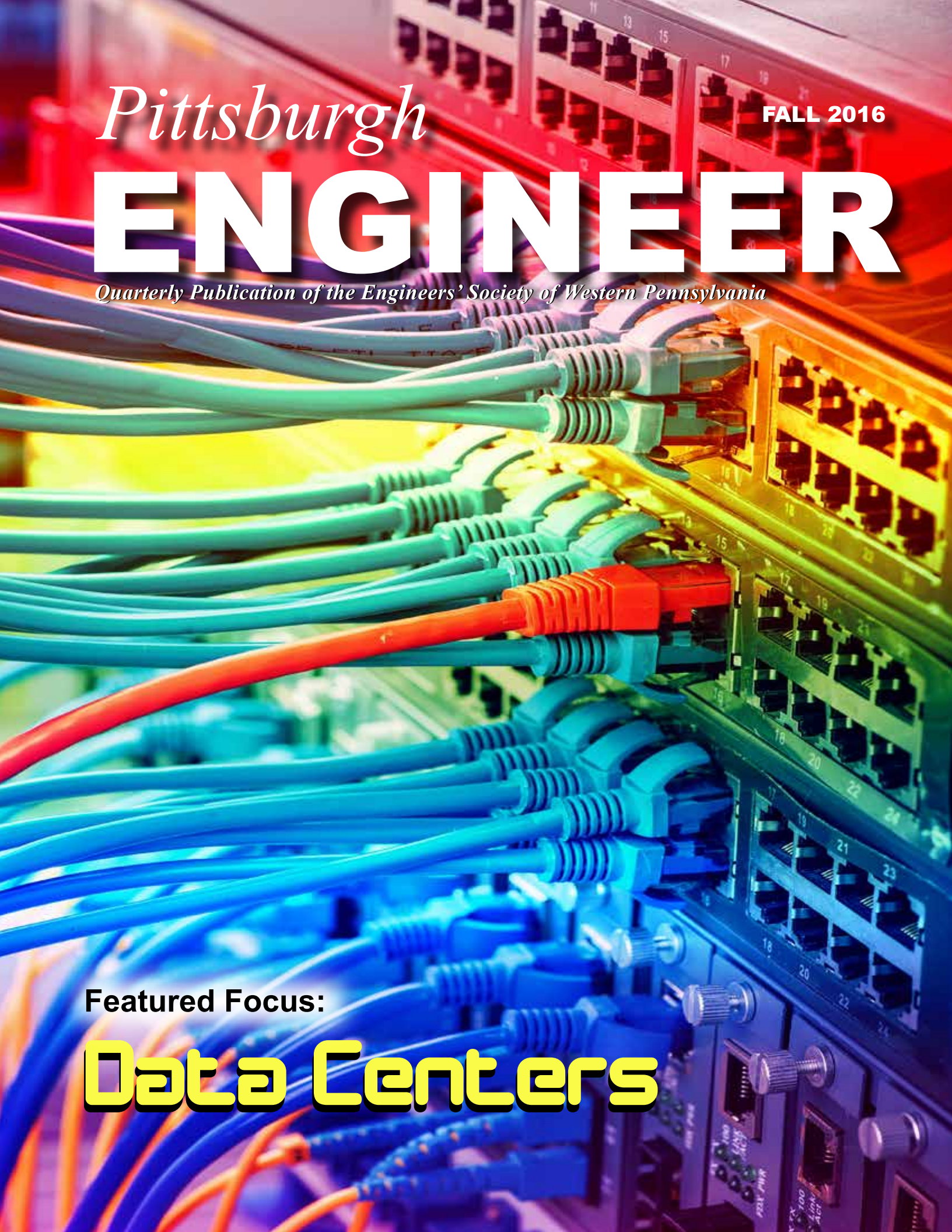


Pittsburgh ENGINEER

FALL 2016

Quarterly Publication of the Engineers' Society of Western Pennsylvania

Featured Focus:

Data Centers

Providing a full continuum of cybersecurity services

Our cybersecurity analysts develop vulnerability assessments and evaluations to defend our clients against cyber intrusions.

Aviation • Banking and Finance • Chemical Facilities • Commercial Dams • Electric • Government Facilities • Nuclear • Oil and Gas • Shipping Transportation • Water & Water Distribution Facilities

Jim Katsafanas, P.E., PTOE, Intelligent Transportation Systems Practice Lead • (412) 269-4635
Mark E. Bodily, Program Manager of Cybersecurity and Information Security • (208) 535-8247

MBAKERINTL.COM

Pittsburgh **FALL 2016**
ENGINEER
Quarterly Publication of the Engineers' Society of Western Pennsylvania

In this issue...

ENGINEERS' SOCIETY of WESTERN PENNSYLVANIA

Pittsburgh Engineers' Building
337 Fourth Avenue
Pittsburgh, PA 15222
P:412-261-0710•F:412-261-1606•E:eswp@eswp.com•W:eswp.com

Guest Editors Column

By Jim Shaw

Data Centers, Own or Outsource?

Does it make sense for a company to own and operate its own data center? It depends. Owning and operating one's own data center gives a business entity complete control over the asset—but it can be an expensive, complex, and risky proposition. Most companies are finding it hard to justify the continuous capital expenditure necessary to maintain a secure and stable datacenter facility.

A data center is a dynamic environment. Over time, hardware continues to shrink in size, possibly freeing up valuable space, but the amount of power and cooling required steadily increases. The problem may be temporarily alleviated by upgrading the electrical and cooling infrastructure, but it is more likely that the capital expended to do so would become nothing more than a sunk cost. As data volume and processing increases, it is inevitable that this upgrading exercise would need to be frequently repeated. An owner must be willing and prepared to take on this challenge. At what point does the company put an end to this madness?

Outsourcing is an option, but in most circumstances, outsourcing should not be an all-or-nothing endeavor. After qualified outsourcers, including cloud providers, have been identified, companies should decide what can be outsourced. To start the process, identify low-risk systems or projects, such as testing and development environments, legacy equipment, or disaster recovery systems. Conducting the outsourcing on an incremental basis provides a means to thoroughly test the outsourcer and to build a trusting relationship over time. As confidence is established, additional projects can be moved.

Ultimately, the risk of owning a data center has been minimized by diversifying computer resources across multiple entities. By moving equipment to the outsourcer, data center space and infrastructure have been reclaimed, which extends the life of the current center, while simultaneously eliminating the need to build or expand.

Too often companies make the mistake of moving their equipment to an outsourced data center and then experiencing the "out of sight, out of mind" problem. Like any outsourced solution, a relationship with a data center provider must be carefully managed and grown over time.

In an environment that requires an unlimited ability for growth and where risks and costs need to be minimized, a well-managed and trusted outsourcing relationship provides the near-perfect solution.

Jim Shaw

Jim Shaw is Chief Information Officer and Senior Vice President of Management Science Associates. Jim has over 35 years of IT experience, with the last 15 as Chief Information Officer and Senior Vice President for Pittsburgh based Management Science Associates, Inc. (MSA). Although Jim has experience in systems and software development, his main area of expertise is IT infrastructure. Jim's IT Team not only supplies IT infrastructure and data center services to MSA's internal business divisions, they also service many Pittsburgh area firms. Currently, MSA owns and manages two data centers and leases data center space in three other locations. In 2010, Jim was awarded The Pittsburgh Technology Council's CIO of the Year in the Enterprise category. Jim attended the University of Pittsburgh where he holds BA, BSIS and MSIS degrees. He is originally from Pittsburgh, but now resides in Indiana County, PA

Intro To Data Centers: A CLOUD'S SILVER LINING?

Data Centers

By: Suresh C. Ramanathan

Betting on a Cloud?

New industries have to adopt new meanings for old words or invent new words to introduce new concepts and changes in paradigm. But to choose a white fluffy aerosol Cloud to convey the concept of stability, scalability and security seems ludicrous until you start understanding the image it is meant to convey to the business user. It is the very ephemeral nature is used to convey that you don't have to worry about where it is or even what it is but it will support your changing business needs when and where you need it.

