of security at the national level. This is a weighted average of the "contribution to national security" indices of various teams in the country. This indicator is measured as an index on a scale of 200. It is a shared, global indicator; all teams will have the same value of National Security Index in each round, but have a different Contribution to National Security Index. |
| Network Load Index | This measures the amount of load on the network during the duration of a round. This indicator is measured as an index on a scale of 200. |
| No. of Customers Index | This indicator represents the number of customers of the respective teams. |
| Performance | This indicator represents the system performance of a particular team. This indicator is measured as an index on a scale of 200. |

| Indicator | Description |
|---|---|
| Popular Sentiment Index | The indicator of how the people in the U.S. feel: confidence vs. panic. |
| Productivity Index | This relates to the employee productivity. This indicator is measured as an index on a scale of 200. |
| Profitability Index | An index of how profitable a company or agency is, on a scale of 200. For the federal government team, this represents the surplus. |
| Reputation Index | A measure of the market reputation of a particular team. This indicator is measured as an index on a scale of 200. |
| Revenues | The revenues earned by the company (team) at the end of a particular round. Revenues are measured in dollars. |
| Security Index | This represents the level of security in a particular team.  This relates to the security status of a particular team. This indicator is measured as an index on a scale of 200. It is derived from Internal Security Index and Technical Security Index. |
| System Health Index | This is a measure of the condition of systems of a particular team. The delay effects involved in the relationships help capture the phenomenon of recovery over time. This indicator is measured as an index on a scale of 200. |
| System Recovery Index | This measures the degree to which systems recover from a state of disaster or attack from the outside world per round. Measured as an index on a scale of 200. |
| System Resiliency Index | This affects the rate of recovery of the system. This indicator is measured as an index on a scale of 200. |
| Technical Security Index | A security index for the organization stemming only from technical measures. This indicator is measured as an index on a scale of 200. |

# 5. Cross-Team Module

This section details how the CCS computes and applies cross-team effects.

The essence of the cross-team module is that the changes in the key indicators of each team impact the indicators of the other teams. This replicates real-world scenarios where different entities are linked through their performance on key individual metrics.
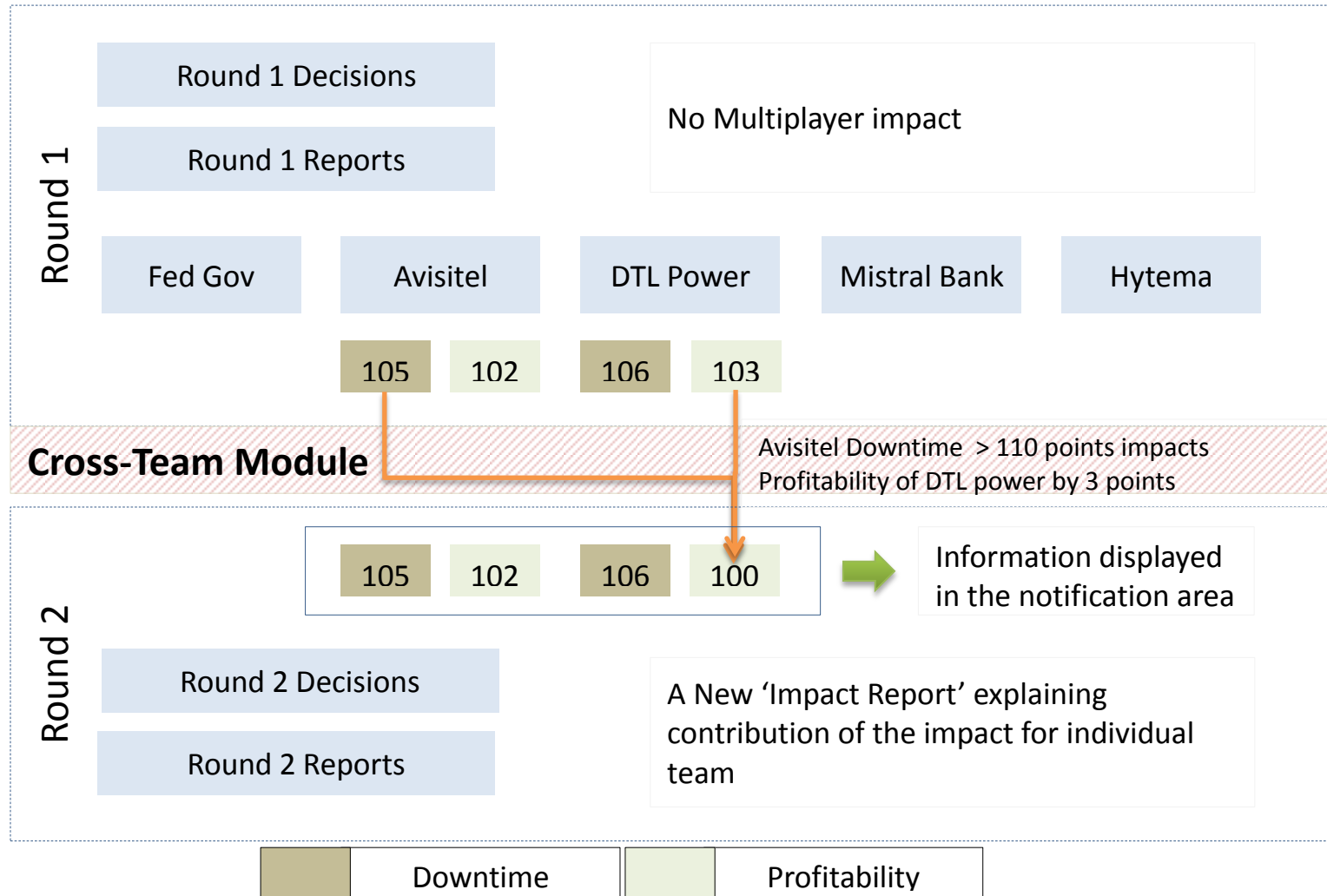
**5.1 Flow and Architecture**



