*Chad Ballay*

*Spring 2020 | Bellevue University CIS312*

*Integrated Distributors Incorporated*

Modernization and Security Proposal

Table of Contents

[Background 2](#_Toc37475477)

[Overview of IDI 2](#_Toc37475478)

[Scope 2](#_Toc37475479)

[Disclosed Challenges 2](#_Toc37475480)

[Site Survey 3](#_Toc37475481)

[Billings, Montana 3](#_Toc37475482)

[Sao Paulo, Brazil 3](#_Toc37475483)

[Warsaw, Poland 3](#_Toc37475484)

[Initial Recommendations 5](#_Toc37475485)

[Modernization and Security Technical Debt 5](#_Toc37475486)

[Application Standardization 5](#_Toc37475487)

[Infrastructure Standardization 5](#_Toc37475488)

[Core Business Functionalities 5](#_Toc37475489)

[Telecommunication Infrastructure Update. 5](#_Toc37475490)

[Internal Controls and Audits 5](#_Toc37475491)

[Implementation Recommendations 6](#_Toc37475492)

# Background

## Overview of IDI

Integrated Distributors Incorporated(IDI) is a logistics company focusing on B2B logistics at the manufacture 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. This in addition to the inherent data breach concerns.

## 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.

## Sydney, Australia

The recent wildfire disaster has caused a large but temporary upheaval to the region covered by the Australian site. The ongoing political tensions and COVID-19 outbreak will be of longer consequences but can be manageable due to relative distance for day to day operations. The dateline/timezone difference from the workday hours of the Billings home office creates a day lag of execution in places of ambiguity or where a lack of autonomy is felt.

We are expecting a higher than projected growth at this site in compute and capacity needs. The network backbones serving Australia are seeing saturation as is and is already driving peering costs higher.

## Tanzania, Africa

Sub-Saharan Africa is chronically underserved for cloud computing capacity so we view that the current compute and network capacity as lacking. This has also been identified by the network bandwidth usage of personal devices. This network access is viewed as an employment benfit by many in the region. The security posture for the local network with regard to firewalls, antivirus, and malware is lacking due to the inherent tension created here.

The global view of corruption and it’s impact on financial efficiency will need to be addressed. Special consideration is needed to reassure the global marketplace even when corruption is not a problem due to the perception that it is endemic in the region. No accusations were noted in the report but the perception still remains.

## Pacific Rim – Japan, China, Hong Kong

The global pandemic of COVID-19 has especially decimated the local workforce and economy. This has led to turnover in the workforce as well as vendors and suppliers. The onboarding process should be restructured to allow for speedier turnaround. As with the Australian site, the timezone delay has impacted the speed and the autonomy exercised with regard to directions from the Billings home office.

Asiatic language character sets are traditional underserved with software localization. Upgrades will be delayed here unless acceptance testing is focused to remediate this during the process.

# Initial Recommendations

## Modernization and Security Technical Debt

* Robust CMDB for inventory adopted. (CMDB Design Guidance, n.d.)
* Implement an enterprise census of network, server, applications.
* Patch automation to be implemented.
* EOL infrastructure remediation plan.
* Cloud first strategy to be adopted as a default position except in Australia and Africa until they become better served.

## Application Standardization

* Individual site adoption of Office365 and other collaboration tools. (Koenigsbauer, n.d.)
* Collaboration tools to be updated to provide consistent employee usage.
* Standard localization policy implemented so as to reduce the duplication of documentation.
* Focus on localization acceptance testing to be done by each branch to better ensure that business impact does not delay adoption.

## Infrastructure Standardization

* SAS solution replacements to be implemented at the global level.
* A cloud first strategy to be the focus to leverage elasticity to meet business needs. (Cloud Computing Use Cases, n.d.)
* For Africa and Australia, on premise standardization of resources should be coordinated to capture some economy of scale.
* User hardware procurement to shifted to site specific standardization at a minimum.

## Core Business Functionalities

* Core business functionality not enumerated clearly.
* Australia and Pacific Rim sites will need business process and IT process autonomy to reduce turnaround time of rollout adoption.
* Logisuite and RouteSim integrations and upgrades to be prioritized.
* Business continuity plans to be developed to classify the existing risks and guide implementation of all recommendations. (Business continuity and resiliency services from IBM, n.d.)

## Telecommunication Infrastructure Update.

* PBX modernization
* WAN modernization
* All sites to have separate employee public WiFi networks audited for capacity. Focus on Africa and Polish sites due to identified usage patterns.
* Enterprise wide adoption of firewall hardening and increased network monitoring to be done at all sites.

## Internal Controls and Audits

* Financial Audit and process review needed.
* Separation of Roles and Responsibilities as well as other familial policy review.
* Africa site will have greater financial overview communicated outwardly to help focus their buy in on roadmap.

# Implementation Recommendations

A site by site approach should be adopted rather than a global wide approach. This will allow for best practices to be developed and efficiently reused. If capacity exists, smaller projects can be spun up or spun off for implementation. We also recommend the Sydney, Australia site as the first candidate to be selected. The overlap in business day hours will allow for minimal impact to employee work/life balance. The overlap is also offset enough so that off hour updates can be ran out of the home office with minimal impact to employee work/life balance.

Due to the early start and positioning of Sydney in the project timeline, a suitable multi person home should be leased now. This will help ease the employee impact of a lengthy duration of in country stays for the project duration. Building the expertise is critical and employee turnover is a key roadblock to prevent.

A weekly cadence of email or PowerPoint only project updates should be owned by the project manager(s) with the target audience being the VP level. This should help cross functional teams be spun up and aligned quickly. A quarterly all hands meeting of the effort should be shared with the company at large. A targeted Board of Directors specific review should be performed no more than every three months. This meeting should align with the financial quarters to ensure that funding is adequately tied to milestones.

# Bibliography

*Business continuity and resiliency services from IBM*. (n.d.). Retrieved from Continuity Forum: http://www.continuityforum.org/sites/default/files/images/BUW03007USEN\_HR.pdf

*Cloud Computing Use Cases*. (n.d.). Retrieved from Cloud-Council: http://www.cloud-council.org/Cloud\_Computing\_Use\_Cases\_Whitepaper-4\_0.pdf

*CMDB Design Guidance*. (n.d.). Retrieved from ServiceNow: https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/white-paper/wp-cmdb-design-guidance.pdf

Koenigsbauer, K. (n.d.). *Harvard Business Review - The Workplace Evolution*. Retrieved from Microsoft: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE23w1o