For the engineer in us, the National Institute of Science and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." There is not a single mention of data centers in that definition.

Evolution of Data Centers

Data Centers used to be the computer room, or a department (as defined by Gartner Group at one point) that managed a large group of networked computers used by organizations for the storage, processing or distribution of large amounts of data. Then Data Centers evolved to be the large physical building that included the outer shell and the raised flooring for the cooling required, all of the IT equipment, the electrical infrastructure to support the IT equipment, the cooling infrastructure to manage the heat generated and the communication and energy requirements that have to be managed to support the data center operations. As the capital investment increased, these became the investments of large corporations and third-parties who in turn leased access to facilities and equipment to others that needed it.

"Organizations may not ever make an investment in data centers and all of the related equipment and hardware, but they may buy access to these assets on an as-needed basis"

Data Centers Obsolescence?

To leverage the benefits of scale and increase efficiencies, multiple trends happened. One of them was virtualization, which means "using software to partition servers" so that the existing investments can be further leveraged. Gartner further identifies and defines a Software Defined Data Center as "a data center in which all of the infrastructure is virtualized and delivered as-a-service." All the same, behind every virtual software defined data center there will be one or more data center or centers. But the users of these data centers may not know which physical data centers, equipment, or perhaps even the vendor(s) associated with those centers. All that may be "clouded" from the end-user, who may be paying based on what they are using.

Peering into the Cloud

Now that we have established that the cloud is not soft and fluffy but has a physical layer that someone else will own and you as an user or business owner may not care about. This physical layer will contain all the building(s), the equipment including but not limited to servers, storage, and network components, and all of the cooling, energy and mechanical components required to the support the attributes required by the abstraction layer. The abstraction layer is the software layer that lies on top of the physical layer ranging from operating systems to applications and related tools. The abstraction layer is where the concept of cloud evolves from as at this point the user or the business owner is more interested in the attributes of the abstraction layer rather than where the physical layer exists or that it even exists. However, there are specific expectations of the cloud ranging from security, scalability, availability and redundancy to elasticity and measured service.

Build, Buy or Operate?

Most organizations may not ever make an investment in data centers and all of the related equipment and hardware, but they may buy access to these assets on an as-needed basis.

However they may buy or rent cloud computing services in the following ways:

X as a Service	What They Buy / Rent	What They Will Own / Manage
Infrastructure as a Service (IaaS or IaS)	The physical layer	The abstraction layer from the operating system up. They may have some leverage on the choice of hardware
Platform as a Service (PaaS or PaS)	The entire physical layer, Parts of the abstraction layer from the operating system and some fundamental services	The application parts of the abstraction layer and perhaps some of the related configuration
Software as a Service (Saas or Sas)	The entire physical and most, if not all of the abstraction layer	Some of the configuration related to the unique business requirements and the data of the business

Cumulus, Cirrus, Stratus... there's more?

The NIST recognizes four types of deployments of the cloud. These can also be viewed as strategies of usage and ownership.

Private Cloud

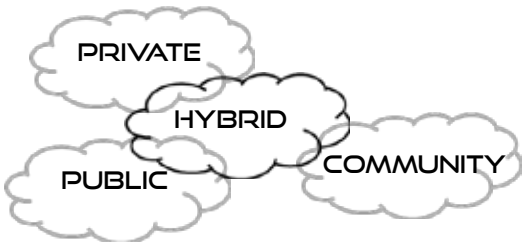
A private cloud is owned by a given organizational entity for the purposes of its own exclusive ownership and those of its business units and subsidiaries. Traditionally this has been the ownership model for data centers and a lot of organizations prefer the control and security benefits of this model. This model does not have to be owned by the organization, but it may have to pay a premium for an exclusive use. Further, the organization may trade off the benefits of flexibility and costs for perceived benefits of security and control. Private clouds are usually the domain of large organizations; increasingly, medium and small organizations are veering away from this option.

A private cloud could be on-premise (a traditional data center evolution with additional virtualization) or off-premise. The off-premises, or "hosted model" again offers infrastructure-as-a-service, or the platform-as-a-service model. These private cloud offerings are common with companies like Amazon, or organizations who make an investment in infrastructure, then manage it, or have a third-party manage it for them.

Public Cloud

A public cloud is usually designed and operated by an organization for the use of external organizations, entities, or even individuals.

In a Public Cloud model, Platform-as-a-Service, and Software-as-a-Service are the common service models as these are more standard offerings, and therefore the most cost effective models. Google AppEngine and Force.com are



good examples of a Platform-as-a-Service, while SalesForce.com is a good example of Software-as-a-Service.

Amazon's Elastic Compute Cloud (EC2), IBM's Blue Cloud, and Windows Azure are other examples in this public domain. Here the investment and operational costs are borne by the owner of the assets, but various service offerings and usage models exist. The security, availability, service level offerings and other criteria are controlled and managed by the public cloud operator. Since the costs are shared across numerous users and there is a level of standardization at the physical and abstraction layers, the overall operational costs are lower and therefore offer potential cost-effective options for most organizations.

Community Cloud

A community cloud is one where organizations belonging to a particular group that has a shared mission, security requirements, policy requirements or compliance considerations come together to share a hosted environment. The actual ownership of the hosted environment may be shared or owned by a given entity, and the costs shared using a predetermined model. Organizations with a given industry – say finance or accounting – or agencies within a common location, may share a community cloud. A community cloud could be viewed as a private cloud limited to the organizations that are allowed to leverage it. All of the ownership models seen under the private cloud model could apply here as well.

Hybrid Cloud

As the name suggests, in a hybrid cloud model, one or more of the distinct cloud infrastructures (private, public or community) are used based on the needs of a given organization. The hybrid model may serve as a very pragmatic and strategic initiative for an organization that has to balance the various needs even as the cloud offerings mature and

evolve. Each of the components of the hybrid strategy will remain separate and distinct, but they may be brought together by standards and certain technologies. An evolved hybrid cloud may seek to have data and application portability that may bring about functional and technical benefits. Hybrid clouds could also allow load balancing, disaster recovery and other event-driven initiatives across the heterogeneous clouds. Challenges of this hybrid approach is the degree of standardization and the lack of compatibilities across various cloud entities.


Exterior view of Facebook's Prineville, OR Data Center


Misting fans help provide proper humidity level for outside cooling air


Server racks inside Facebook's 350,000 square foot Data Center

Deciding Your Cloud or Data Center Strategy

Here are some questions for you to consider when selecting your cloud strategy:

1. What are the applications that you are using currently, and do they fulfill your current requirements?
2. Among the portfolio of business applications you use, how many are "off the shelf" and how many are custom developed applications?
3. Have you grown out of your current custom developed applications and considering other options?
4. How mature is your IT organization and how well do they currently support your existing applications?
5. Do you currently own your own data centers and do you mange them yourself?
6. What is the current IT spend on the data centers and any private cloud that you may have?
7. One a scale of 1-10, how responsive is your IT organization to operational and network related issues? Do you have many unplanned outages?
8. What is the age of your current infrastructure?
9. Do you have an established Disaster Recovery Plan? Do you have a current Business Continuity plan? When was the last time you tested these plans?
10. How important is cybersecurity to your business? How well do you manage cybersecurity today.

