Battling Breach Fatigue: The End is Not in Sight?

10 Data Center Migration Red Flags and How to Avoid Them
Future Direction and New Leadership

By: Jim Bradley, Chair, Technology First Board of Directors

As the new Chair for the Board of Directors of Technology First, I would like to introduce and welcome, Marcia Albers as the new Executive Director of the organization. Marcia steps into the leadership role that has been held by Ann Gallaher for the last fourteen years. Ann announced that she would be retiring at the end of 2016, having provided dedicated leadership throughout her tenure that has resulted in the consistent growth and financial stability of the organization. I also wish to extend my sincere appreciation for all Ann has done and best wishes for a long and rewarding retirement.

In my seven years with Technology First, I have seen growth, stability and many improvements. We have continued to set the bar higher each year and have predominantly exceeded our goals. My journey began as a member very active with the CIO Council and I participated on a CIO Forecast Panel. I then became Chair of the Events Committee and revived the Data Analytics (Business Intelligence) Special Interest Group. I was invited to become a member of the Board of Directors, was then Vice-Chair prior to becoming Chair. This is how I got more involved in Technology First, however, there are many paths to leadership and influencing the direction of our organization. Find something that you are passionate about and get involved. This is your organization and a chance to make a difference.

We are in the process of reviewing our previous three year strategic plan and accomplishments. We will soon be developing our new strategic plan for the next three years. Our objective is to continue to push the organization to even higher levels. The way forward is to provide even better benefits to our growing membership including both those that provide IT solutions as well as those enabled by technology. We are looking for feedback and input on our future direction. Conversations with participating members and volunteers will help feed our strategic plan. I look forward to the coming years, working with Marcia, the Board of Directors, the Technology First staff and our many volunteers and members.

As Executive Director, Marcia will lead the promotion of Technology First, ensure revenue growth, manage the operational budget and drive the expansion of provided services in support of the region’s IT industry. Marcia has extensive experience in leading a non-profit organization, having spent eight years as the Executive Director of the Ohio Association of Advanced Practices Nurses (OAAPN). Prior to that, Marcia held positions at Lexis/Nexis and Ameritech. She holds a Bachelor’s degree in accounting from Miami University and an MBA in management from Wright State University. She resides in Dayton with her husband and family.
Companies are grappling with the increased demand to protect their information and assets from the growing threat landscape. At the same time, they are trying to manage a shrinking budget and a constant push from the C-suite to do more with less. This delicate balancing act sounds impossible when trying to secure your company, but with the right focus and support, it can be done. But first, why do you need security, and how do you approach it more strategically?

Breaches Impact Your Bottom Line
A security group and security program do not have to be seen as a large cost center, but rather a value add proposition. Solutions can be scalable based on the size of an organization. Throwing money at securing a business is not only unnecessary but is also a reactive practice that should be avoided. Companies need to be proactive by having a strategic plan. When building an organized security program, one thing must always remain consistent: it should be composed of a multi-layered approach, also known as Defense in Depth (DiD). The National Information Assurance Partnership (NIAP) supports a three-pronged approach for such defense: people, technology, and operations. It boils down to this:

- **People**: Hire the good people, implement continuous training, and reward them well.
- **Technology**: Deploy solutions that support a layered network defense strategy.
- **Operations**: Enforce security policy, respond rapidly to incidents, and restore critical services as quickly as possible.

The idea behind a layered approach is that it creates more obstacles for intruders. Networks with more obstacles make less secure networks appear more attractive to intruders. But let’s be honest, despite best efforts, the intruders can still make it through. Don’t let this discourage you. Companies will always have incidents to manage and vulnerabilities caused by people and technology. The incidents and vulnerabilities shouldn’t deter the quest for a sound security approach. Doing nothing is not an option.

As threats become more sophisticated, let’s take a look at what happens when they culminate into a security incident or a data breach. But first, what’s the difference between a security incident and a data breach and why should you care? A security incident is any event that compromises the confidentiality, integrity, or availability of an information asset. A data breach is an incident that results in a confirmed disclosure (not just exposure) to an unauthorized party. Security incidents are plentiful and often should be an expected risk of doing business. When identified, not all security incidents are required to be reported. Breaches, however, must be reported and follow a specific protocol to inform all those affected by the data loss. Breaches are what we see splashed across the headlines resulting in substantial monetary loss and, in some cases, heavy regulatory fines. The most critical effect is the long-lasting reputational damage and declined customer confidence companies can experience after a breach.

