AUCIT

SILOS

Silo is a management system incapable of reciprocal operation with other related management systems. With department specialization came a silo operational culture for many large organizations, especially with the government, which I can speak comfortable, since I worked for the Government of this country, [At NASA – National Aeronautics and Space Administration – GISS – Goddard Institute for Space Studies] and overseas for more than 20 years. The silo effect is characterized by a lack of communication or common goals between departments in an organization. A bank's management system, for example, is considered a silo if it cannot exchange information with other related systems within its own organization, or with the management systems of its customers, vendors or business partners. "Information silo" is a pejorative expression that is useful for describing the absence of operational reciprocity.

From a technology viewpoint, information silos are managed by computer systems that do not provide efficient machine communication systems to other computers. In this view, "silo technologies" limit what software developers can do, and are the reason organizations must employ middleware and web services to overcome the limitations of disparate systems. While effective for addressing specific needs, middleware and web services are considered stopgap measures because they must be applied on a case-by-case basis and cannot achieve business process interoperability among all disparate management systems worldwide.

Silo technologies restrict the capabilities of the applications which manage much of the world's structured information. Databases are the time-tested way of storing, using and safeguarding vital enterprise business procedures and data. Most of every organization's computerized information is controlled by database applications, including all the "back end" data on the web.

Storage Tek Silo used at NASA-GISS

They're everywhere—those invisible but oh-so-destructive barriers that can loom between functions in an institution.[1]

Often called silos, these barriers can elicit numerous nasty behaviors—including function leaders' unwillingness to communicate, share information, or collaborate with each other, and their tendency to scuffle over scarce resources.

The Dark Side of Silos

Silos between an institution's PR function and other functions can be particularly damaging. For example, in many institutions, management asks PR to operate in a vacuum. PR's goal is to come up with new offerings without considering their cost or market demand. Management often rationalizes this approach by saying that it does not want to constrain creativity. But without input from the IR staff, PR risks creating products/service that fall flat in the educational marketplace because costumers don't care about the features and benefits they offer.
Busting the silos between IT and other functions isn't easy. But the following five tactics can help.

1. Focus your colleagues' attention on the customer

Help managers from other functions understand what customers want from our institution. Then explain to them what happens when customers don't get what they want because different parts of our institution aren't collaborating.

For example:

"Customers want to tell us about their problem only once—not over and over again as we hand them off from one department to another because our [*example only]* registrar office-processing and customer-service teams aren't talking to each other.

2. Use technology to sharpen customer focus

We must use our institution's customer relationship management (CRM) technology to sharpen our institution's focus on the customer. For example, carefully analyze the data in our CRM system. Then use that data to show our colleagues:

- How customers are making their decisions
- What touch points they're interacting with as they do business with our institution
- What problems they're running into at each touch point
- How much those problems are costing our institution.

For instance: [*example only, but it can be elaborated*]

"Our system is showing that we're extremely inefficient with your Registration/Recruitment processes. Delays and errors are increasing our operational expenses by 3% and driving 5% of our customers away every year. That translates into revenue losses of $200,000 to $440,000."[2]

[1] Internet article, [Wiley, 2006]
[2] Numbers are based in an hypothetical 400 student/enrollment at $22K each

3. Regularly network with colleagues

Foster mutual understanding of one another's biggest challenges and priorities by regularly networking with colleagues. As often as possible, meet informally with your counterparts in PR, IR, FA, BUS, IT, HR, and other functions. Find out what these peer managers' most pressing on-the-job difficulties are. Share similar information with them about your own department's challenges.

Steady networking is valuable for several reasons:

- It gives all participants a **wider view of the institution** and generates insights into how you can help each other.
- It enables function leaders to **gain familiarity with each other's skills and expertise**. Once you're aware of what each of you brings to the institution, you can draw on one another's abilities to solve cross-functional problems.
- It helps us **identify and break down silos**. For example, suppose you're having lunch with the head of your institution's academic affairs, and he/she mentions how the lack of registration online, closing of pivotal courses are jeopardizing his/hers enrollment possibilities. You could start breaking down this silo by helping to devise an acceptable plan of action online registration and make available different certification programs. [*example: Microsoft Certification, Intuit Certification*][3]
- It gives you the chance to **win your colleagues' support for marketing strategies**. Whenever you network with managers from other functions, take the opportunity to get their input on ideas you have percolating for new marketing initiatives. Get their thoughts about how a particular program might affect them and what cross-functional implementation challenges it might raise.