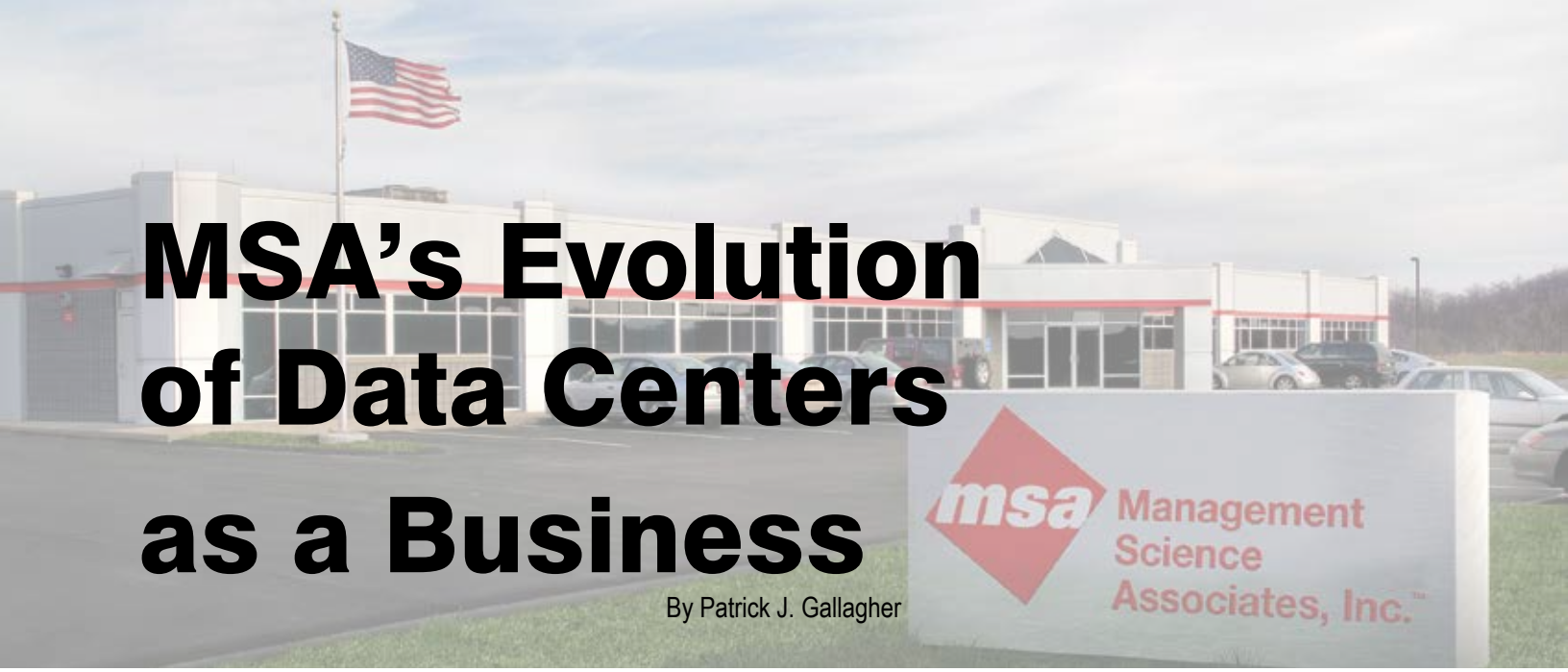
The Elite Cloud

Technology companies like Facebook, Google, Amazon, and Microsoft use their own data centers to manage the costs and to control the platform, where their software businesses are hosted. Most of these data centers consume a lot of energy that is both expensive and environmentally impactful as it creates a huge carbon foot print. Facebook had built a state-of-the-art data center in Prineville, Oregon and decided to publish its designs to help other companies become greener and to make hardware open source. With their innovative design they have reportedly saved $2 billion and they are now sharing the design and making the hardware open source. This is extremely new in the industry. They have established an organization called Open Compute project and their organizational membership is like "who's who" in the technology industry. This has already disrupted the hardware industry to a certain level and organizations like IBM have now joined this group.

Facebook evidently shuts down some of its data center to see how their software will behave and learn from that experience. They have developed an automated runbook to see how they can shut down a data center and bring it back up. They time themselves much like a pit crew on Daytona 500 would.

About the author...

Suresh C. Ramanathan is the President & CEO of KORYAK. Suresh left Deloitte Consulting to co-found KORYAK 16 years ago. He is the recently elected chair of South Western Pennsylvania Engineering Outreach (SPEO).
For more information, please visit www.koryak.com or phone toll free: 1-866-4KORYAK



MSA's Evolution of Data Centers as a Business

By Patrick J. Gallagher

In 1962, the Internal Revenue Service (IRS) found that Dr. Alfred Kuehn had paid 47 students as part- time contractors in 1960, and ruled that this activity was not "academic research", as Kuehn claimed, but was in fact a business. This led to the incorporation of Market Science Associates in 1963, and eventually a name change to Management Science Associates (MSA). At the time of the company's founding, Dr. Kuehn was a Professor at Carnegie Tech's Graduate School of Industrial Administration and head of its marketing faculty. Dr. Kuehn earned his MS and Ph.D. in Industrial Administration and a BS in Chemical Engineering from Carnegie Tech.

Dr. Kuehn's Chemical Engineering background, where one analyzes the effects of catalysts and other factors on the dynamics of a process, influenced his Ph.D. thesis and MSA's eventual products and services. The title of Dr. Kuehn's thesis was, "An Analysis of the Dynamics of Consumer Behavior and its Implications for Marketing Management". From its beginnings and continuing through today, MSA has relied on computers to study and manage new product introductions, develop forecasts and other types of models, and conduct related research for consumer packaged goods, media, life sciences, gaming, manufacturing and government.

The consistent underpinning of all of MSA's offerings is the use of computers and networks to formulate and answer the questions posed by clients. Often times, MSA needed to push the capabilities of the computers and operating systems available in terms of the use of disk space, accessing memory, quickly traversing large data sets for faster retrieval and other technical enhancements. This led the group to develop a variety of skills and knowledge of technology and how to get the most out of the equipment and systems. Well-known terms today like multi-dimensional database, data mining, online analytical processing (OLAP), business intelligence, and web-based reporting were already being used in operations at MSA long before the terms were popularized.

> When the MSA team introduced new equipment to the DR site, or tested failover procedures, the vendor would often comment, 'You guys do this really well.'

As the 1980s and 1990s progressed, MSA's success depended on computers and networking to provide solutions to its clients. A mid-1980s dial-up client-server system allowed clients to formulate a query on their internal PC, and when ready, connect to a MSA server through a dial-up modem. Once connected, the saved query would automatically be invoked. If the user had submitted a previous query, that retrieved dataset would be downloaded to the remote client PC for analysis. This system saved telephone charges for these dial-up clients by allowing the processing to be done remotely on the MSA servers while the client could disconnect.

MSA was an early adapter of using the Internet for internal and external purposes. MSA established commercial use of the MSA.com domain in 1992. Years later, when another Pittsburgh-based company with eerily similar initials tried to take away the domain name from Management Science Associates, the internet governing body ICANN (International Committee for the Assignment of Names & Numbers) denied the request, recognizing that Management Science Associates had established use of the domain name.

Through all of this time, MSA owned and operated their own data centers, supported by a knowledgeable team who expanded and pushed the ca-

pabilities of the equipment and systems. Understanding the value and importance of data, MSA established offsite storage of backups in the 1960s, initially in a home closet of a senior employee and then into secure climate-controlled mines around Pittsburgh. In the 1990s, MSA's customers started inquiring about MSA's processes and procedures revolving around their data centers and the handling of data. The clients recognized that the data and systems hosted by MSA were mission critical components of their business, and they wanted to ensure that good plans and procedures were in place for their protection.

For a short period of time, MSA did contract with a third-party group for business continuity and disaster recovery (DR). It became apparent very quickly to the MSA team that the knowledge and skill set of its internal groups was a match for the third-party company. When the MSA team introduced new equipment to the DR site, or tested failover procedures, the vendor would often comment, "You guys do this really well." During one test at the DR facility that encompassed interfacing with bar code scanners, an important input device for MSA at the time, the testing company was unable to correctly configure a box of dirty, second hand bar code scanners, even though the test had been planned for months. That event and other issues made the MSA team start considering alternative solutions to outsourcing the DR/BC capability. Ultimately, the leadership team of MSA's IT group generated a proposal to design and build a dedicated Business Continuity and Disaster Recovery Data Center. This proposal was submitted to MSA's Office of the Executive and was approved.

MSA's RockPointe Data Center

MSA's existing data centers were professionally run, secure centers, but as legacy facilities, they struggled with space issues and the ability to take advantage of recent advances in technology.