In the last year, over 90% of businesses surveyed by Kaspersky Labs experienced some form of external threat, ranging from minor to significant (“Global IT Security Risks Survey,” 2015). 22% of businesses lost data as a result of those threats, which culminated into data breaches. These percentages showed that an average cost of a data breach
Breaches impact your bottom line, no matter how big or small the business ("Gartner Says Worldwide Information Security," 2014).

**Top Security Priorities in 2016**

Now we know what happened over the last year, but what are the top security priorities in 2016 to help prevent incidents and breaches? Note: All these can be baked into a Defense in Depth (DiD) strategy:

1. Malware Detection
2. Preventing Data Leaks
3. Patching/Vulnerabilities
4. Securing Cloud Infrastructure
5. Continuity of Service On Systems
6. Focus On Security of Third Parties
7. Physical Security of Systems
8. Securing Mobile Devices
9. Securing Virtualized Infrastructure
10. Security Awareness Training

But wait! Why are we spending $80 billion and rising year over year to secure data? There’s no arguing that information security is a necessary investment. In financial investing, people don’t throw money at a stock without first understanding risk and potential ROI. Security is no different. I’m not surmising we spend less on security. Instead, we need to invest more wisely to maximize ROI. Companies should not spend money on pricey tools they will never use or systems and software that end up underutilized. That doesn’t mean the CFO should slash budgets and demand more for less. Rather, it suggests taking a structured, holistic, and risk-based approach to security. The method needs to be reasonable and scaled to protect the organization as it grows and changes. Below are some basic requirements companies must implement, at a minimum, to understand their risk of exposure as we move through 2016:

1. Conduct a security risk assessment. Identify the scope of your systems and focus on where confidential and restricted information is stored, processed, or transmitted.
2. Understand the threat landscape and the vulnerabilities that can be exploited.
3. Estimate the impact of a vulnerability if it was exploited using a classification matrix to identify the level of impact.
4. Determine the risk using a risk matrix that identifies the likelihood of a threat, magnitude of impact, and adequacy of existing controls around the risk.
5. Identify controls that could reduce or eliminate the risk.

Organizations that do not have the resources should look into outsourcing security. Many companies can shepherd them through the process without charging astronomical fees and bulging their budget.

Finally, as we move through 2016, Gartner has predicted 5 key security trends on the horizon that will affect the way companies approach security. The security priorities noted earlier will be impacted by these trends. All should be considered when building your DiD security program.

1. **Mind the Gap.** Companies are having an increasingly difficult time filling open security positions. Qualified candidates can afford to be picky, and they want to be assured the security is endorsed at the highest level.
2. **Back to Basics.** Chief Information Security Officers (CISO’s) are moving away from dumping money into tools and technologies that will never be implemented or not used to their fullest potential. Instead, they make smarter, more targeted decisions that support the fundamentals of security first, such as security awareness training and policy restructure.
3. **Across the Pond.** In 2016, US companies will face tough decisions and trade-offs if they continue or plan to invest in some international markets. For example, China demands a backdoor software and technology access from their business partners. Backdoor into software and technology may expose intellectual property and other sensitive data. The risk may not be worth the reward for many CISO’s looking to expand business into the world’s largest market.
4. **One is the Loneliest Number.** As breach reports continue to rise, companies are inspecting their current security organization. They are looking for ways to restructure or add resources so the breach burden does not rest squarely on the shoulders of a brave one or two employees.
5. **Threat Intel Throughput.** With the rise of Big Data analytics, companies have massive amounts of threat intelligence data at their fingertips. Access to quick

(continued on page 5)
In Stormy Seas…

If you made it through this article, the days of adding security on a whim, or when it’s convenient, or when you have resources are over.

Security is far more expensive and risky to retrofit in a world where technology moves faster than a fleeting thought. Smart planning will save you valuable time, resources, and money. Working security measures into your current architecture will provide the added benefit of securing your data properly. In a world where many are breach fatigued, and companies are budget strapped, securing your data should not be left hanging in the balance.

In stormy seas, it’s better to have an experienced captain than a big boat. Approach your security stance accordingly.

References


(continued from page 4)

intel around user anomalies and threat detection will change the way we approach security on a global scale.

Putting technology into practice, it’s what our consultants do...

7 practices, 1 partner: Sogeti

With experts in Advisory Services, Application Development, BIM, Infrastructure, Mobile, Product Engineering and Testing, our Local Touch—Global Reach approach to consulting means you have access to local experts and a global team.
When was your most recent data center migration? For many, the answer may be never. There are some common, but not so obvious, items that can sidetrack or even derail some migration projects. You should take these into account as early as possible in your migration planning process to ensure a smooth and successful migration.

