

Data is Money

Mass Digitization and the Internet

November 2008

**Online Tech Inc.
220 Huron Street
Ann Arbor, MI 48104
(734) 213-2020**

www.onlinetech.com

1. Audience

Owners, Chief Executive Officers, Presidents, Chief Financial Officers, Chief Operating Officers, and IT Directors of small to medium-sized businesses facing significant growth.

2. Abstract

As data and business content becomes digitized and automated the need to store and manage this data has become eminent. Data is like money, as they both require safe, reliable storage needs. And as data becomes more important to everyday business operations, it is quickly becoming an irreplaceable business asset. To ensure your business' data is secure, scalable, and reliable, your business needs a data center that provides security, reliability, scalability.

3. Introduction

As the world digitizes everything the value of data goes up exponentially. This makes sense as we migrate from an industrial to a knowledge economy.

One example of digitization is the automation of many processes for which there are no feasible manual alternatives to operate. Many organizations have software applications or websites that are required for their business to operate.

At the same time threats to data are on the rise. Few believe we will experience a decline of weather disasters, cyber-attacks, data theft or terrorist activity in the decades to come. The complexities of cyber attacks, severity of weather attacks and ferocity of terrorist activity are increasing.

As if these trends alone aren't enough, end-users expect applications to be "always on and always online." Imagine an airline that doesn't have online bookings. This requires cost-effective high availability systems that go beyond disaster recovery.

This mass digitization results in significant quantity of data that for many organizations becomes as difficult to replace as cash. In many cases this data cannot be replaced at almost any cost, making it more precious than cash.

Every organization keeps their cash assets in a bank. Data assets as valuable as cash belong in a vault with highly secure access to the world. This vault is a Data Center.

4. Digitalization of Everything

4.1 Mass Digitalization of Everything

Digitization is the process of taking information and turning it into 1s and 0s so you can process it with computer chips. There are many examples of digitization in our daily lives. Look around your home or office and you'll see:

- emails not letters and envelopes
- pdfs not faxes
- websites not brochures
- digital x-rays not film
- memory cards with digital pictures not cameras and photos
- instant messages not post cards
- online billing not envelopes of bills
- E-tickets not paper tickets

Few would argue that this trend of digitizing everything is likely to subside. We call this Mass Digitization. Every company, large and small is experiencing mass digitization as they operate. Some organizations are completely defined by their data. E-Commerce companies, Application Service Providers (ASPs), banks, and credit unions are examples of companies who are completely inseparable from their data. They are so “digitized” that their *data is their company*.

Look around your company, how many things do you track on paper and how many do you track online using spreadsheets, databases, documents, presentations and other digital representations? That’s “mass digitization.”

4.2 Data Concentration

This mass digitization drives demand for ever denser digital storage. The result is a slew of products that store tens of thousands of music, pictures, or movies on a device that fits in the palm of your hand. Yet, we all seem to run out of disk space every few years. It’s like the storage space at your first house. The new homeowner marvels at the amount of storage space only to ask, two years hence, “honey, where can I put this?”

The prospect of Terabytes (1,000 Gigabytes) of data fitting in the palm of your hand is incredibly exciting. However, data is valuable and often very difficult to reproduce. If you think about the concentration of value in the palm of your hand, you begin to wonder the risks. If I can fit that much value in the palm of my hand how can it be safe? What if I lose it, drop it or heaven forbid what if someone steals it?

4.3 Mass Automation

In this hyper-competitive age, every company is looking for efficiencies and strategic advantages. To that end they automate processes with software (almost always web based these days). These software applications collect data and make use of it, contributing greatly to mass digitization. How many processes in your company are automated? Billing, payroll, and, in fact, all accounting functions have been automated for quite some time. Other processes specific to your organization have likely been automated with software as well.

Even communications, a low-level generic activity absolutely critical to every organization has been automated with email and instant messaging.

By leveraging the power of the web, organizations are including their customers as users of this automation. In fact, your website is really just software that you programmed to deliver a specific interactive experience to your customers.

For many of these automated processes there's no feasible manual work around. The implication is that if the automated process fails you just stop being in business. Can you image EBay handling 10,000 auctions simultaneously with no website? It would take more than an army of people and phones. In fact, it can't be done.

Take email...try telling all your employees that they cannot use any email for 3 days. What manual process could serve as a viable alternative? There really is none. Companies who use their website to service customers are extremely vulnerable. Take your customer web-portal...could you handle the traffic it gets with your telephone and existing staff? Probably not. For, almost always, websites are designed (intentionally) to serve many more customers than could be done manually - that's the whole point of moving the process to the web in the first place.