MSA's RockPointe Data Center opened in early 2002

In late 2000, MSA made the decision to design and build a state of the art disaster recovery center. The purpose of the facility was to provide a safe and secure environment for all of MSA's internal systems. In 2001, MSA purchased 30 acres in a Keystone Opportunity Zone location in West Deer Township, Pennsylvania that had recently been chartered. Tenants inside a Keystone Opportunity Zone are exempt from paying some state and local taxes for a 12-year period.


MSA's CIO Jim Shaw (left) and Chairman Dr. Alfred Kuehn (right) in the Data Center

During the design of the building, the IT Team recommended expanding the raised floor footprint of the building to account for potential new opportunities. A few modest inquiries to peers in the IT field in Western Pennsylvania indicated that there may well be additional opportunities for the data center beyond the support of the existing internal systems. The opportunity to expand MSA's offering to include data center services for external clients soon became a realty with the opening of the new RockPointe Data Center in early 2002.

MSA acted as its own General Contractor on this activity and engaged the services of a number of important vendors and local engineering firms. MSA's knowledge gleaned over 37 years of running innovative data centers was invaluable in designing and building this facility. To connect the new facility with MSA's corporate office and other local data centers, MSA extended DQE Communication's fiber network 18 miles to create a loop that serviced the RockPointe facility. MSA lights and manages its fiber segment.

The specific features of the RockPointe facility include:

- Service Organization Control (SOC 1) Type 2 audited facility
- 42,000 sq. ft. facility; 20,000 sq. ft. raised Data Center floor space
- Exceeds Tier III uptime standards of 99.98%
- Staff of 65+ network Engineers, Systems Administrators, Technicians
- Physical and electronic security and access control
- Dedicated fiber network; part of MSA's and local fiber networks
- State-of-the-art fire suppression systems
- Redundant electrical systems, including multiple generators in an (N + 1) configuration; 5x1MW diesel

generators
- 24x7 fully manned Command Center
- Redundant Internet connectivity
- Multiple communication providers
- Independent power substations
- Video conferencing
- DRs seats and equipment

Fiber Optic Network with MSA's facilities labeled

The build out of the fiber optic loop and the lighting of the fiber strands provided many advantages for MSA's internal and external customers. The ability to provide virtual data center services across two data centers, remote replication services for backups, and near real-time data backup are just a few examples of these advantages.

Evergreen Heights Technology Center

As MSA's cloud-based offerings and Disaster Recovery and Business Continuity business continued to grow, the decision to invest in a second hardened data center was made. MSA acquired a building on 10.67 acres in the North Hills of Pittsburgh in the Fall of 2010. The existing building had a data center in questionable condition. The MSA team was a little disconcerted when, on an initial visit during a rain storm, one of the data center operators was calmly walking around putting garbage cans and pails under some number of leaks inside the data center.

The renovation began with a replacement of the roof and the acquisition and installation of new AC units. Further upgrades occurred as legacy tenets lease agreements expired. These projects included a number of building infrastructure and asbestos abatement activities. Three of the major data center related projects included an excavation of a hill side to clear space for new generator pads, a complete gutting of the existing data center, a renovation of the entire second floor to accommodate the new expanded space, and the build out of a network operation center. MSA's Evergreen Heights Technology Center was opened in April of 2013.

The specifics of the Evergreen Heights facility include:

- 65,000 sq. ft. facility; 7,000 sq. ft. raised Data Center floor space with expansion to 15,000 sq. ft.
- Designed to meet Tier III data center specifications
- Service Organization Control (SOC 1) Type 2 audited facility
- Dedicated fiber network; part of MSA's and local fiber networks
- Multiple communication carriers
- Redundant generators and UPS systems in an (N+1) configuration; 2x2 MW diesel generators
- Dual power feeds
- State-of-the-art fire suppression systems
- Building initially designed as Data Center space
- 24x7 fully manned Command Center
- Near PAT bus routes
- 170 parking spaces with expansion capability
- DR seats and equipment

In addition to MSA's two SOC 1 Type 2 facilities, MSA maintains and operates three other data and communication centers that include MSA Headquarters, a location hosted at the Pittsburgh Technology Center, and a facility at the former Allegheny Center. These facilities include:

MSA Headquarters – Penn Avenue

- 130,000+ sq. ft. facility; 2,500 sq. ft. ground-level Data Center
- Easy access to central Pittsburgh and the airport
- Dedicated fiber network; part of MSA's and local fiber networks
- DR seats and equipment
- 24x7 fully manned Command Center
- Remote security monitoring
- Located on several bus lines
- DR backup or basic processing

Pittsburgh Technology Center

- Communication providers "meet me" facility
- Dedicated fiber network; part of MSA's and local fiber networks

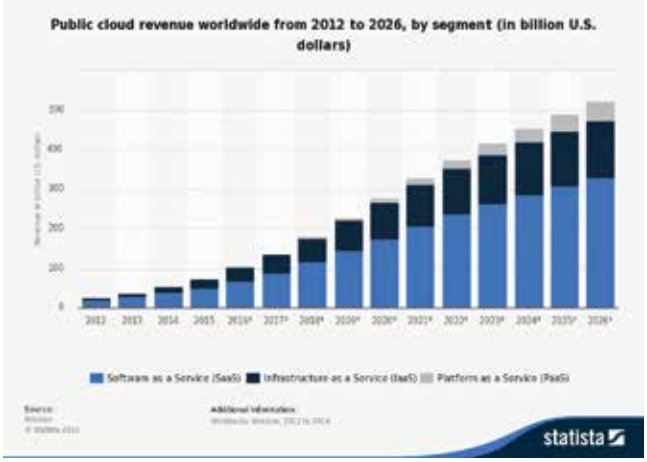
Allegheny Center

- Communications providers "meet me" facility
- Dedicated fiber network; part of MSA's and local fiber networks.

Products and Services provided through Data Centers

When one discusses data center services and cloud computing, there is often an overlap in the terminology. Part of this ambiguity is due to the rapid expansion and changing nature of the capabilities available, the necessity of all businesses to have a web presence and a solid, secure IT infrastructure available, and the fast pace of change in terms of commercial offerings. The National Institute of Standards and

Technology (NIST) defines Cloud Computing as a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.



Past and future revenue trends of Data Center Services

The following sections detail some of the standard products and services available in data centers in general and those in use by MSA specifically. These include Security, Disaster Recovery and Business Continuity (DR/BC), Hosting and Colocation services, Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

Security

Security is one of the most important aspects to consider when evaluating Data Centers. Security is a broad term that encompasses many different components as it pertains to Data Centers. Security concerns include the physical security of the facility, access to internal locations inside the facility, availability and reliability of power and network connections, firewalls and access control information for networks, and confidentiality and protection of data.

The following are important security considerations to evaluate:

- Implement security in layers
- Physical security of the facility and the data centers
- Personnel security clearances as appropriate
- Continuous investment in security
- Law of least privilege
- External / internal scanning / penetration testing
- System hardening from the operating system on up
- Requiring web-facing applications to pass an audit by a security team independent from the software developers
- Network segmentation
- Intrusion detection and prevention systems
- Knowledgeable security staff available 24x7
- Utilization of encryption algorithms as appropriate (e.g., SHA-256, SHA-512, Block Cipher-ICE)
- DR /BC Planning
- Multiple Backup and Restore options
- Virtualization

Disaster Recovery and Business Continuity (DR/BC)

Traditional Disaster Recovery companies maintain servers which are available on a first-declared, first-served basis. In the traditional model, access to servers are sold to multiple companies, where the first company to declare an event is provided access. Within 45 minutes of the first plane hitting the World Trade Center on 9/11/2001, all of one DR provider's northeast facilities were 100% committed. Companies that subsequently declared disasters had to travel to other of that company's facilities in the South and West.

Within 45 minutes of the first plane hitting the World Trade Center on 9/11/2001, all of one DR provider's northeast facilities were 100% committed.

A sample of companies that provide DR/BC services include IBM Global Business Services, Sungard Availability Services®, NTT Communications® and many others.