Here are 10 data center migration red flags and how you can avoid them:

1. **Viewing migrations as only an IT infrastructure project vs. a business initiative**
   When planning and executing a data center migration, it is easy to think of it as an infrastructure project for which the end goal is to move the physical and logical servers, storage, etc. While this is true, the purpose of those infrastructure components is to meet a business function or process through running applications. This means one of the keys for successful migration is the consideration of application and business capabilities in addition to infrastructure.

2. **Inaccurate understanding of project scope**
   A complete and accurate understanding of both the assets and applications that are impacted by the migration is critical. A holistic approach needs to be taken that considers applications, their dependencies to multiple servers and the dependencies between applications. It is important to understand the business context of the applications, including business impact and allowed outage window for migration, along with the infrastructure and desired end-state.

3. **Underestimating storage migration time and complexity**
   On the surface, storage migration appears to be fairly straightforward. You have a certain amount of data stored, and you want to move it to a new location. Yet it is not a simple one-for-one swap. The volume of data alone can make it time consuming and disruptive, especially if you need to shut down a production system in order to make the migration. Differences in architectures across vendors or product releases from the same vendor can get in the way.

4. **The right tools are essential but they are not “auto magic”**
   Migration tools can be helpful. However, each tool is designed with certain assumptions in mind—assumptions that may or may not apply to your specific situation. For example, your storage migration requirements will take shape as you plan the migration. Factors such as the specific storage platforms you are migrating between, connectivity and available time will impact the fit of a tool for your migration.

With the appropriate tool(s) identified, there will need to be investment of both financial and personnel resources. Individuals will need to install and configure the tools. Establish a pilot platform, where possible, to confirm that the tools function as anticipated within your environment and for your intended purposes.

5. **Not connecting the current data center with the new environments**
   Connectivity is a critical factor in data center migrations, but one that is easy to overlook as you focus on other issues. You may need a short-term increase in network bandwidth, which comes at a premium price and typically has a long lead time for engineering and installing. If you are running the old and new data centers in parallel as you migrate, you need to plan for sufficient bandwidth, acceptable latency, and maintaining quality of service for production traffic. This configuration needs to simultaneously support production requirements along with ongoing data migration and potential backups across the wire.

6. **Failing to address all of the logistical details**
   This is another area that is easy to overlook until you are in the middle of a migration. You should ensure you have coordinated all the details. It is important to schedule all the pieces so they happen at the right time and in the right order. It is valuable to ensure that you understand the implications the schedule will have on the facilities. Often businesses and their data centers are in shared facilities, and plans made by other tenants or the property management company can significantly impact the logistics required for your migration. There are typically multiple vendors involved, each with its own requirements, so coordinating across all of them is critical. The better you understand and schedule the logistics, the smoother the data center migration will go.

7. **Over-valuing uptime**
   In the UNIX world in particular, the longer a system has been ‘up’ the more favorable the up-time metric is considered. When a data center migration is looming, it is usually recommended to reboot the system to ensure all updates have been successfully applied and a smooth reboot occurs. This simple operation helps you avoid thinking there is a problem with the data center migration, when, in fact, it is a result of a system coming up in a different state than prior to the move. Performing the reboot prior to the migration is often easier said than done since these are typically critical systems and scheduling an outage window for the reboot may require approval from multiple areas.

(continued on page 7)
A similar risk, but almost in reverse, can occur with network devices. Updates can be applied and active in RAM but they must, also, be saved to flash on the device. Otherwise, when the devices come up after the migration they may effectively be downgraded to a prior configuration. Additionally, saving the configurations to a separate location from where it can be restored is recommended. These are common practices among network administrators, but we are human and mistakes happen. Taking the time to confirm the completion of these steps prior to a migration will help avoid issues.

Not decommissioning old applications

Many companies do not take full advantage of the opportunity to optimize and/or rationalize their applications or operations when migrating. This can be a prime opportunity to have a discussion with the business to take the final (or initial) step in decommissioning an application that no one uses. The decommissioning should occur prior to the actual migration.

An honest and frank discussion about the value of an application or component vs. the cost to migrate should occur. For apps that are either redundant or at the end of their life, this discussion should be fairly straightforward. The harder discussion is for apps that are not quite at their end of life but close enough for consideration. This discussion is particularly valuable for organizations that have experienced mergers and/or acquisitions and are migrating to consolidate operations.