5. Challenges and Risks Presented by the Mass Digitization

The rewards and value of digitization are clear and evident. Few would argue that it's not worth it. However the challenges and risks presented by the mass digitization can be daunting. To help, we organize these risks into four categories: Scalability, Reliability; Security and Regulatory.

5.1 Scalability

Two scalability challenges surface with mass digitization. The first is storage. How much storage do you buy if your business is digitizing at an unknown rate? The second is access. How many people need to access your data simultaneously? E-commerce, ASP and media companies often require significant simultaneous access to their data - that's what they do. The ability to grow their business is directly related to their ability to deliver their data to enough consumers simultaneously.

As your organization grows and as you digitize more data your storage needs grow exponentially. For many companies this has resulted in more and more servers, storage devices, additional disk drives, disk drive upgrades and a plethora of solutions to keep up. It seems there's never enough storage.

5.2 Computing Capacity

As more people need access to your data (which is everyone if you're an Internet company) you will need more and more, faster servers. How many you need, exactly what type, and by when can be very difficult to predict.

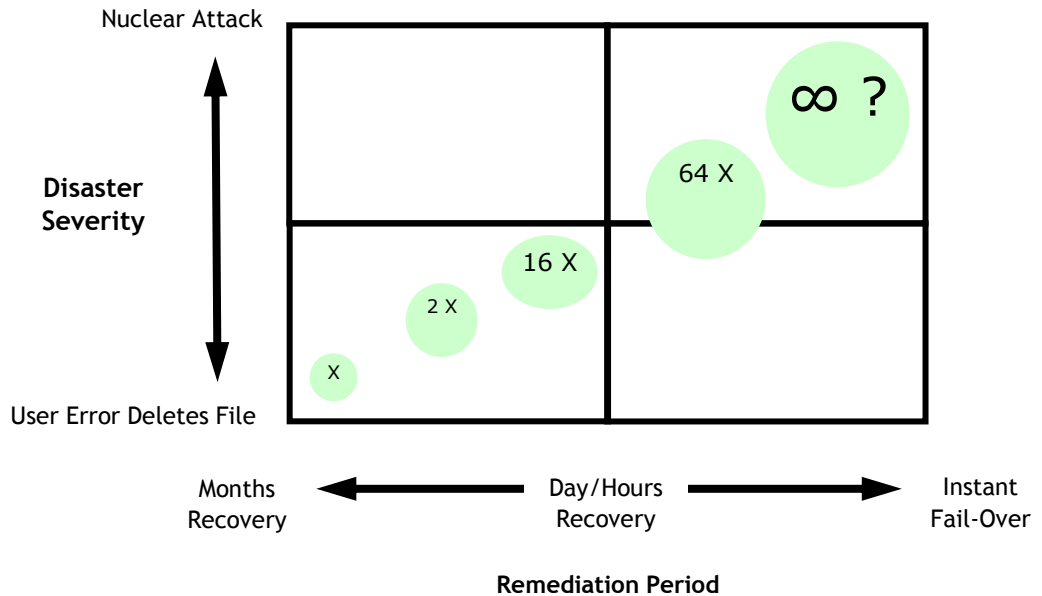
Meeting your scalability challenge is often not as simple as buying another server and plugging it in. Often the software or database architecture can't just "spread the load." Even more challenging is where to put the servers. Many organizations are struggling with their earlier choices to put servers in a room not suitable for growth. Now they are unable to deploy new applications, new users or new products all due to lack of capacity (generally power or cooling) for their servers. This is a very unfortunate case of a very tactical commodity (electricity) having very negative strategic (new products, new customers) effect on a business.

5.3 Reliability

A second challenge, and equally important to scalability is reliability. Unfortunately, there are no theoretical limits on how much you can spend on reliability - only practical ones. A severity/remediation grid can help to explain the relationship between the severity of a disaster, the remediation time and costs.

Disaster scenarios run a spectrum of severity from the least severe such as a low-end component failure to extremely severe such as a fire or nuclear attack. Every scenario on that spectrum has some chance of occurring. Generally the more extreme scenarios are less likely. This represents the Y-axis in our grid.

Independent of severity is the question of time to remediation. That is, how fast and to what degree do you need to be able to recover from the various levels of severity? The time to remediation is represented in the X-axis of the grid.



Ideally, one would like to be able to recover immediately from the most severe disasters. This represents the upper right corner of the grid. The lower left quadrant represents the inability to recover from even the most sublime scenario. As you make your way from the lower left quadrant to the upper right quadrant, costs go up exponentially. Due to mass digitization, the need to avoid the lower left quadrant has grown dramatically. Fortunately, there's new cost effective technology and providers to help with that.