**Figure 1: Cross-Team Module**

The flow of the cross-team effects is detailed above.

At the end of the first round, there is no effect from the cross-team effects on the indicator values shown for each team, it being the first round.

Prior to the start of the second round, however, the values of the indicators are compared to certain benchmarks, and if the benchmarks are broken, the cross-team module will cause some changes to certain indicators of the teams for the second round. In our example above, Avisitel's Downtime crosses the 110 threshold in Round 1 and reduces the Profitability of DTL Power by 3 points.

The resulting impacts are available in the impact report in the application.

Keep in mind that these impacts will add on to the decisions made in Round 2. Therefore, in the situation above, DTL Power starts 'behind' on Profitability in Round 2 by 3 points. If it makes decisions that improve its Profitability, it can overcome this deficit.

Also remember that the cross-team module operates at the end of each round (except for the last round). So if Avisitel's Downtime were to stay above 110 for every round till the end, ***the teams would get their Profitability affected similarly in every round***, not just the first time the indicator crossed 110.

# 6. Other Calculations

In this section we detail any calculation procedures that are not related to the model directly.

## 6.1 Cost Considerations

Each decision in the CCS has costs associated with it, as detailed in Section 3 of this document.

The costs are:

- **Capital costs**; these costs are applied only when there is a change in the decision setting from the previous round in the current round.

- **Operating costs**; these costs are applied every round whether the decision setting changes or remains the same.

For some decisions that are sliders instead of drop-downs, note that the values displayed on the slider are the capital costs alone. Therefore, increasing or decreasing the slider will also change the operating costs involved in direct proportion based on the ranges provided in the reference tables. *Consequently, the change in the actual budgets will not match the change in the slider, because the budget must also take into account the operating cost change because of your decision.*

Therefore, in each round, the CCS calculates the total cost as follows:

**Total Cost** = **Capital Cost** for all team members + **Operating Cost** for all team members

This total cost then gets used in two ways:

- It is subtracted from the **Budget Allocated** to obtain **Budget Used**.

- It is subtracted from the **Revenues**, thus indirectly affecting **Profitability**. So the higher the costs of the team, the lower its profitability. Because **Profitability** affects **Budget Allocated**, this also causes the next round budget allocation to decrease.

## 6.2 Budget Calculations

**Budget** is an indicator that is affected by other indicators in the model, but unlike other indicators, it is also linked directly to your decisions of the students through the costs of those decisions.

There are four budgetary values: **Budget Allocated**, **Budget Used**, **Budget Left**, and **Overdraft**. Note that the last three are shown on the screen. The relationships between these are as follows:

- **Budget Allocated** is the constant budget set by the game master at simulation creation for the whole team. This is actually the **Budget** used in the model.

- **Budget Used** indicates the actual budget used by the whole team. It is derived from the costs that have been set for the decisions. For each decision, the CCS sums up the cost corresponding to each decision (as described in **Section 3** of this document), and calculates the total budget usage across the team.

