Lamar Roulhac

Risk Assessment

EXAMPLE 1

Background

Risk assessment is an important part of cybersecurity and recovery planning. As an organization it's important to evaluate potential financial impacts due to equipment being lost and have plans for what to do when that occurs.

First, I identified all assets in the school network that require replacement in case of a disaster, I then researched and estimated the replacement costs for each item. Used that information to determine the overall replacement cost for all the assets. i then put all of the assets and their cost on a graph to show what the budget was going to and used the information I have to figure out the cost necessary for replacing lab equipment.

The school network assets:

- **20 Workstations** (Precision 7820 Tower Workstations, Intel Xeon Silver 4112 2.6GHz, Windows 10 Pro, Radeon Pro WX 2100, 32GB RAM, 1TB HDD) - **$1,350 each ($27,000 total)**
- **28 Monitors** (Dell 27 Monitor, model P2719H) - **$230 each ($6,440 total)**
- **10 External SSD Drives** (1TB each) - **$100 each (1,000 total)**
- **3 HP Printers** (1 HP Color LaserJet Enterprise Flow MFP M681f - **$2,300**, 2 inkjet - **$450 each (3,200 total)**
- **1 Wireless Router** (Netgear Nighthawk) - **$200**
- **2 Solution Servers** (HPE ProLiant DL385 Gen10 7351 1P 32GB-R P408i-a 8SFF 800W PS) - **$3,650 each (7,300 total)**