Missing opportunities to transform your IT environment

Beyond the hardware and software within the data center, a migration is both impacted by and can influence other processes within the IT organization. Tracking and closely monitoring changes which are occurring within the landscape of the servers and applications throughout the migration process leads to a successful migration. Put another way, take this as an opportunity to tighten your change control processes and have them become part of the of the entire IT organization vs. an afterthought. Significant data will be gathered during the data center migration project that can be incorporated into a configuration management system. It is essential to have the configuration management processes defined and consistently adhered to throughout the organization. A configuration system without effective processes is little better than proceeding without the system.

Similarly, standard operating procedures for data center operations should be confirmed and followed. There is no magic bullet. It requires intentional effort and support throughout the IT organizations.

Not confirming all assumptions

Throughout the planning effort, assumptions must be verified. Proceeding down a path too far without verification and buy-in from all parties can lead to a waste of time and money. An example is that all applications on a non-production server are non-critical. We have probably all seen situations of a pilot system slipping into a pseudo production usage by a key sponsor; often an executive of the project. Finding this out late in the game would likely alter the move plan causing additional planning effort and potential rescheduling.

Also, we must be cognizant of external business events impacting the project and the personnel available for working on a project. Some data center migrations occur as a result of a merger or acquisition. In these situations, there is a risk of increased attrition of personnel with a resulting loss of the institutional knowledge about applications and systems.

Data Center Migrations Affect Every Part of Your Organization

Data center migrations don't occur every year for many companies so it is important to work with a partner who can help you look at a migration holistically and how it will affect every part of your organization. By understanding the potential common pitfalls of data center migration projects, you can better ensure a smooth and successful migration that won't jeopardize your reputation and internal brand to your company.
Award-Winning Project Enables Enhanced Case Management for the Disabled

BY: RSM

Overview
The developmental disabilities’ community is shifting to a person-centered approach, where the individual drives the development of their Individual Service Plan (ISP), which outlines goals and the plan to reach those goals (including what supports and providers will be used). This includes what’s important to them and for them, and involving them in the decision-making process. The person-centered approach is critical to helping individuals live fulfilling lives and realizing their dreams.

To support this shift, 18 county partners (referred to as the county collaborative) embarked on a business transformation process called imagine. With the support of the Ohio Department of Developmental Disabilities (DODD), the county collaborative focused on developing common business practices that enable the person-centered philosophy, including standardizing the ISP process and improving the delivery of service. The team also looked for ways to reduce administrative expenses and increase efficiency through sharing information and resources across counties.

To support the work of the team, DODD offered to build a technology solution that made it easy for participating counties to implement the new business processes. The solution would develop a case management system that would improve service delivery for individuals and families, county boards, and providers, while allowing individual counties to retain their autonomy and identity.

Microsoft Dynamics CRM® was selected as the system’s core, and while the client was impressed with our team’s proposal and experience, they had reservations because they knew other states’ agencies attempted something similar and failed. McGladrey’s team invested significant time creating screen mock-ups to illustrate the Dynamics CRM system’s effectiveness in automating case management processes. DODD liked RSM’s creative approach, and the engagement began in earnest.

The Project
DODD oversees a statewide system of supports and services for people with developmental disabilities and their families. Eighty-eight county boards of developmental disabilities deliver programs and services to county residents. Because the system is county-based, each of the 88 counties has largely unique business processes and service delivery systems that are tailored to the needs of their local community.

While this system has its benefits, it presents some challenges when developing a technology solution to support case management. Some of the considerations the McGladrey-DODD team focused on included:

• Varying processes, procedures and providers across counties
• Established paper-based processes, which sometimes conflict with each other and require a multi-step approval process
• The need for collaboration across the team, some of whom are outside of the state’s offices and network; the team may include the individual, guardian, case financial manager, Human Rights and Behavior Support Committees, providers and others
• Separate provider lists (by county), which can make it difficult to access the full scope of providers able to work with an individual
• A diverse user base with varying needs; input was sought from 18 different counties, which was tied to more than 500 individual user stories and numerous specifications
• Required integration with multiple legacy systems
• Compliance with specific HIPAA and section 504 guidelines to protect the privacy of individuals’ case files, which contain sensitive personal information

Outcomes
Over the course of 12 months, RSM’s team and DODD, using a “blended team” approach, completed an analysis of a three-year requirements-gathering process and developed the imagine system to support person-centered case management. The newly designed imagine system:

• Makes it easy to develop goals and outcomes by capturing information in eight key life areas, and sharing that information across the team for ISP development

(continued on page 9)
• Provides complete information about each individual’s ISP, including agreement and approval, goals, services, providers, funding sources and progress
• Provides an easy method for tracking agreement and approval of the ISP
• Tracks changes and creates snapshots of the ISP for auditing, as well as consolidates reporting for easy distribution to stakeholders
• Leverages dashboards to enable easy access for caseworkers to see the status of ISPs and high-priority tasks
• Keeps all team members informed of all outstanding tasks and key changes
• Replaces manual processes for tracking and calculating local services, budgeting, funding sources and approval of services
• Integrates key data from other systems to streamline the case workers’ workloads and provides a more complete view of the individual and their case
• In addition, DODD created an ISV portal solution, allowing everyone involved in a specific case to view the individual service plan. This transparency helps ensure each service provided makes sense and is synergistic, not counterproductive.

Customer Excellence Award

As the engagement wrapped up, DODD was pleased with the result. Microsoft also noticed the work and nominated DODD for the Microsoft Dynamics Public Sector Industry Customer Excellence Award, with RSM as the engagement partner. In each category, award winners are chosen on their ability to provide amazing experiences for their customers through the use of their Microsoft Dynamics solution.

In naming DODD a winner, Microsoft commented, “The imagine project is not only an inspiring story about improving the lives of individuals with developmental disabilities, but is one of our best examples of how government organizations can use CRM to create a 360 degree view of their constituents.”

Currently, DODD has started implementing the imagine system within the 18 county collaborative. Other counties wishing to participate will soon be able to begin using the imagine system.
What is Discovery? The Best Way to Start Application Development Requirements

We’ve previously talked about what you need to know before you talk to an application development company, but what happens if you don’t really have the answers to those questions? What if you have nothing more than a basic sense of how your application is supposed to work but don’t really know how to get to the point where you can have a reasonable conversation with the firms you contact? The simple answer is—Discovery.

What is Discovery?

If you contact Segue Technologies in the previously-mentioned situation, we’ll likely suggest a “Discovery” engagement, which—as the name suggests—helps us “discover” what it is that needs to be accomplished. Specifically, it allows Segue to work with potential customers to refine their vision of their intended application, develop a deeper understanding of the functionality and related business rules, and to garner enough information to provide a reasonable cost estimate for development. Typical deliverables from Discovery include high-level system requirements and basic design concepts (maybe a logo, or wireframes of a few screens that help explain how the system should behave, etc.). Essentially, Discovery helps us to write a Statement of Work (SOW) that could be used as part of a Request for Proposal (RFP) to solicit bids for development. Simply put, it helps us understand the work that will be required, and what that work is likely to cost.

What Happens During Discovery?

Many times, non-technical entrepreneurs may have an idea of what functions their intended app should perform at a high level (“My app will let people schedule laundry pickup from a roster of local dry cleaners!”) but not have any real clarity on how that should happen (Who manages enrollment? How are users validated? How is payment handled?) During Discovery, Segue collaborates with the customer to better understand how all of the pieces of the application should work together, and what the cost implications are of the decisions they’ve made.

Discovery is an interactive process, and succeeds or fails based on the involvement of the customer and their level of preparation and knowledge of their intended market. While we have the expertise to translate objectives into requirements, if the customer does not know what they’re looking to accomplish, or cannot express it clearly, the Discovery effort may not reach its full potential. As always, being an educated customer is the best way to ensure success.

Benefits of Discovery

It’s also important to note that sometimes, Discovery also serves as a means to determine that a proposed project is not feasible, or is too expensive for the customer’s budget. By completing Discovery as a sort of “mini-project” the customer reduces their outlay for a project that would have been prohibitively expensive to fully develop. This sort of “surprise cost” tends to be more typical of entrepreneurial/startup sorts of applications or systems, where there are a lot of unknowns and new ground that needs to be broken to realize the system. By developing high-level requirements and some basic design concepts, we can gain a much better picture of the overall size of the effort required for full development.

Of course, not every customer or project requires a formal Discovery phase. Customers with well-written RFPs or SOWs do not typically need Discovery. On the other hand, when we are faced with an incomplete picture of the customer’s needs, we will generally recommend Discovery as a tool to flesh out the details to the point that we can confidently bid for the work. In the end, Discovery can save a lot of headaches for both the customer and Segue, and can go a long way to making sure that the customer will get what they have asked for, for a price they are willing to pay.
Privacy in the Cloud: Protecting Yourself

BY: Diane Reynolds, Taft Law

Demand for cloud computing is mounting swiftly, with double-digit annual growth rates expected through 2018.