MSA's approach to the DR/BC business has been to focus on avoiding disaster and looking for ways to innovate to reduce costs and risks while improving efficiency. In thinking about efficiency and innovation, MSA opted to consider dedicated DR equipment as opposed to the shared asset models of the traditional providers. As an example, one DR client uses its DR servers to house downloadable software product upgrades for their users. Another client, who started using MSA's site as a DR facility, switched its production servers to the MSA data center, and used their own internal data center as the backup and DR site. In 2009, when the G20 Summit was hosted in Pittsburgh, two MSA clients used MSA's facilities to continue running their 150-person call center and a 30-seat help desk operation, after being "locked out" of their own facilities due to security arrangements in downtown Pittsburgh.

MSA's orientation toward using a dedicated server model (as opposed to the shared hardware concept) has become more prevalent in the DR/BC space over the years.

Hosting and Colocation Services

Hosting services encompass a wide variety of options that include web site and e-mail servers (either client owned or data center provided), e-commerce

ESWP Member News

More than 75 firms are represented in the Corporate Member program of the Engineers' Society of Western Pennsylvania (ESWP). Memberships are available at 3 levels: Gold, Silver and Bronze. Gold members are entitled to 14 memberships that can be exchanged by employees; Silver, 9; and Bronze, 5 — annual dues are $2400, $1700, and $1000 respectively. In addition, ESWP Corporate Member Firms may add 2 additional individuals in our Under-35 age category at no additional cost. More information can be found at eswp.com. Please contact the ESWP Office (412-261-0710) for additional details.

NEW! For Government Employees (full-time), Individual Membership Rates are now $50.00!

Membership in ESWP comes with a long list of benefits! From our continuing education opportunities earning you Professional Development Hours (PDHs), to the business networking events in our Executive Dining Room, there is something for everyone in your organization. Also, ESWP is helping the next generation of engineers with student outreach programs, giving you the opportunity to participate in many rewarding programs.

ESWP Gold Corporate Member Firms

AECOM

gai consultants
transforming ideas into reality

Michael Baker
INTERNATIONAL

GATEWAY
On Call. On Time. On Target.

ARCADIS
Infrastructure · Water · Environment · Buildings

HATCH

Orbital
Engineering, Inc.

CDM Smith

HDR

PARSONS

DiGioia Gray
& Associates

i+icon USA
Infrastructure & Industrial Constructors USA

solutions21

DEI
DeSalvo Enterprises, Inc.

MATRIX NAC

USS

ESWP Silver Corporate Member Firms

ALCOA

CANNONDESIGN

CEC
Civil & Environmental
Consultants, Inc.

CDR MAGUIRE

CSD
CARNEGIE STRATEGIC DESIGN
ENGINEERS
LLC

KU Resources, Inc.

Lennon, Smith, Souleret
Engineering, Inc.
Civil Engineers and Surveyors

PJ DICK
TRUMBULL
LINDY PAVING

Uhde Corporation

ESWP Bronze Corporate Member Firms

initiatives, backup and restore features, etc.

Colocation is a model whereby companies rent space for servers, racks and other computing hardware. The data center provides the building, physical security, power, cooling, and sometimes office space.

One key distinction between hosting services and colocation is who owns the hardware. Under a hosting agreement, the data center group owns and maintains the hardware, whereas in a colocation approach, the client company owns and maintains the equipment. There are many derivatives and permutations of these models and classifications.

Well-known hosting companies include GoDaddy®, ehost.com, Web.com® and Amazon®. Colocation services are offered by the major Data Center providers like 365 DataCenters®, AT&T®, CoreSite® and many others.

MSA provides a variety of hosting models that range from simple websites, to hosting and maintaining clients' enterprise-wide operational systems connected through proprietary networks and internal clouds.

MSA's largest hosting client is MSA. MSA's Data Centers provide hosting services for all of MSA's Divisions. All of MSA's businesses revolve around data analytics, data management, and the application of the latest technology, no matter the industry being served. Across all of MSA's business groups, there are nearly a petabyte of data being hosted and used for a variety of products and services for more than 300 clients. These data include shipment and point of sales data for fast-moving consumer goods, medical and transplant data, cable and broadcast TV schedule and audience share information, ferrous scrap price and volume data for benchmarking, pharmaceutical data, slot machine utilization data, and many other data sets. The hosting services used by MSA's Life Sciences Division conform to the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) certifications.

Software as a Service (SaaS)
Under the Software as a Service (SaaS) model, a software application is hosted on a remote server and accessed by clients through the Internet. Advantages of using the SaaS model include: no upfront capital investment in hardware or software, regular software updates occur automatically upon login, the software can be accessed from virtually anywhere, pricing is generally provided on a monthly/annual subscription fee, and for many applications used by multiple clients, a more robust and thoroughly tested system. Industry examples include GoToMeeting® by Citrix®, Google® Apps, and Contact Management Systems like SalesForce® and Zoho®.

MSA's Data Center clients also provide SaaS offerings to their own clients through these facilities. These include software distribution and update services, ERP modules, real estate listing services and others.

MSA has a number of SaaS applications including:

- Blending Optimization Software Suite™ (BOSS™) - The BOSS uses state-of-the-art mathematical programming models to determine the least-cost combination of raw materials necessary to manufacture a clients' product. This application is used by steel, aluminum, and other metals companies, but is also applicable to cement, food processing, and pulp and paper applications.
- eSource™ - MSA's eSource offering is a reverse auction and RFP/RFQ tool kit that has been used for international steel trading, medical device leasing, waste handling projects and other applications.
- foreTV™ - An international broadcast management system for satellite, cable and terrestrial television stations; providing program scheduling, sales and inventory management, on-demand, analytics, media management and other services.
- Alec™ - a brand allocation media schedule tool for advertisers. This MSA built application is hosted on the Amazon Web Service (AWS) platform.

Infrastructure as a Service (IaaS)
The Infrastructure as a Service (IaaS) model is where users can access, monitor and control data center infrastructure like networking, storage and databases. Under this model, companies contract with a third-party data center which provides secure access and tools that allow the company's IT staff to manage the virtual and remote infrastructure, either through a web-based graphical user interface or through programmable API library calls. Examples include Amazon Web Services®, Microsoft® Azure®, and Google® Cloud Platform.

Private and Public Cloud services also fall under the definition of IaaS. Public Cloud services are provided over the internet through a third-party data center, where the company has no responsibility for maintaining or managing the necessary infrastructure. In most instances, Public Clouds perform in a multi-tenant architecture, meaning sharing resources (processors, storage) with others. A Private Cloud implementation, on the other hand, dedicates resources to a single company or group. Advantages of a Public Cloud include scalability, no system responsibility, and a pay-as-you-go model. Private Clouds can be more secure and customizable, as they are a dedicated infrastructure.

MSA provides backup and other services to clients in the IaaS model.

These services include full infrastructure hosting to failover site provisioning. MSA's Cloud Backup provides for Tiered Recovery Options (as all data is not equal), Pay-for-What-You-Use, Simplified Reconstitution, Complete Server Protection, Full-Service Management and other flexible options.

Platform as a Service (PaaS)

The Platform as a Service (PaaS) model is where users can access software development tools, operating systems, databases and other environments, without having to directly own those assets. PaaS are an effective way to collaboratively develop software across an enterprise, and utilize features developed by others. Industry examples include Google®'s App Engine, Microsoft® Azure®, Salesforce.com®, and Red Hat®.

For internal divisions, MSA does provide some PaaS. These include implementations of Team Foundation Server® (a code management utility), Hadoop® servers, Microsoft® SQL Server® and other database instances.

Our anticipation is that the Software, Infrastructure and Platform as a Service models will continue to grow, and the types and suite of offerings under these labels will increase.

Summary – Future Direction

Globalization, social media, and the continued expansion of Cloud Computing offerings paint a bright future for Data Centers and their services. JLL's North America Data Center Outlook report predicts double-digit growth for both the data center (12.1% CAGR 2015-2018) and cloud computing (16.6% CAGR through 2021) markets. The Wikibon Statista graphic above show similar compound annual growth rates for these services as well.