By inviting peers' input early, you boost your chances of winning their support for your idea. And you learn more about how activities initiated in the marketing department can affect other parts of the institution.

4. Seek out cross-functional teams

Cross-functional teams contain at least four members from diverse functions— recruitment/enrollment, marketing, finance, operations, IT, and so forth—all of them working together on a special project with a common goal and time deadline. For example, people from marketing and product development might form a team focused on creating a specific new offering that marketing has determined customers want.

Because a cross-functional team's work depends on input from several functions, collaboration is essential. When led properly, such teams leverage their members' diverse knowledge and expertise to accomplish vital objectives quickly and flexibly. But in many institutions, marketing's participation in such teams is sketchy—possibly owing to underestimation of marketing's value on the part of managers in other functions.

How to combat these perceptions? Do whatever it takes to identify and seize cross-functional opportunities. And once you're on a cross-functional team, demonstrate productive team behavior.

For example, ease the conflict that can arise in a team whose members bring diverse expertise and viewpoints to the project. An operations manager, for instance, may want the most efficient production system possible, while you want the right mix of products/service available at the right time, even if that means short production/service runs and/or men-power.

[3] This program is being in development phase at AUC

You can help resolve this conflict by understanding that if your institution's enrollment/retention is inefficient, costs will rise and margins will suffer or prices will have to go up. You can also help the operations manager understand that if the product/service isn't available, customers will go elsewhere—which affects the institution's overall budget.

Look for opportunities to compromise or to come up with a "third way" to solve such impasses. And keep everyone focused on the higher-level goal: **to make money by satisfying customers**.

5. Encourage job shadowing

Spend time in other parts of your institution; observe how your peers do their jobs—even perform some of their duties. Encourage your colleagues from other functions to do the same in your department.

By engaging in mutual job shadowing, you deepen your understanding of one another's view of the institution and uncover additional ideas for collaborating on common problems. You also gain further opportunities to stress the importance of articulating and satisfying customers' needs.

Some institutions make job shadowing a required practice. Take Intuit. This maker of the renowned Quicken/QuickBooks accounting application required its programmers to spend time working at the help desk. The programmers heard users' concerns and were better positioned to program the software in ways that avoided creating problems for customers.

Silo Busting Pays Off—for Us and Our Institution

Silo-busting swiftly wins you a reputation as a Marketing Champion. Why? When we help break down silos between IT and other functions in our institution, managers stop hoarding their power and knowledge and start sharing it. This cross-boundary collaboration ratchets up the institution's power to better serve its customers, which translates directly into profits!

And that's a payoff that everyone can appreciate—no matter where in the institution they work.

Breaking Silos at AUC

Institution leadership is made up of many individual parts. Though they need to work together, they aren't typically very good at it

We are:

- Department –Divided: [and this frustrates any management for the compartmentalization of AUC functions and departments that often keeps them separated. This is a problem not just at AUC, but in other institutions where the sheer size and/or dysfunction of the place institutionally segregate departments who regularly need to or at least should be working together].
- There's no cross-communication: [and when it comes to projects that can benefit from inter-departmental collaboration like creating a new program that would benefit student, faculty and staff alike, the separation can affect the quality of the outcome. This is very frustrating and limiting.
- The lack of interaction: [We must design a strategic plan with fellow administrators where all the department managers can work together on the same strategic page. Without STARS….. This