- **Budget Left** is simply derived as: **Budget Left = Budget – Budget Used**. *It does not carry over into the next round.*

- **Overdraft** is an additional budget that is fixed at 10 percent of the **Budget Allocated** to you.

The **Budget Allocated** round to round for a team changes somewhat based on the team's collective decisions. Factors that affect budgeting include:

- **Profitability:** If the profitability of a team exceeds 100 in a round, it increases the budget allocated in the next round, and if it drops below 100, it decreases the budget allocated in the next round. This is a lag effect, as shown in the causal loop diagram.

- **Insurance Payout:** If a team's downtime exceeds 100, the net insurance payout (after adjustment for premium) is a positive contribution that adds to the budget allocated for the second succeeding round. If a team's downtime drops below 100, the net insurance payout goes negative and is hence deducted from the budget allocated from the second succeeding round.

### 6.3 National Security Index Calculation

The National Security Index is an indicator that is shared across all teams, yet derives its value from the respective contributions made by the five teams towards their respective Security Indices. The Federal Government, given its national role, has decision categories that affect National Security Index directly as well.

From the Security Index of each team we derive their contribution to the National Security Index, and then we average these numbers to arrive at a single common National Security Index.

# 7. Glossary

This section details frequently used terms of the CCS.

**Table 9: Glossary of CCS Terminology**

| Term | Description |
|------|-------------|
| Budget | An allotted amount of funds available for an organization (e.g., DTL Power) to spend within a single year (i.e., a round within the simulation game). An organization's annual budget may vary from year to year, depending on that organization's decisions and annual performance indicators (i.e., round outcomes).<br><br>Budget surpluses in one year are not carried forward to the next year (i.e., round).<br><br>A budget overdraft will become available if an organization overspends its budget for the year.<br><br>The Cybersecurity Capstone Simulation uses the terms *budget* and *allocated budget* synonymously. |
| CCS | The Cybersecurity Capstone Simulation. |
| Decision | A virtual lever that you use to respond to the events within the game world, and create outcomes that improve the state of the virtual USA. Decisions are chosen by students at the outset and are restricted accordingly in the actual simulation play period. |
| Economic Downturn | A situation in which the national economy suffers due to one or more of the following macroeconomic factors: increased inflation, increased unemployment, decreased gross domestic product (GDP), lower stock market indexes, a decrease in foreign currency exchange rates for the U.S. dollar, a lack of consumer spending, or other related factors. |
| Economic Upturn | A situation in which the national economy improves and is strengthened. This can be attributed to one or more of the following macroeconomic factors: increased employment, higher gross domestic product (GDP), higher stock market indexes, a stronger U.S. dollar in relation to other major currencies, decreased inflation, decreased interest rates, or lower national debt. |
| Events | Scenarios or occurrences resembling real life that are injected by the game master into simulation rounds, such as worm and virus attacks, and natural disasters like floods. Students see events in terms of media items within the simulation. |

| Term | Description |
|---|---|
| Game Master | The administrative role in charge of the CCS as a whole, with ultimate privileges in terms of controlling the simulation. |
| Indicator | An index that the simulation uses to show the user the state of the virtual nation in the simulation. |
| Media Inputs/Items | Fictitious media inputs resembling real-life news notifications that are supplied to students between rounds. These may warn students of upcoming events, and detail outcomes of the events of past rounds. |
| Outcome | The state of the simulation after an event has occurred. Events can create multiple outcomes for a given round, which the simulation integrates to arrive at a final simulation state for that round. Students see outcomes in terms of their effects: a successful worm intrusion creates downtime as an outcome. Media items are also linked to these outcomes, as well as internal notifications. |
| Overdraft | A budget addition that is provided to an organization (e.g., Avisitel) when it has spent its entire allocated budget within a single year (i.e., a round within the simulation). Therefore, an overdraft enables the organization to continue considering critical decisions that might require additional funds after a budget overrun.<br><br>The organization will receive an overdraft that is 10 percent of its allocated budget for that particular year. However, the organization is not required to spend the overdraft.<br><br>An organization that uses an overdraft will have its profitability reduced for the current year, which will in turn reduce its budget for the following year. |
| Round | A decision-making cycle representing a single year. A discrete set of choices that is isolated in time, but not necessarily in terms of impact, from other such cycles. |
| Section | The virtual class. The student body will be divided into sections internally by UMUC. |