Our anticipation is that the Software, Infrastructure and Platform as a Service models will continue to grow, and the types and suite of offerings under these labels will increase. Many companies will find themselves in need of these offerings to remain competitive.

Whether one contracts these services to third parties, or expands their internal capabilities to incorporate them in the offerings, are key decision points.

Management Science Associates' decision to invest in building internal Data Centers may not be the right decision for all companies. A combination of strong relevant technical skills, early mover advantages, and a risk-tolerant leadership team drove MSA to its decision.

About the author...

Patrick J. Gallagher is the Vice President of Management Science Associates Metals and Advanced Manufacturing Division

The changing challenge of cybersecurity

By: Dr. Michael Spring

Back in the late 1990's, the Department of Information Science and Telecommunications began to look at possible relationships with the emerging Computer Emergency Response Team (CERT) that had grown out of the efforts of the Federal Research lab in Pittsburgh – the Software Engineering Institute. The University of Pittsburgh (Pitt) began to recruit faculty with an interest in cybersecurity and managed to obtain funding that allowed them to develop graduate courses that would prepare folks to meet security needs in several areas.

As these efforts took shape, Pitt formed the Laboratory for Education and Research on Security Assured Information Systems (LERSAIS), where efforts in wireless security and ad hoc networks was growing. LERSAIS developed strong capabilities related to access control and privacy mechanisms. Graduate students were working on a variety of projects that provided new approaches to insider threats, secure coding, and a variety of other topics. LERSAIS secured funding to develop more courses and laboratory simulations in information systems, telecommunications, and health care systems. Progress was quite remarkable given the relatively limited resources available at the University.

As the internet and the business components of the web continued to grow, so to did criminal behavior. It was thought that at some level systems security was keeping a reasonable pace with the attacks despite the fact that there were still financial losses. Then in 2014, several shocking compromises in government and private sector arenas occurred. The Sony Pictures compromise as well as several other less well publicized intellectual property thefts among defense contractors raised the U.S. Government's level of concern as did the vulnerabilities suffered by the U.S. Office of Personnel Management.

While the story is far from over, LERSAIS is are engaged in a number of initiatives in Pittsburgh that may well help to shape the future of cyber security. At the request of Congressman Tim Murphy, Pitt Chancellor Patrick Gallagher called together more than 80 representatives of public and private organizations to look at how Pittsburgh might serve as a cybersecurity center of excellence for the military. While the picture is complex, one might imagine that ultimately the trained workforce of cybersecurity specialists going forward will include individuals in private organizations, military organizations, and academic and research organizations. One of the interesting intersections would be members of the National Guard and military reserves. Keep in mind that these are individuals who benefit from military training but for the most part function in the private sector. Pitt, Carnegie-Mellon University (CMU), Computer Emergency Readiness Team (CERT) , and the National CyberForensics Training Alliance are all moving forward to help establish such a center for excellence which might expand the number of individuals with expertise in cybersecurity that could benefit both the private sector and the military as needed.

Most recently, it has become clear both locally and nationally that our young people are not as aware as they might be of the opportunities in the field of cybersecurity. In general, our young people see teachers and doctors and police and lawyers as they grow up. This is not as true for people in cybersecurity, who are generally less prone to talk about what they do. With rapidly growing job opportunities and high pay, a number of organizations are becoming involved in efforts to make students aware of the opportunities and to encourage them to consider careers in this field. The National Security Agency and the National Science Foundation are funding "Gencyber" camps which provide high school students with an opportunity to experience the kinds of work security analysts do and encourage them to look at career opportunities. In Pittsburgh, the FBI has been spearheading an effort to generate interest. The FBI, the Norwin School District, the Pitt's School of Information Sciences have joined together to make three undergraduate courses available as a part of Pitt's College in High School program. This fall, as a part of the roll out, more than 100 students in the Norwin School District will participate in three courses in cybersecurity. They will have the opportunity to earn college credit and consider a career in the field. FBI agents will be actively engaged and students will be exposed to the research at Pitt, the work of the FBI cybersecurity teams, and the work of the various agencies in Pittsburgh – the National Cyber-Forensics & Training Alliance and CMU's Software Engineering Institute/ CERT.

About the author...

Michael Spring is an Associate Professor of Information Science at the University of Pittsburgh. His research involves the application of technology to the workplace with particular attention large scale electronic document processing and visualization, intelligent agents, and interface design.

Cybersecurity for Critical Infrastructures

By: Suresh C. Ramanathan

What is a Critical Infrastructure?

A Critical Infrastructure is defined by Presidential Policy Directive 21 as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters." In short, this includes every single physical and digital asset that when compromised or destroyed could terminate or disrupt our day to day economic, health and safety operations across various sectors and industries.

Increasing Interdependence of physical and digital assets

Critical infrastructures by definition include both physical and virtual assets and systems. But as we increase the use of sensors and remote technologies to monitor and manage our physical infrastructures and related equipment, we increase the exposure to potential vulnerabilities. Further when we incorporate wireless and wired connectivity to integrate and enhance entire systems, a single point of failure can be exposed or exploited by internal or external actors either accidentally or deliberately.

Cybersecurity defined

The National Institute of Science and Technology (NIST) defines cybersecurity as "the process of protecting information by preventing, detecting and responding to attacks". A cybersecurity event is defined "as the change that may have an impact on organizational operations including mission, capabilities or reputation."

The Cybersecurity Balancing Act

In the Presidential Executive Order 13636, it states that it is the "Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation and economic prosperity while promoting safety, security, business confidentiality, privacy and civil liberties." Legislations that pertain to certain industries like the HIPAA and HITECH act for the Healthcare provide further prescriptive details about security and privacy in those industries.

NIST Cybersecurity Framework

The Executive Order also called for the development of a voluntary risk-based cybersecurity Framework that has been developed by NIST. This framework was developed with input from both private and public sector and incorporates "a set of industry standards and best practices to help organizations manage cybersecurity risks."

The NIST Cybersecurity Framework has three major components: Core, the implementation Tiers and the Profile.

The Framework Structure		
Core	**Implementation Tiers**	**Profile**
Five functions provide a high-level, strategic overview of the lifecycle of an organization's cybersecurity risk and are further divided into Categories and Subcategories.	Tiers provide context for how an organization views cybersecurity risk and their in-place processes.	The profile represents the outcomes based on business needs tha an organization has selected from the Framework Categories.
Functions	**Tiers**	**Profiles**
1. Identity 2. Protect 3. Detect 4. Respond 5. Recover	1. Partial 2. Risk Informed 3. Repeatable 4. Adaptive	1. Current Profile 2. Target (Goal) Profile

Source: Commercial Facilities Sector Cybersecurity Framework Implementation Guide produced by the Department of Homeland Security.

NIST continues to refine the framework to address specific current limitations such as: Authentication and Supply Chain Risk Management. NIST has also developed self assessment tools and has just released the Baldridge based tool for cybersecurity excellence.

Plan at the Sector level

There are sixteen Critical Infrastructure Sectors that have been identified in the Presidential Directive along with a designated Sector Agency each. The cybersecurity framework has been leveraged by the designated agency and related industry experts to develop a sector specific plan in each case.

Critical Infrastructure Sector	Designated Agency
1. Chemical Sector	Department of Homeland Security
2. Commercial Facilities Sector	Department of Homeland Security
3. Communications Sector	Department of Homeland Security
4. Critical Manufacturing Sector	Department of Homeland Security
5. Dams Sector	Department of Homeland Security
6. Defense Industrial Base Sector	Department of Defense
7. Emergency Services Sector	Department of Homeland Security
8. Energy Sector	Department of Energy
9. Financial Services Sector	Department of Treasury
10. Food and Agriculture Sector	Department of Health and Department of Health and Human Services
11. Government Facilities Sector	Department of Homeland Security and GSA
12. Healthcare and Public Health Sector	Department of Health and Human Services
13. Information Technology Sector	Department of Homeland Security
14. Nuclear Reactors, Materials and Waste Sector	Department of Homeland Security
15. Transportation Systems Sector	Department of Homeland Security and Department of Transportation
16. Water and Wastewater Systems Sector	Environmental Protection Agency

Each of these designated Agencies is responsible for developing a Sector Plan by leveraging the NIST Cybersecurity Framework. These plans are responsible for identify the unique risks of each of these industries and is not limited to cybersecurity risks alone.

