*Chad Ballay*

*Spring 2020 | Bellevue University CIS312*

*Integrated Distributors Incorporated*

Modernization and Security Proposal

Table of Contents

[Background 2](#_Toc37470929)

[Overview of IDI 2](#_Toc37470930)

[Scope 2](#_Toc37470931)

[Disclosed Challenges 2](#_Toc37470932)

# Background

## 

## Overview of IDI

Integrated Distributors Incorporated(IDI) is a logistics company focusing on B2B logistics at the manufactur and distributor level of the supply chain. Corporate offices are in Billings, Montana with a workforce presence of 600 employees. Worldwide presences are represented:

* Sao Paulo, Brazil, 580 employees
* Warsaw, Poland, 975 employees
* Sydney, Australia, 340 employees
* Tanzania, Africa, 675 employees
* Japan, China, and Hong Kong, 700 employees

Client base is focused on large retailers, federal governments and large state governments. Primary business focus is fleet trucking and secondary focus is subcontracting the forwarding, storage, and delivery aspects of the business.

## 

## Scope

IDI’s heterogenous and aging IT infrastructure has limited their responsiveness to changing market dynamics. As a benefit to standardizing and updating this infrastructure a secondary objective is to increase the security posture against further security breaches. The tertiary goal is to implement efficiencies into the operations to capitalize on cost savings and profit margin growth.

## Disclosed Challenges

* Localization required to drive adoption of initiative.
* Cultural awareness required.
* Budgetary constraints around depreciation of IT assets.
* Existing policies will require contextual understanding.
* 10-15% future growth to be accounted for over next 7 years.
* Joint Ventures and Strategic Alliances are not in scope.
* Previous security breaches have occurred.

# Site Survey

## Billings, Montana

Inventory of the server infrastructure reveals that several core functionalities are compromised by legacy OS and inconsistent patching. For HP-UX servers we found several major versions of the OS was present with the majority of them already at End-Of-Life(EOL) levels of age. We also found that Windows servers did not fare any better. The majority were Windows 2003. Key business functionalities are at risk. Logisuite, the third party logistics software, is running on a 10 year old version that has been heavily localized from the standard installation. RouteSim is not integrated into Logisuite, which means that the simulation of routes, costs, and profits will have inefficiencies.

The individual user procurement process for hardware is no better. Office productivity tools are not consistent across business areas. Desktop/laptop procurement policy is lacking. This has led to an environment of only moving as fast as the slowest path in the graph.

Telecommunications and network are another area of concern. The WAN capacity has reached threshold and during peak traffic has impacted business functionality. The antiquated telecommunications is no longer supported and is missing several key items of functionality.

Finally, the bring your own device(BYOD) policy is being ignored by management. This is concerning on multiple fronts. By having policies in place that are overridden by management it sends the message that the culture is by fiat instead of by core ideals.

## Sao Paulo, Brazil

The area of concern here is the communications infrastructure. The local vendor has no contractual SLA’s and their techs are undertrained and overallocated. The connection to the headquarters is through a VPN with a single shared credential by all employees. This credential is a 6-character password. There is anecdotal concern that elevation of user credentials is informal, and no policy enforcement and audit is in place. Finally, the lack of antivirus or malware protection will need to be addressed.

IT infrastructure and user procurement is remarkedly better here. Several best practices have been identified around standardization and compartmentalization. The mapping of their site-specific process should be fast tracked to see if aspects can be socialized to the other locations.

## Warsaw, Poland

A business-critical pain point is the lack of headroom from the IT compute capacity. This has impacted production and revenue expectations and will require remedy. The telecommunications infrastructure here is a pain point due to being EOL.

Financial irregularities point to a critical gap in the feedback loop for auditing. The employee relation policy as well as the job duty assessments for several key employees should be reviewed with HR.

Points of minor concern do exist around protecting the employee access to a third party public wifi. In addition the separate enclave for JV and SA partners does segregate them which is good. The lack of monitoring though is troublesome.

# Initial Recommendations

## Modernization and Security Technical Debt

* Robust CMDB for inventory adopted.
* Implement an enterprise census of network, server, applications.
* Patch automation to be implemented.
* EOL infrastructure remediation plan.

## Application Standardization

* Individual site adoption of Office365 and other collaboration tools.
* Logisuite/RouteSIM updates to be prioritized to further allow integration.
* Standard localization policy implemented so as to reduce the duplication of documentation.

## Infrastructure Standardization

* SAS solution replacements to be implemented at the global level.
* A cloud first strategy to be the focus d
* Localization has been abused