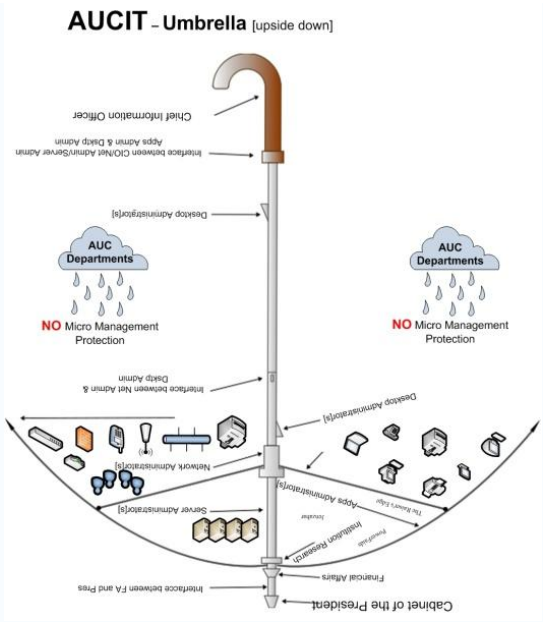
will broaden the scope of what each individual department does and recast those separate roles into one holistic vision.

WHAT AUCIT BELIEVE:

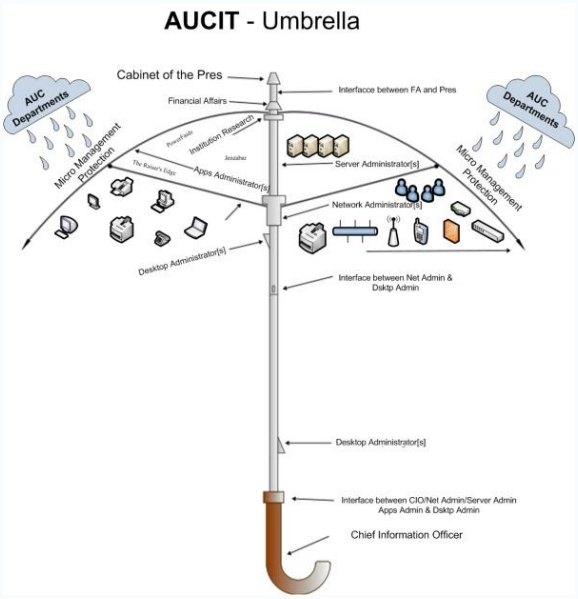
AUCIT believes that under the umbrella of Information Technology Department, these different Silos [Network Administrators, System Administrator, Application Administrator and Desktop Administrator, must get their different functions to work together for sharing data and forecasts. Our strong answers to eliminating siloed behavior in the AUCIT lies in abolishing the existent functional walls that exist between the different IT functions, and between internal departments. And most important of all: keep those four silos under the AUCIT Umbrella.

[*See graphics next page*]

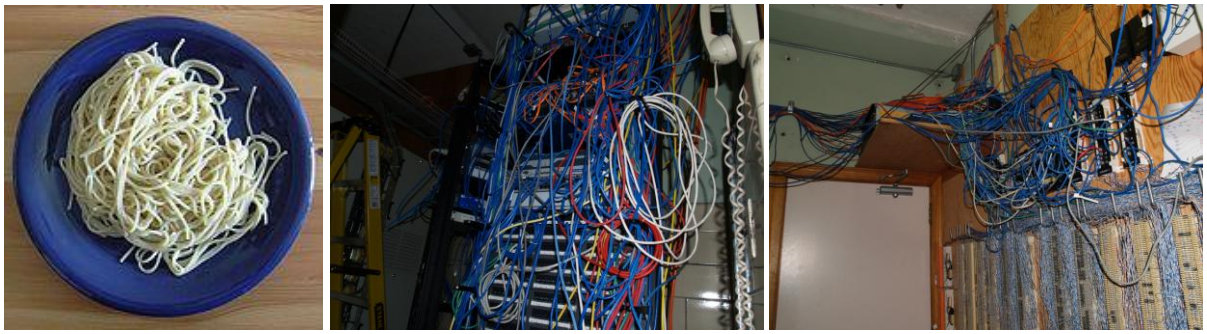
TODAY



Recommended [strongly] by AUCIT



The results of an Upside down AUCIT Umbrella:



This is a sample of what we have here at AUC today, which is changing dramatically in the last 2-years period.