An Example of a Sector-Specific Plan: Water and Wastewater Systems Sector

EPA as the designated agency of the Water and Waste Water sector has developed a Water and Waste Water Sector-Specific Plan. It identifies all of the risks unique to this sector including cybersecurity framework.

Any critical infrastructure has three fundamental elements: Physical, Cyber and Human. Each of these elements of critical infrastructure though discrete and distinct is yet intertwined and interdependent. The Risk Management Framework begins with "Setting Goals and objectives" followed by "Identifying the Infrastructure" that has to be managed. The Risks are then analyzed and assessed and this information is used to develop a Risk Management plan. The Plan is then implemented and the effectiveness of the program is measured. The results that are measured are then used to inform and modify the various upstream steps as appropriate. This self correcting iterative approach makes the process more efficient going forward.

Common Software at Water and Waste Water Environments

EPA recognizes the following major systems in its Sector-Specific Plan:

1. Supervisory Control and Data Acquisition (SCADA) system
2. Process systems and Operational Controls
3. Enterprise Systems

Interestingly these are but broad categories of systems. There are numerous information technology assets ranging from portals, GIS systems, asset management systems, laboratory systems, inspection systems to regional data assets and data ware houses. They have to all be included in any kind of cybersecurity assessment and the development of cybersecurity initiatives plan.

Major Risks Identified in the Water and Waste Water System Sector-Specific Plan
Most Significant Risks
• Natural disasters (such as impacts on water quality and quantity from floods, hurricanes, earthquakes, ice storms, pandemic flu and other geographic catastrophes)
• Economic implications of aging infrastructure
• Cyber events
• Capability in managing an area-wide loss of water
• Although the water sector has been identified as a lifeline sector, this is not commonly recognized among all relevant stakeholders, a situation that can escalate consequences during an area-wide event
High Risks
• Economic costs of preparation and response
• Ignorance about the consequences of inaction and apathy from some stakeholders in utilities, the customer base, state/local government and Federal government /Congress
• Inadequate coordination and information sharing during preparation, response and recovery
• Intentionally malicious acts
• Limited resource availability: many utilities are faced with competing needs that are immediate (e.g., regulatory, aging infrastructure, workforce succession) , concrete and can limit resource availability for implementing preparedness and resiliency improvements
• Unenforced and outdated requirements that do not address evolving threats
Medium Risks
• Lack if mutual aid agreements, effective education, and outreach to emergency management, and lack of best practices for emergency response planning
• Technology interoperability issues that create information-sharing challenges during response
• Insufficient communication to water utility boards of the definition, management and prioritizing of critical assets and needs

Source: From EPA's Water and Waste Water System Sector Plan that they had adapted from the 2013 Roadmap to a Secure and Resilient Water and Waste Water Sector.

Plan, Coordinate and Communicate within and across sectors

EPA works closely with the Department of Homeland Security in developing and maintaining the Water and Waste Water System Sector Plan for human, cyber and physical assets. EPA recognizes that it has dependencies with each of the other fifteen sectors but specifies that the primary ones are Chemical, Energy, Food and Agriculture, Healthcare and Public Health, Transportation Systems, Dams, Information Technology and Emergency Services sectors.

Though we have used Water and Water system as an example and identified its interdependencies with other sectors, each of the remaining 15 sectors has interdependencies with other sectors. This requires that each and every sector has to be diligently focused on ensuring that each of the public and private organizations within its sector has to fulfill its responsibilities while simultaneously coordinating with other sectors that impact it.

Execute at the Organizational Level

The Center for Information Security (CIS) believes that applying the first five of CIS Controls can reduce and organization's risk of cyber attack by around 85%. Implementing all 20 of the critical controls

increases the reduction to around 94 percent.

The top 20 Critical Controls identified by the Center for Information Security in the 6.1 version of the controls are:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Devices
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capability
11. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Public and Private organizations at both Critical infrastructure and non-critical infrastructure sectors can leverage these controls and make their organizations more mature from a cybersecurity stand point within a short period of time.

Call to action to Boards and Executive Management

All designated agencies for each of the sixteen sectors are responsible for encouraging an operational culture that incorporates physical and cyber security into its day to day operations. Ultimately it is the Board members and the Executive Management of each of the public and private organizations within each of these critical infrastructure sectors that have to demand, authorize, fund and evaluate the cyber (and physical) security initiatives of each of their organizations. It is the fiduciary responsibility of the boards to ensure that Cybersecurity initiatives are underway at their organizations. With many resources, including many free ones, there is no excuse for an organization not to adopt and implement the NIST Cybersecurity framework and leverage its many tools. Regardless of whether you do it internally or seek some assistance, a Cybersecurity program is essential and you can even aspire to Baldridge level competencies and related recognition.

About the author...

Suresh C. Ramanathan is the President & CEO of KORYAK. Suresh left Deloitte Consulting to co-found KORYAK 16 years ago. He is the recently elected chair of South Western Pennsylvania Engineering Outreach (SPEO). For more information, please visit www.koryak.com or phone toll free: 1-866-4KORYAK

Top Challenges for Cloud and Colo Data Center Infrastructure

By: Chris Massetti

User demands are growing and technology is changing, impacting data centers of every size. Large colocation data centers (where a business can rent server space and other computing hardware) as well as cloud storage companies are leading the charge. The handful of large companies in these two industries will develop more than a thousand megawatts of data center capacity in the span of just a few years. They will innovate and adopt new ways to drive down costs, experiment with new technologies and test the limits of data center performance. These companies are also under intense pressure to quickly and more cost effectively build strong, ultra-efficient data centers. This involves a great deal of assessment in terms of technology and practice with a critical eye to the efforts to accomplish this goal. Due to the magnitude of these efforts, companies can work with high-end hyper-scale vendors to create custom solutions, specific to their needs. The growth of these colocation and cloud companies has shifted in terms data center technology and hiring needs.

The main challenge for engineering firms is reaching the next generation of large scale data center owners while keeping pace with the trends in the technology curve — specifically around system design and automation. This is made increasingly difficult as large scale providers are becoming fewer and larger in size. Many of these changes will have dramatic influence in the future and will impact the data center industry in the Pittsburgh area.

Reserve Architectures, Rack-Based Power Protection, and Efficient Technologies

One of the most important developments to come out of this "super group" of technology users is deploying only "what is needed, when it's needed" philosophy, leading to new power system architectures. This includes evaluating the best location for backup power within the data center – room, row or rack.

> "In today's environment the need to optimize capital efficiency and resource utilization is paramount"

In today's environment the need to optimize capital efficiency and resource utilization is paramount. Increasingly, large colocation facilities are replacing the 2N or 2N + 1 dual-bus architecture with various reserve architectures, which essentially create an N+1 or N+2 architecture within the UPS system, while maintaining fault tolerance and concurrent maintainability through the use of static transfer switches (STS).

These new shared reserve architectures can support more than double the kW of common 2N +1 architectures, without increasing UPS capacity. From an economic standpoint, the change to reserve architecture can make a measurable difference, even though these new architectures make maintenance and load deployment more complicated than in a traditional 2N architecture.

Some data centers now use the reserve architecture to mimic 2N, creating significant flexibility in the quest for efficiency, speed and availability. The reserve power configuration, whether shared, dedicated or distributed, has applicability within both colocation and enterprise applications.

Reserve systems are just one example of how power system architectures are evolving to meet the new needs in terms of capacity, modularity, speed and efficiency. Another is the deployment of rack-based power systems to energize DC powered IT equipment inspired by groups such as the Open Compute Project.