Cost Calculations and Graphs

Total estimated replacement cost: $49,450

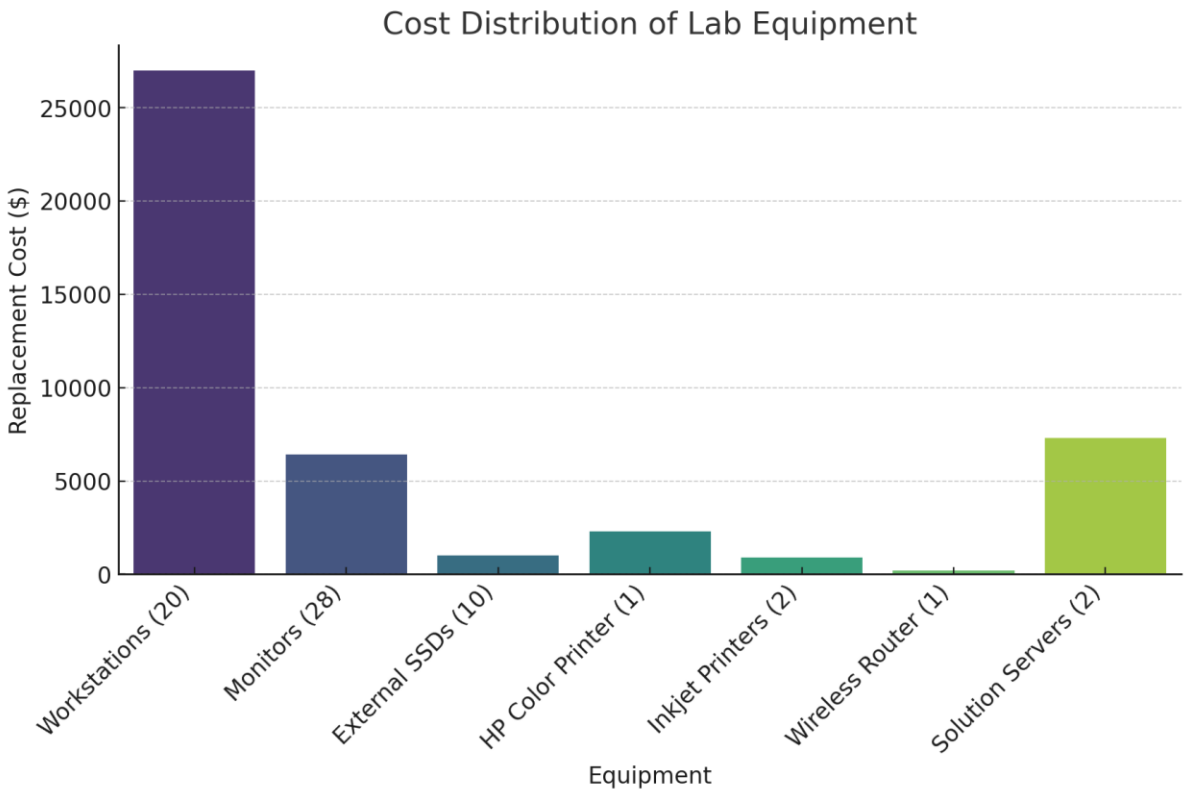

Figure 1: Cost Distribution Graph

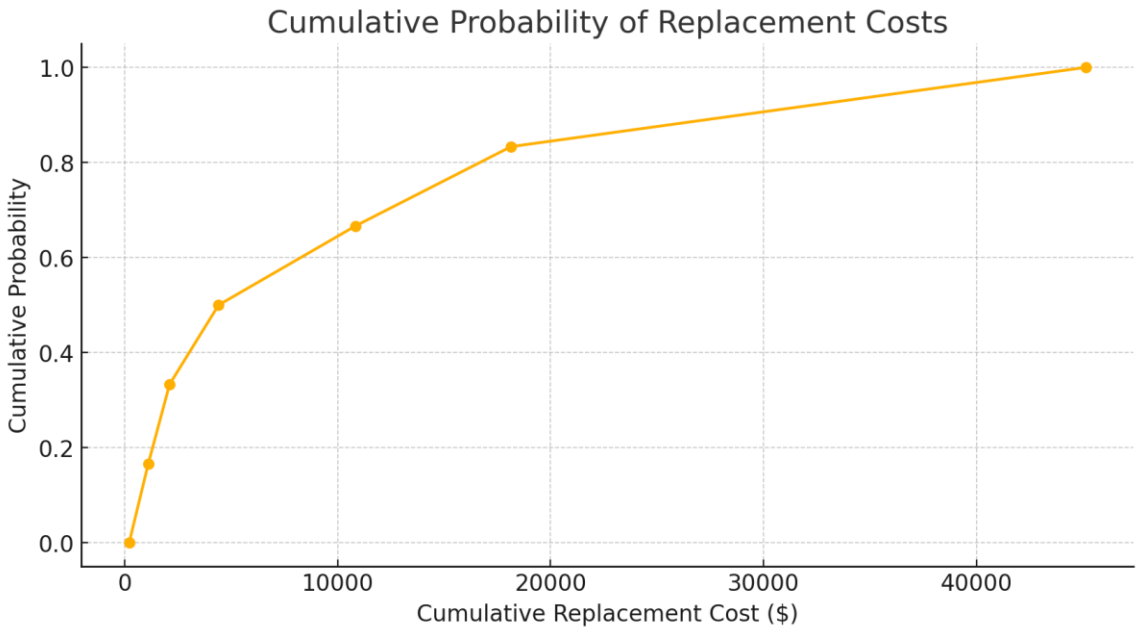

Figure 2: Cumulative Probability Graph

Based on the graphs and information certain equipment, such as servers and workstations, made up a big portion of the overall budget, this makes them high-priority assets for contingency planning due to their high cost.

EXAMPLE 2

Background

Security policies are the foundation for protecting business and customer information. In financial institutions, policies must work with industry regulations to prevent unauthorized access, data breaches, or legal repercussions. This task is about a New York financial service business that had an unauthorized transfer of 4,000 customer records when a trader left for a competing company.

Procedure

With this situation ways you can strengthen the company's security policy would be with:

-Access Controls: Limit who can access sensitive client data such as implementing role-based access controls

-Offboarding Procedures: Immediately revoke access when employees leave to prevent another breach of data

-Data Loss Prevention: Use monitoring tools to prevent unauthorized data transfers.

-Incident Response: Investigate and report any future potential data breaches to reduce loss.

Policy Recommendation

When an employee leaves the company, all access to data will be immediately revoked and a security audit will be done to ensure no data was stolen. Any unauthorized transfer of information will be considered a data breach, and it will be reported as required by GLBA and NYDFS regulations and violations will result in legal action and regulatory penalties.