- Spaghetti Network,
- Spaghetti Code and
- Spaghetti procedures…. etc…

Example of spaghetti network: see our PBX room.

Example of spaghetti code: [Basic]: use of SQL statements to generate reports excel and save it in .PDF format.

Example of Spaghetti Code:

- The **program** prints the numbers 1 to 10 to the screen along with their square. Notice that indentation is not needed and that the program's GOTO statements create a reliance on line numbers. Also observe the unpredictable way the flow of execution jumps from one area to

another. Real-world occurrences of spaghetti code are more complex and can add greatly to a program's maintenance costs.

```
10 i = 0
20 i = i + 1
30 PRINT i; " squared = "; i * iDocument2

40 IF i >= 10 THEN GOTO 60
50 GOTO 20
60 PRINT "Program Completed."
70 END
```

Same code written in a structured programming style:

```
FOR i = 1 TO 10
   PRINT i; " squared = "; i * i
NEXT i
PRINT "Program Completed."
END
```

The program jumps from one area to another but this jumping is predictable and formal. This is because using for loops and functions are standard ways of providing flow control whereas the *goto* statement encourages arbitrary flow control. Though this example is small, real world programs are composed of many lines of code and are difficult to maintain when written in a spaghetti code fashion.

Forget the Silos – Build the Interfaces

Fast Forward

- The AUC's departments borrows IT technologies, but often sees the IT department as its opponent
- The IT department misunderstands the needs of the AUC's Departments needs causing considerable friction.
- Taking steps to resolve conflict is the responsibility of IT management and Institution's management.

Over the past 10 to 15 years, the industrial controls (IC) world has borrowed substantially from the world of information technologies (IT), and not only that but all lines of businesses.

Protocols like Ethernet and TCP/IP and operating systems such as Windows and Linux have made the interfacing of industrial control equipment much easier, but now there is significantly less isolation from the outside world. Data processing is no longer restricted to the huge Glassy data-centers, where all the users/customers/business resourced to provide all their IT needs, but in every desktop we have a potential super-computer [in terms of computing power] if we compare with the super-computers of 10 to 15 years ago. [Don't believe me? Ask yourself what kind machine you have in your desk today]

Network security problems previously only seen in the business network and the world at large now can be passed onto process and supervisory control and data acquisition (SCADA)[4] networks. I experienced it while working at NASA/GISS [National Aeronautics and Space Administration/Goddard Institute for Space Studies, in NY, and then as a consultant for the Electric Facility for the State of Nebraska, putting industrial production and human safety at risk.

Similarly, network security incidents on the plant floor can travel back up into the corporate environment, creating the possibility of considerable business disruption.

At the same time, a core of our information infrastructure—the network—has come under increasing attack from a wide variety of sources, ranging from teenagers on a cyber joyride to professional hackers.

A classic example is the impact of the Slammer Worm on the electrical generation infrastructure in January 2003. While we are aware of a number of incidents, one of the cases reported by the North American Electric Reliability Council illustrates the issues:

"A server on the control center LAN (local area network) running SQL was not patched. The worm did not reach the server via the organization's connection to the Internet. It did apparently migrate through the corporate networks until it finally reached the critical SCADA network via a remote computer through a VPN (virtual private network) connection. The worm propagated, blocking SCADA traffic."

Here we have a worm designed to attack a business application (SQL-Server) and propagated over a non-control media (the Internet) impacting a critical SCADA system because:

a) IT products like SQL-Server have become an integral part of the plant floor.

b) A close coupling of Internet, business, and control networks now exists.

In themselves, these two conditions are not bad—the shared components, protocols, and manufacturers have created greater synergy, lower costs, and free access to information for both IT and IC members. However, without improved security practices on all sides, the price for these gains may be unacceptable high.