Large colocation and cloud data centers need to bring on capacity quickly and incrementally without compromising capital efficiency. These new rack-based power systems create the speed of deployment developers are looking for driving power protection to the row and ultimately to the rack, making the rack an autonomous unit. These types of systems can be brought on line without adding to the load of a room- or aisle-based power protection system.

On the power front, there is no more anticipated technology than lithium based batteries. Lithium-Ion battery technology provides a much more robust, yet surprisingly compact alternative to the existing lead acid batteries that are the current standard. Lithium battery technology provides a compact backup power source, high power density and the ability to operate in the increasingly high temperatures that exist in this new generation of data center. While initial cost is an issue, they are becoming far more affordable.

In the event of a power interruption, some hyper-scale users are deploying lithium battery backup units (BBUs) to provide short-term ride through of 12V DC power. This creates an efficient backup power strategy and provides the ultimate in flexibility by enabling capacity to be added one rack at a time.

Trending Employment Needs

A 2015 Emerson Network Power Survey (Data Center 2025) showed that 37 percent of data center professionals in the United States expect to retire by 2025. This shift in management may be a driving factor behind the need for integration and automation.

While some might think the shift to colocation centers would drive down hiring in the data center industry, those within the industry think differently. Considering the drive for automation and unmanned operation, 50 percent of data center professionals in the United States expect to be employed in the industry. In addition, there may be opportunities for newcomers to the field, as the U.S. stands to take the biggest hit from retirement of all of the countries surveyed. In Pittsburgh, you can see the influence of these hiring trends. Many national and regional players in the colocation space are making an impact in the local market.

Colocation and Cloud Innovation

The focus of data center design is shifting to capacity, modularity, speed, efficiency and integration. By embracing new power topologies and creating new reserve architectures, colocation and cloud innovators are leading the way to revolutionary new approaches to how a data center is built and scaled. An upcoming wave of retirements will also change how the data center is staffed. The long held belief is that the vendors whom best understand the needs of the user will continue to grow and thrive. It is important that those looking to serve the needs of the next generation of data center professionals understand how the user gets hired, promoted or fired. In other words, centralizing your solutions and capabilities around that set of metrics. Does efficiency count? Get educated on energy efficient cooling. Is low first cost a driving factor? Be prepared to design power systems that are scalable to avoid 'standing' capacity and capital.

This wave of development—and the innovations emerging from it—will bring new choices to organizations of all sizes, not only in how they acquire capacity, but in how they deploy it and support it within their own facilities. By meeting new requirements and providing new technologies while adapting proven architectures, we can design and manage high-availability data centers that deliver the capacity, efficiency, speed and integration necessary to meet tomorrow's critical needs.

About the author...

Chris Massetti is President of Donwil. Chris has worked in all facets of Data center equipment sales and design for 21 years.

SETON HILL LAUNCHES OFFICE OF ACADEMIC INNOVATION AND PLANNING

CYBERSECURITY MAJOR PLANNED FOR SPRING 2017

By Mary C. Finger

Seton Hill University has an extraordinary commitment by the University's faculty to ensure the success of our students and the rich spirit of innovation on the campus sparked by our pioneering founders, the Sisters of Charity of Seton Hill.

Seton Hill has been innovative through partnerships – both with leaders in the City of Greensburg and Westmoreland County in bringing our arts programs into the downtown Cultural District and with leaders of other institutions of higher learning in collaborating on distinct opportunities such as the opening of a campus of the Lake Erie College of Osteopathic Medicine (LECOM) at Seton Hill.

The University has been innovative in the use of technology. Seton Hill's mobile learning program provides all students with the same digital platform and offers faculty the education and resources to use technology in the classroom to enhance learning.

And Seton Hill remains innovative in the development of new academic programs – from the adult degree program, which was one of the first in the region in the 1970s, to health sciences offerings such as the Physician Assistant program that fill the need for trained healthcare workers in the Pittsburgh region.

As Seton Hill continues to grow and evolve to meet the ever-changing needs of our students and the region's employers, the University began to look at ways that we could institutionalize the academic innovation and planning that we have historically found success.

With a $500,000 grant from The Richard King Mellon Foundation, Seton Hill created The Office of Academic Innovation and Planning, which will explore new academic programs and partnerships to provide the southwestern Pennsylvania region with the skilled workers ready to take on the jobs of the future.

Among the first new academic programs the Office of Academic Innovation and Planning is developing is an undergraduate major in cybersecurity.

The Allegheny Conference on Community Development's recent report on workforce development, "Inflection Point," cited cybersecurity as one area where job demand is strong and growing. In fact, the report states, cybersecurity postings have grown rapidly in Pittsburgh – at three times the rate of Information Technology jobs overall since 2010.

Over the next ten years, the need for Information Security Analysts is projected to grow at 20%.

Over the next ten years, the need for Information Security Analysts is projected to grow at 20%. It's one of the top IT occupations and is among the top 5 percent of all occupation growth.

With Seton Hill's undergraduate program in Computer Science and the University's commitment to infuse technology into all aspects of the educational experience, a major in cybersecurity is especially relevant. Organizations of all types – from financial institutions and medical facilities to retail companies and government agencies – will need cybersecurity analysts to protect confidential data.

With the rising number and sophistication of cyberattacks and episodes of digital spying, the University recognizes cybersecurity will continue to draw interest from students and become a sought after major. Seton Hill's cybersecurity program is expected to launch in the Spring 2017 semester.

The Office of Academic Innovation and Planning institutionalizes and provides additional resources for what Seton Hill has historically done - strategically develop new academic programs that meet our region's workforce needs. The Office enables Seton Hill to centralize our processes in developing new academic programs and help the University assess the jobs and skills needed in our region to ensure students are well-prepared for a workplace that is evolving constantly.

While academic innovation offices are found at large, research universities, such centers at liberal arts institutions are not commonplace. However, institutions like Seton Hill can be more agile when it comes to developing new academic programs, and Seton Hill's new Office of Academic Innovation and Planning can serve as a model for other private liberal arts universities. The Office will allow Seton Hill to more readily address changes in the technology, healthcare and business sectors in Southwestern Pennsylvania and bring new academic programs, such as cybersecurity, to the marketplace more rapidly than before.

The Office of Academic Innovation and Planning, which will be led by Bernadette Fondy, Ph.D., Professor of Biology and Chair of the Division of Natural and Health Sciences at Seton Hill, will provide the resources to conduct the necessary marketplace research and curriculum development.

Over the next ten years, more than 1.2 million new and retrained workers will be needed throughout the region as older workers reach retirement age. Seton Hill will work closely with employers to ensure that our students are prepared for these opportunities – whether it be cybersecurity or another area of need.

About the author...

Mary C. Finger, Ed.D. is President of Seton Hill University. For more information on Seton Hill academic programs, visit www.setonhill.edu.

The 77th Annual INTERNATIONAL WATER CONFERENCE®

The IWC has always been a strong educational conference. Attendees come to learn about the latest applications available in the industrial water treatment industry, educate themselves in current technology and applications through attendance in IWC workshops, and network heavily with their peers active in water treatment in the IWC Exhibit Hall. This year, more than 75 technical papers and 24 Continuing Education Workshops are scheduled. All are carefully peer reviewed for quality and to ensure no commercial aspect is evident. Each paper presentation at the IWC is followed by a prepared discussion–a thoroughly considered, different perspective on the topic, followed by an open floor discussion when all audience members and presenters can fully interact–ask questions, seek clarification, and raise alternative viewpoints. If you have previously attended the IWC, we look forward to seeing you again! If you are new to the IWC, come and give it a try! There are many educational and networking opportunities for you to broaden your knowledge and your network. You will not be disappointed!

NOVEMBER 6-10, 2016

SAN ANTONIO, TX USA

WWW.ESWP.COM/WATER

The 34th Annual

INTERNATIONAL BRIDGE CONFERENCE®

THE IBC RETURNS TO THE NATION'S CAPITAL REGION

JUNE 4-8, 2017

GAYLORD NATIONAL RESORT, NATIONAL HARBOR, MD

GAYLORD NATIONAL RESORT & CONVENTION CENTER