Use of a remote, shared computer network to store, manage and process data can save time and money by eliminating the need for a local data center and an IT team to run it. Whether on a smart phone, a laptop or a desktop computer, cloud computing gives users immediate access to data anywhere there is an Internet connection.

Gartner, one of the world’s foremost IT research companies, expects cloud computing to become a $250 billion industry by 2017. Other estimates vary but they are all high. Forrester Research forecasts that public cloud computing revenues will reach $191 billion by 2020. Cisco forecasts a steady migration of IT work from traditional data centers to the cloud.

Industry analysts say the edge that businesses gain from moving data to the cloud accounts for its rollicking growth. So what’s not to like? In a word, security.

Many organizations are uncertain how safe even the most reputable cloud providers are. In fact, it’s the nature of the beast: Someone else, a third party, has access to your data and is responsible for keeping it secure, at a location other than your business.

Here are some steps you can take to minimize the risk of your data being stolen, damaged or accidentally deleted.

Research Cloud Providers

Look for providers that are independently certified as following best security practices.

Also, be aware that rules governing data retention, data protection, medical file management and other areas can vary by jurisdiction and country. It’s important to have an understanding of the specific laws and regulations that apply to the services you’re using.

Use Authentication

Companies that have applications running in the cloud should make sure the applications are accessible only to the employees that need to be using them. Two-factor authentications require you to enter a short numeric code in addition to your password before you can gain access to an account.

Use Encryption to Protect Cloud Files

When moving data to the cloud, it should be encrypted to protect against unauthorized access. Encryption should be in force both when data is being transferred and when it’s in the cloud. Only authorized users should be able to decrypt and read the information.

Monitor Who and What Devices are Using Your Cloud Accounts

Secure web gateways allow IT departments to see how data is flowing in and out of cloud accounts. Also important is protecting all PCs, laptops, tablets and smartphones that have access to cloud data.

Know the Rules in the Event of a Data Breach

Be clear about your cloud provider’s disclosure policy should your information be compromised, including how quickly the provider is required to notify you. Disclosure laws vary among U.S. states and among foreign countries. Terms should be spelled out in your initial contract with the cloud host.

Also, if you discover the breach first, you may need to inform the cloud provider, which may have ramifications for its other clients sharing the same server. Having agreed-upon steps in the contract and an incident response plan in place that’s been approved by both parties will lessen the consequences of a breach.
Leveraging Server Monitoring to Improve Your Network

By: Derrin Rummelt, US Signal

How much of a payback would you like to receive from your investments in monitoring your IT environment?

Most people never think about a payback from IT monitoring. They see it as a preventative measure that will alert them when something goes wrong. It becomes categorized as an operating expense, a necessary cost of doing business.

The “Other” Thing Server Monitoring Does

Beyond waiting for anomalies to occur in your servers and other endpoint devices, monitoring constantly collects and stores information about what your devices are doing. How much memory they’re using. How much storage. How many input/output operations. How many requests are being made of various devices, and much more.

Since this data is constantly collected over time, it builds a history of how each device is performing, and since it tracks various performance metrics, how things are going can be correlated with what was going on at any given moment in time, and then tracked over time to see what creates improvement, and what causes problems.

How Does That Create a Payback from Monitoring?

Time is money. When memory is being used inefficiently, or input/output operations are inhibited by improper settings or insufficient resources, the end result is that reports take more time to produce, screen changes take longer to refresh and people end up waiting to continue working. Every moment of time spent waiting instead of working creates cost. The more time spent waiting, the higher the cost.

When US Signal meets with your management to discuss our observations from the most recent monitoring reports, it’s not just to make you aware of the problems we fixed before you ever would know about them. It’s also about our observations of what’s been happening in your servers and other endpoint devices, and what the impact has been on performance.

We also discuss adjustments, changes, or other steps we would take to improve performance by eliminating or otherwise resolving the challenges we’ve identified.

Your first sign of payback will more than likely come from your users themselves as they report less waiting time, better responsiveness from the servers, and more work getting done. To get some idea of the possibilities, look at the number of people using any given server. Conservatively estimating that their pay rate is $30 per hour, that’s a half dollar every minute. Every two minutes of delay is costing one dollar. Multiply by the number of working days in a year. Recapturing those lost minutes pays back all those lost dollars.