[4] Supervisory Control And Data Acquisition – heavily used in the Government

Where does one start when attempting to improve the security of the network from these threats from outside world? We believe the only technique with a high chance of success is a highly coordinated effort by both IT, and all the other departments, and this document will look and address techniques that can make this possible.

Blaming the wrong people

The ultimate goal of improved security is a shared goal, menace is a combined threat to all, and most of the technologies are common technologies. Thus, it is reasonable to have a harmonized IT/IR/FA/BUS/HR/ED, and defense is appropriate.

Unfortunately, this is often the exception rather than the rule. As I have worked in different segments of the industry in the US, I have seen a wide range in the attitudes and level of cooperation between the organizations as whole and IT departments.

It seems that we are drawn back into a war of all against all, and if not all, then all perceived "enemies", but until when? Today it is Fin Aid against AUCIT, IR and/or BizOffice against AUCIT, and tomorrow who will it be? In the state of nature[5] there are finally no friends.

In the Brazilian Military we used this corollary in the logic of anticipatory self-defense, "the preventive war strategy relies on long-term prediction and a presumed concatenation of events far less certain than those appealed to by the immediate logic of self-defense." By shooting first and asking question later, it opens the ways to tragic miscalculations. Lots of people and/or organizations are still using these same principles.[6]

In the Soccer arena, especially in Brazil, where I can speak "ex cathedra", we used it intensively and extensively in the 50's to the 70's. Until the world learned what we were doing and then they copied us, with reasonable success. And we experienced a long drought-out period for worldwide titles for more than 20 years. Finally in 1994 we recovered the worldwide hegemony.

What was it; that rest of the world didn't have? Simple… we applied to the soccer the military principles I described above: "The best defense is to have lethal attack". Yes, we succeed for more than 25 years… and yes, if you scored one goal against us we would attack you merciless and would score two, three, or more times. Once the world learned what we were doing, they stopped us very easily. Worse yet, because we didn't have a defense that was well structured, we experienced humiliating defeats from teams much more technically inferior than us, or so we thought.

The common enemy

Blaming each other for who does what, and security issues is missing the point—the enemy is not the other department, but the hacker or virus attempting to infiltrate the institution systems.

[5] **State of Nature** - The "natural condition of mankind" is what would exist if there were no government, no civilization, no laws, and no common power to restrain human nature. The state of nature is a "war of all against all," in which human beings constantly seek to destroy each other in an incessant pursuit for power. Life in the state of nature is "nasty, brutish and short."

[6] See slide presentation distributed with this document

It is easy to point the finger at the other business unit for security issues, but it is certainly not helpful in reducing the risk. The existence of numerous common technologies means the enemy is not unique to either the other departments or IT environments; it is a common and shared adversary.

For example, a Denial of Service (DoS) attack against a file server is likely to be just as devastating against the JZweb and or Jenzabar at IT floor.

Similarly, a poorly configured wireless network is a security risk whether it links to the president's laptop or the desktop computer of a maintenance worker.

Furthermore, regardless if security incidents are the result of ignorance or intentional acts, the basic outcome is the same—potential loss to the institution that can affect everyone.

What to Do? - Building Interfaces, not Silos - [they already are here]

There are plenty of examples in the industry of what can go wrong in IT/departments security cooperation and of the subsequent consequences.

What is it that makes the difference between an open interface versus two or three silos in terms of IT/IR/BUS security cooperation?

To help answer this question, we researched the Internet, visited old documents from past experiences in the past, consulted with experts representing process control industries that included, electric, utilities, hospitality, governments and others. The roles of the people we spoken with, ranged from trades people to executive directors working in both IT and Process Control departments.

Some of the people spoke about the involvement of their senior leadership team and how this has been instrumental in creating trust between people and departments.

Over time, I believe this culture can and will contribute to producing positive bottom-line results.

One company has had significant success in building interfaces between the IT and Process Automation groups. One automation group supervisor at a large electrical plant facility, noted that as far as communication and cooperation was concerned, staff at the local levels had enjoyed a relatively good level of this because they worked together daily. People knew each other, and there was a trust built up between them. Unfortunately, at the city level, getting the same degree of interaction between different departments was more difficult.