The lesson is that there's no limit to what you can spend to protect against severe data loss. The question is what disasters or risks should you focus on given your business and which data or applications are mission critical?

5.4 Security

Security can broadly be categorized as physical or digital. Physical security includes protection from physical theft, fire, flood or power outages while digital security protects your network and data.

5.4.1 Physical Security

Physical risks include flood, fire, hardware theft and other such disasters that are clearly visible to the naked eye and generally involve the damage or loss of equipment. It can require significant capital to mitigate physical risks. To help prioritize your needs or investments, create a table similar to the one below, and apply it to your situation.

Scenario	Risk	Mitigation
----------	------	------------

Fire	Complete data loss and inability to carry out any automated processes. Generally requires complete rebuild relying on offsite backup resources.	FM-200 agent, pre-action dry pipe water, strict policies, fire proof materials, professionally, wired facility. Offsite backup.
Flood	Risk of data loss and likely loss of hardware and hence inability to carry out any processes requiring access to damaged equipment.	Isolate all piping. Zoning of any water-based fire protection. Install environmental monitors.
Power Blackout	Complete loss of main power for an extended period.	Generators and uninterruptible power supply (UPS) with transfer switch and batteries.
Brown Out	Power dips but does not go out.	Uninterruptible power supply (UPS), with surge protectors, which properly clean the power to the server.
Power Spike	Power spikes damage hardware which results in downtime or potential data loss.	Deploy an uninterruptible power supply (UPS), with surge protectors, which properly cleans the power to the server.

5.3.2 Digital Security

Digital risks include cyber attacks, data theft, and generally any other attack to your data sourcing from your network connections. In this case, the negative agent could be 10,000 miles away attacking you in the middle of the night.

The fight against Cyber Attacks is a Spy versus Spy game. The negative agents rapidly find and exploit security holes in protection and infrastructure technology. Therefore the degree of security is often determined more by the process of applying protections than the technology itself. Sound patch, password, and firewall management policies are important protections against common security breaches. Using a 3rd party to manage these functions allow you to quickly modify or restrict access to important servers and data.

Digital security generally begins by isolating information available to those inside your company, versus the information you want to open to the public using a website or other information. Virtual Private Networks (VPN) will extend your private information securely

through the Internet to employees on the go, or for your virtual office. Firewalls will protect the various layers of your website.

5.5 Regulatory

Universal Threat Management (UTM) is the latest network security solution as the industry evolves from traditional firewalls and VPNs into more advanced security required to address the sophisticated and destructive Internet threats. Using a layered security approach, UTM provides protection against blended security threats to help ensure your server infrastructure is safe, with defense against port scanning, Denial of Service (DoS) attacks, Distributed DoS attacks, and policy violations.

“Mass Digitization” has dramatically increased the potential for the rapid misuse of large amounts of data. This combined with recent events business, criminal, weather, and terrorist activity have resulted in a plethora of new regulations and public awareness regarding data use, retention, and protection.

Personally identifiable medical information requires special treatment per HIPAA¹ (Health Information Portability and Accountability Act) with significant penalties, including fines up to \$250,000 and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information.

Sarbanes-Oxley², commonly referred to as “SarBox” has driven public companies to revamp their data retention and handling processes to meet new controls. Many smaller providers to these public companies are now being scrutinized by their customers as they seek to assure compliance.

Data privacy, while not regulated has received significant public and media attention. Reports of stolen backup tapes containing private financial and medical data are commonplace in the national media.

Standards for credit card processing such as PCI or CISP also contain strict data handling and security (physical and digital) requirements including regular audits. This collection of regulations, data privacy, and industry standards adds to the risks and complexity of managing your data.

5.5 Summary of Risks

Data is money. It’s important that you properly protect that data. The key risks being scalability, reliability, and security. All three risks work together. If you only address two of the three risks you can’t grow:

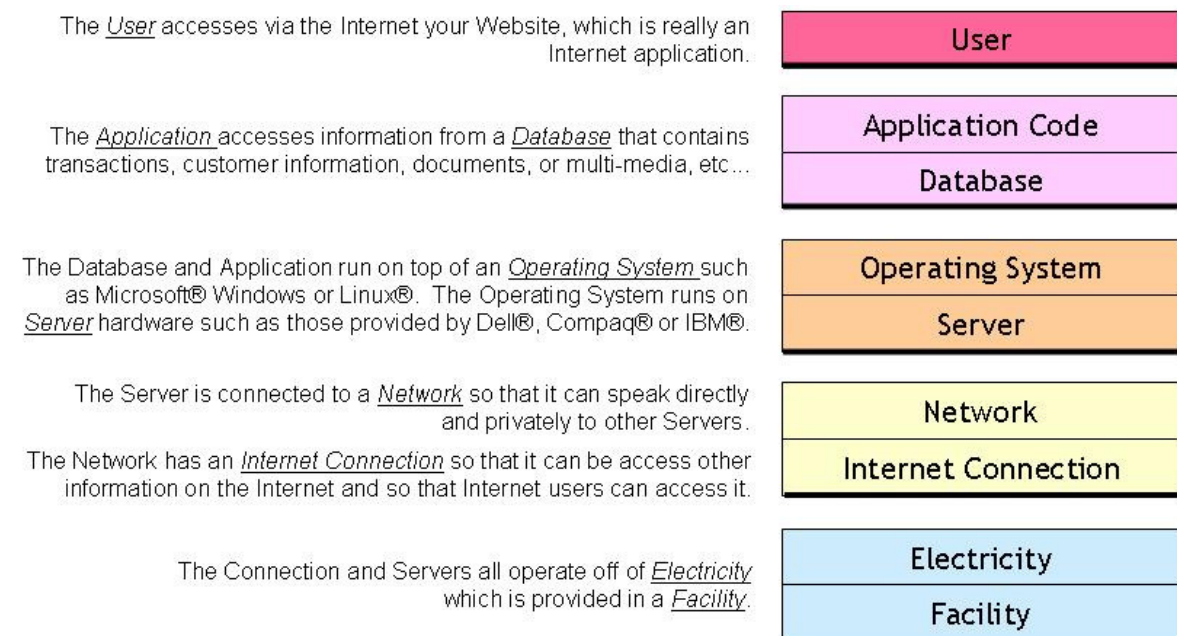
- ...if you reliably deliver a secure solution that can’t scale, you can’t grow

- ...if you reliably deliver a scalable solution that's not safe, you can't grow
- ...if you securely deliver a scalable solution that's unreliable, you can't grow

6. Framework for Security, Reliability and Scalability

It's important to have a holistic framework to properly manage the reliability, scalability, and security of your entire system. For example, the Internet Delivery Stack™ (IDS)³ isolates the layers of an Internet offering that allow you to more easily manage the reliability, scalability, and security issues for the entire offering by focusing on each layer.

There are nine layers to the stack. Each layer requires design, implementation, and management to assure a certain degree of security, reliability, and scalability in that layer. These layers are described in the diagram below.



Internet Delivery Stack™ (IDS)

7. Data Center

You keep your money in a bank. If your data is as valuable as money, then you need a “bank that holds data.” That’s a data center. A data center that is designed specifically to house servers, storage devices, and networking gear. They were designed precisely to provide a secure, reliable, and scalable facility for organizations to house critical data and computer

equipment. With “mass digitization” just about every company now needs to have their data and computing in a data center.

For many organizations the “data center” is a closet or office room with power strips, some network equipment, Internet connectivity and a handful of servers. These small “server rooms” suffer from an inability to scale; are often very unreliable; and highly unsecure.

A data center has special characteristics in three categories a) physical facility; b) power and cooling; and c) network to connect it to the world. For each of these categories you are looking for ways to 1) prevent negative affects to reduce risk; 2) monitor the status so you know when something is wrong ,ideally before the negative effect; 3) design failover and remediation strategies for handling failures.

The data center provides more than a peace of mind that your data is securely stored, reliably available, compliant, and scalable. This frees your organization to focus on the more strategic activity creating more high-value data, then finding and serving customers.

8. Summary

For most organizations “mass digitization” has made their data one of their most valuable assets. Data is now like money. No one keeps money in a closet, so why do organizations keep servers there? Money is kept in a bank and servers with important data should be kept in secure, managed data center. This is the only way to properly manage the security, reliability, and scalability risks associated with “mass digitization.”

About Online Tech

Online Tech (www.onlinetech.net) is Michigan’s premier Managed Data Center Operator. Online Tech helps companies manage their growing demand for data and computing capacity through it’s highly secure and reliable data centers across Southeast Michigan. With a full range of colocation, dedicated server and managed service options, industry leaders trust Online Tech to ensure their servers are always on, always online, and always safe.

9. End Notes

¹See <http://www.hipaadvisory.com/regs/HIPAAprimer.htm> for a good primer on HIPAA.

²See <http://www.sarbanes-oxley-forum.com/> for a comprehensive online forum.

³See Online Tech's white paper Internet Delivery Stack, available at www.onlinetech.net/library.aspx