Many Moving Parts to Better System Performance

Anyone who has ever looked at the various server consoles, even if they have no technical background, will observe that there are many adjustments that can be made, many controls on each console.

Each of those controls represents an opportunity for something to be set incorrectly. Constant monitoring uncovers these problems, enabling us to readjust them based on what is actually happening in your IT environment.
Achieving Data Center Transformation

By: David Mettler, Vice President Sales, Market Director—US, IO

Colocation is a top consideration for companies looking to address their data center capacity constraints. Colocation refers to when an organization houses its IT equipment (servers, storage, network gear) in a multi-tenant data center. This strategy typically helps businesses gain access to economies of scale, advanced infrastructure, greater bandwidth and operational expertise.

For technology companies, your quest in selecting colocation services needs to be about more than just scaling existing capacity. Your company needs to see this journey as an opportunity to transform the data center to improve efficiency and increase flexibility to adapt easily to business change.

Colocation Fundamentals Done Right

The first step in transformation is to ensure all the data center service basics are well covered in a colocation offering. These include having reliable and resilient power and cooling capabilities in place to help ensure always-on uptime and optimal performance, having multiple layers of physical and logical security, and carrier neutral network connectivity.

Physical security needs to include video cameras to monitor all general areas within the facility; man-traps, equipped with biometric authentication, to prevent impersonation and unauthorized tail-gating; and fire-rated walls and doors to protect against a disaster.

Network options should allow you to extend private networks without using the public Internet. This approach needs to not only include communications between multiple systems within a data center footprint but also cover communications between colocation infrastructure and any end point, including other data centers and public cloud services. Doing so will enable a borderless data center, connecting any location with a network presence.

Modular Colocation — Go Beyond the Fundamentals

Most colocation providers operate construction-based data centers, in which they leverage traditional design, build, and operations practices from the commercial real estate industry. To achieve data center transformation, your company needs to leverage a model based on modular data center technology, which allows for colocation solutions that traditional data centers cannot provide. These include:

Scalable Growth — Fast. A modular data center colocation service provider can help you future proof your data center by delivering standardized deployment options that give you the flexibility to meet the demands of your compute today and beyond. The modular form factor allows for thin provisioning of the data center, meaning that you can deploy the actual capacity you require and then expand when needed. If your modular data center provider operates at a large scale, and uses manufactured, purpose-built modular technology, they’ll be well positioned to deliver new capacity to you in as few as 30-90 days.

Operational Efficiency. Modular data centers enable enterprises to achieve efficient utilization of their data center infrastructure. Too often an organization that has felt the pain of running out of capacity in their traditional data center will over buy new capacity when they move to a larger data center. This inefficient use of the company’s capital has two direct costs: 1) paying for services they do not actually need, and 2) underutilization of their data center space which increases the cost to power and cool the data center they are using. By offering capacity in small increments a service provider can offer significant savings to their customers.

Improved Security. Modular technology also improves security by providing a data center within a data center — with each module being its own private steel vault. And modules that have a compartmentalized architecture go one step further by enabling the segmentation of colocation users, eliminating any risk of noisy neighbor syndrome and keeping potential hazards from spreading.

Flexibility — An Adaptable Data Center

Next on the road to data center transformation is being able to leverage cloud services and traditional colocation services under one roof. The key is to have a data center platform that allows for flexibility among colocation, public cloud and private cloud so that you have the ability to fully understand your costs, your data security risks and obligations, and determine the best solution for your business.

With this strategy, your organization can know where your data is physically, and who is managing the infrastructure that stores your data and runs your applications. Additionally, for large amounts of data, network performance is not an issue if your entire infrastructure is physically located in the same building. Many organizations enjoy the peace of mind that accompanies knowing where their data physically resides.

Software Optimized Data Center

We live in a software-defined era. Much of the value of the data center going forward will be driven by software innovation. Data center infrastructure management (DCIM) software monitors and manages all enterprise data center assets inside of your colocation space, but DCIM does not provide insight into the critical systems that enable your data center space to operate. You need to have full transparency of your colocation service which means real time information on your power utilization, your PUE, temperature, humidity, and access controls. This requires a data center operating system and, if you can integrate this information with your DCIM, then you can receive the business intelligence, real-time visibility and control needed to transform your company’s infrastructure management.