Top city management recognized the need for better communication and cooperation at the city level between IT and process control groups in order to protect the business. With that important goal in mind, they launched a pilot meeting to bring the two groups together in the same room, at the same time, to focus on this single important issue.

However, while the subject matter was the main focus for the meeting, he stated, "We took time to learn about each other's needs and to also get to know each other. We could put a face to a name or a voice. Once we had this, we were able to sit down to educate and influence each other. There was a tremendous amount of positive discussion as we started to see each other's world."

One of the tangible outcomes from that meeting was a commitment by the groups to collaborate to improve the business. The first project was jointly developing policies and standards. Because of the first meeting, a culture of cooperation between the groups has continued to develop.

We have an informal saying here. There is no hole in just our end of the boat.

To make the partnership between all departments and IT work, senior leaders at this institution need to recognize that there is a need to invest in relationship building. We as a team must look for solutions that would create the framework for sustaining a culture of cooperation.

There are three foundational values that contribute to create a working platform between IT and other departments. There must be shared vision, shared power, and shared accountability.

There is no formal way of measuring success, but it is easily seen in the behaviors of the people. The real problems between IT and different groups are not about re-assigning people or re-structuring but about culture, behaviors, and people's individual points of view.

Not all disconnects between IT and the rest are the result of conflict and tension. They can also come from 'innocent' mistakes.

Do We Need Senior Leadership?

Does IT Maters?

For the first question I would say:

No Leader Rides Alone

Not everyone recognizes that those closest to you will make or break you. There are still leaders who hold up the Lone Ranger as their model for leadership. One of the best illustrations of how unrealistic that ideal of leadership really is can be found in "American Spirit" by Lawrence Miller:

> Problems are always solved in the same way. The Lone Ranger and his faithful Indian companion … come riding into town. The Lone Ranger, with his mask and mysterious identity, background, and lifestyle, never becomes intimate with those whom he will help. His power is partly in his mystique. Within ten minutes the Lone Ranger has understood the problem, identified who the bad guys are, and has set out to catch them. He quickly outwits the bad guys, draws his gun, and has them behind bars. And then there was always that wonderful scene at the end [where] the helpless victims are standing in front of their ranch or in the town square marveling at how wonderful it is now that they have been saved. [7]

No Way! There is no such thing. If you're alone, you're not leading anybody, are you?

More to it…

When people respect you as a person, they admire you.

When they respect you as a friend, they love you.

When they respect you as a leader they follow you.

Dictators and other autocratic leaders rely on violence, intimidation, and fear to get people to do what they want. That's not really leadership. In contrast, good leaders rely on respect. They understand that all leadership is voluntary. When leaders show respect for others – especially for people who have less power or a lower position than theirs – they gain respect from others. And people want to follow people they respect greatly.

[7] Maxwell, John C. , " The 21 Irrefutable Laws of Leadership" [2007]

I would go farther in saying that when it comes to identifying a real leader, that task could be much easier accomplished if we:

- Don't listen to the claims of the person professing to be the leader.
- Don't' examine his credentials.
- Don't check is title, but…
- Check his influence [and I am not saying here influence of power, but the power of the influence]

The proof of leadership is found in the followers.

In the country of Brazil, in the late 60's yearly 70's, a special candy was sold in the stores that took the youth by frenzy: It was a very well orchestrate marketing campaign where each candy was wrapped in a paper that spoke about love. On the outside of the wrapping it said: " LOVE IS…" and when you unwrapped the candy it would complement the sentence, saying… Love is to care about…, or Love is to be kind… etc!

I will use it to illustrate the profile of the leadership we ought to have:

LEADERSHIP IS…

CHARACTER – Who They Are

True leadership always begins with the inner person. That's why someone like Billy Graham is able to draw more and more follower to him as time goes by.

RELATIONSHIPS – Who They Know

You're a leader only if you have followers, and that always requires the development of relationships – the deeper the relationships, the stronger the potential for leadership.

KNOWLEDGE – What They Know

Information is vital to a leader. You need a grasp of the facts, and understanding the dynamic factors and timing, and a vision for the future. Knowledge alone won't make someone a leader, but without knowledge, no one can become a leader.

INTUITION – What They Feel

Leadership requires more than just a command of data. It demands an ability to deal with numerous intangibles. In fact, that is often one the main differences between managers and leaders. Leaders seek to recognize and influence intangibles such as energy, morale, timing and momentum.

EXPERIENCE – Where They Have Been

The greater the challenges you have faced as a leader in the past, the more likely followers are to give you a chance in the present. Experience does not guarantee credibility, but it encourages people to give you a change to prove that you are capable.

PAST SUCCESS – What They Have Done

Nothing speaks to follower like a good track record.

ABILITY – What They Can Do

The bottom line for followers is what a leader is capable of doing. Followers want to know their leader can lead the team to victory. As soon as they no longer believe you can deliver, they will stop listening and following.

There must be a top down approval at the institution level that makes sense and allows for implementations; otherwise there will be no successes without this level of support.

If our institution is looking to make headway, there are several suggestions to consider:

- Conduct annual staff surveys that measure elements of cooperation between the groups such as utilization of resources, trust and conflict, clarity of goals and objectives, controls and procedures, and the like.
- Develop cross-department training programs that focus on values and behaviors expected in order to foster a culture of co-operation and communication. [i.e. QuickBooks training, Microsoft MOAC[8] training for faculty and staff, re-training in Jenzabar, etc…]
- As part of a formal talent management program, place high talent performers in the various departments. Most successful leaders are those who have worked both sides of the fence. This can also be a design element for a college graduate after entering the organization.
- Create cross-functional teams to work on developing policies, standards, projects, etc. Imbedded in this is metrics for both completing projects and for the quality of collaboration used to develop and execute the project.
- Informal networks are important. In the context of a real problem, create opportunities for people from the different departments to network and work together.
- Leadership by example, after all people do what people see.
- We must apply or be willing to use The Law of Legacy, where a leader's lasting value is measured by succession. What will people say at our funeral? The thing they say tomorrow depend on how we live today using The Law of Legacy.
- We must realize that improvement is impossible without change.
- We must follow The Law of Intuition – which states: whenever leaders face a problem, they automatically measure it – and begin solving it.
- Finally, there is something each one of us can do to improve and maintain effective relationships. Be willing to make the effort to reach out to the other side and be willing to walk in their shoes.

Conclusion:

Trust is ultimately the crucial factor in creating great working relationships.

Conflict and misunderstandings are a part of life and a part of working together. Taking the first steps to resolving conflict is ultimately the responsibility of the leadership.

Dr. Freeman A. Hrabowski, III, president of Maryland County University said: "All institutions have their "F&!*^#A?" but they are needed to help us to improve. But also he said of the leadership in education in this nation: "They will be judged for the importance they give to their IT department in their Institutions." And one of the most important statements I have ever heard came from his mouth, that I would like it had come from mine: "Think what you going to say, and then make sure you do it, because it eventually will turn to be a habit, that will mold your character that eventually will determine your destiny."

[8] Programs under development where we can train our faculty and staff on Microsoft Official Application Certification program

DP, Vice Chancellor for IT at LLU said: “You always will have stupidity to deal with. If you want to be a leader in the IT, so then learn how to deal with it.”

I say: “The two most common errors in IT are coded as: “**ID10T**” & **PEBKAC**. We must work around it. Thru it. Over it. Under it. But not “with” it.

Oh, yes… you may be wonder if I forgot to answer the second question: Does IT Matter? Of course it does [this is embedded in my conclusion.

-

Ademir Soares, Chief Information Officer
Atlantic Union College

References

Maxwell, John C.; " The 21 Irrefutable Laws of Leadership" [2007]

Maxwell, John C.; " The 21 Indispensable Qualities of A Leader" [1999]

Barber, Benjamin R; " Fear's Empire" [2003]

Maxwell, John C.; "Leadership 101" [2002]