Transforming Your Data Center

As your business looks to address the inevitable need to scale your data center environment and considers colocation options, you should take a strategic approach and look towards transformation. Create a next generation data center with a modular colocation service that is truly scalable, efficient, secure, and software managed. By doing so, you will position your company to intelligently manage the data center to drive more efficient operations and improved performance.
INFORMATION

NEW JOB POSTINGS

IT Manager/Director .............................................................. Lighthouse Technologies, Inc.
Database Developer (Oracle, SQL) ........................................ Speedway
Business/System Analyst ...................................................... NCR Corporation
Help Desk ............................................................................. Montgomery County Job and Family Services
Business/System Analyst ...................................................... Montgomery County Job and Family Services
Network/Systems Admin ........................................................ Montgomery County Job and Family Services
Business/System Analyst ...................................................... Midmark Corporation

Security .................................................................................. Speedway
Infrastructure Manager ......................................................... Speedway
Programmer Analyst/Software Developer ............................ Montgomery County
IT Architect ............................................................................. Aileron
Sales Associate ...................................................................... Cincinnati Bell Business
Programmer Analyst/Software Developer ............................ CIVICA CMI
Help Desk .............................................................................. CIVICA CMI

TECHNOLOGY FIRST BOARD OF DIRECTORS

Diana Bolden
Senior Vice President, Information Technology and Operations
Teradata

Jim Bradley
Global IT Director
Tecomet

Gary Codeluppi
VP, Marketing and Business Development
The Ross Group

Doug Couch
Vice President, Information Technology Services
Speedway

Ann Gallaher
Chief Operating Officer
Technology First

Gary Ginter
System Vice President/CIO
Premier Health

Steve Hangen
Chief Information Officer
Mikesell’s Snack Food Company

Bryan Hogan
President / CEO
AfdenceIT

David Hoskins
Director of IT Workflow and Collaboration
CareSource

John Huelsman
Director, Business Support Services
Hobart Service

Tim Hull
President
Bitstorm Web/ TDH Marketing

Scott McCollum
Chief Information Officer
Sinclair Community College

Monique McGlinch
VP of IT and Customer Experience
Midmark Corporation

Paul Moorman
IT Strategist
Catalyst Paper Corporation

Dave Rotman
Associate Vice President for Technology/CIO
Cedarville University

Leigh Sandy
Founder
Extra Mile Fiber

Shu Schiller
Chair, Information Systems and Operations Management
Wright State University

Thomas Skill
Associate Provost & CIO
University of Dayton

Diana Tullio
President
Lighthouse Technologies, Inc.

Jeff Van Fleet
President
Lighthouse Technologies, Inc.

Technology First would like to thank and recognize its Board of Directors. They provide input into the strategic direction of the organization and actively lead working committees that drive our programs and services.

Technology First Board of Directors

Writers: Our mission is to support the growth of Greater Dayton’s information technology industry. Technology First provides a forum for educators, business, and technical professionals to communicate their expertise and lessons learned while working in the field. Please submit the article in Word, preferably with 500 to 700 words, with any graphics in pdf to agallaher@technologyfirst.org. Please include your name, business organization, business address, phone number, fax number, e-mail address, and a brief description of any professional accomplishments. Please also include a digital photograph if available.

Subscriptions: Non-member business/home delivery of this publication is available at $120/year (11 issues). Mail name, address and check made payable to Technology First.

2015 Technology First; All rights reserved

714 E. Monument Avenue; Suite 106 • Dayton, OH 45402 p: 937.229.0054

www.technologyfirst.org
Take control of your data security.

Applied Cybersecurity Training at Austin Landing

Focusing on the need for training in cybersecurity, intelligent systems and data analytics, Sinclair College’s Cyber Technology Center at Austin Landing is designed to help prepare businesses to mitigate the threat of cyber crimes.

Business Intelligence • Analytics • Cloud Cyber Physical Systems • Robotics Health and Medical • Data Analytics Smart Systems • Computer Forensics

SINCLAIR
CYBER TECHNOLOGY CENTER

workforce.sinclair.edu
937.512.2428

Sinclair Cyber Technology Center at Austin Landing
10100 Innovation Dr., Suite 310

workforce.sinclair.edu
Website Neglect

The Leading Cause of Missed Business Opportunities

Take advantage of the economical Managed Web Maintenance Programs from Bitstorm Web.

- Reduce your load times
- Improve security
- Maintain site upgrades
- Boost your content management
- Optimize search marketing
- Enhance ROI

Why go it alone when time is so limited? Partner with Bitstorm Web for effective web management services.