Mike Schleif

Executive Biography

Senior Global Business Architect

Visionary business systems architect, designer & developer solves complex problems. Maximizes ROI by implementing technology-driven solutions. World-renowned as a Security Information & Event Management (SIEM) authority.

Mike Schleif delivers more than 30 years experience in technical consulting, problem solving, project management and knowledge transfer. My career has taken me to the inner circles of World Class companies spanning multiple industries, countries and continents.

My extensive client base ranges from organizations as small as one person to multinational firms operating numerous facilities. I serve each company by solving critical business problems through better Systems Management. Drawing on this wealth of experience, innovative spirit, collaboration and technology skills, I architect, design and implement cost-effective solutions.

Down-to-earth, real-world perspectives on Best Practices, and intimate knowledge of the systems and processes companies utilize to achieve and retain their leadership positions, minimize my time to understanding what your company needs to accomplish. Hands-on practice hones my ability to mentor and direct cross-functional teams to interface with key operations.

Every day, I demonstrate my command of the Information Technology Infrastructure Library (ITIL) and its five basic principles for managing Information Technology (IT) services:

Strategy ► Design ► Transition ► Operation ►► Continual Service Improvement

I am considered a Subject Matter Expert in multiple disciplines:

IT Infrastructure • Network & Systems Architecture • Enterprise Security
Enterprise Systems Management • Payment Card Industry Data Security Standard
Encryption / Decryption • Automation Programming • Disaster Recovery

My client list includes IBM, a customer since 1992. Sister affiliates, Ameritech, SBC and AT&T, benefit from my guidance since 1994. Other long-term customers include UnitedHealth Group (UHG), Target Corporation, Health Care Services Corporation (HCSC), Platinum Systems Specialists, Inc. (PSSI) & Sempris LLC.

I am a graduate of Northwestern University where I earned a BA in Mathematics and Philosophy. A multilingual student of German, Mandarin, Russian and Spanish, I enjoy meeting and working with cosmopolitan people.

CAREER HIGHLIGHTS

Sempris LLC, Minnetonka, MN

Sempris, LLC is a privately-held business services company based in Minnetonka, Minnesota, that develops and manages membership and customer relationship marketing programs. Since Sempris is heavily invested in credit card processing, I was brought on board to maximize security, and to automate as much production file and transaction processing as possible.

Problems:

A) How can Sempris best meet all requirements of PCI DSS 3.2?
B) How can Sempris effectively process credit card information without human eyes?
C) How can Sempris reduce cost & increase security in the cloud?
D) How can Sempris effectively monitor Enterprise systems and production processes?

Solutions:

Automation removes hands and eyes from sensitive information. All data exchanges with banks, credit card processors, clients and vendors traverse the internet inside encrypted tunnels. All files remain encrypted, except during internal processing. All decrypted files are deleted immediately after processing. All online data exchanges are via SSL and are processed securely, never existing in readable format. All passwords and encryption keys are stored encrypted and are decrypted only during transaction processing. Credit card numbers are hashed (i.e., one way encryption.) The hosts on which these processes run are on an isolated VLAN, accessible only by few people using two-factor RSA authentication. Quarterly internal PCI audits are conducted and fully documented. At the end of each year, an accredited third party Qualified Security Assessor (QSA) performs a Level 1 onsite assessment, results of which are published as the Report on Compliance (ROC).

Migrating from hardware infrastructure in a physical data center to the Cloud presents challenges unheard of twenty years ago. Engineering this in Amazon Web Services (AWS) to exceed PCI Merchant Level 1 criteria requires an Enterprise Architect with cutting edge expertise. Several months into design, a couple of security bugs were discovered requiring AWS to correct. Careful creation of this new paradigm promises to reduce operational costs, and to improve overall security.

Automation is the key to this success. All exceptions are formally published as Security Incidents, including all actions and resolution. All changes to systems and processes are recorded as projects, trouble tickets and Change Board Requests. Access is granted only after formal Need to Know review.

Round the clock, automated monitoring of all Enterprise systems informs management of Production health. Remote VPN access is granted to key systems administrators using two-factor RSA authentication. Critical metrics are formally established and published. Many tools are used to measure systems and process health, results of which are pushed up to a mobile app console used by management. Formal Disaster Recovery policies and procedures, including quarterly testing and documentation review, are fully documented.

Target Corporation, Minneapolis, MN

Target Corporation is the second-largest discount retailer in the United States and is a component of the S&P 500 Index. On a recent contract, I was selected from more than 20 candidates to architect, design and implement a custom solution to enhance the value of the company's IBM Tivoli Enterprise Systems Management software.

Problems:

A) How can Target effectively transition from its 15-year old IBM Enterprise Management software system to the new, cutting-edge system?
B) How can Target best leverage fifteen years of software customizations and move all of that functionality to the new system?
C) How can Target ensure that the new IBM Enterprise Systems Management system meets and exceeds all of the expectations demanded from legacy systems?

Solutions:

I helped implement this IBM Enterprise management system in the early 1990's, when they were named Dayton-Hudson Corporation. Over years, I developed many customizations to best meet Target's growing Enterprise expectations, and trained staff to further enhance

them, as required. IBM developed vastly improved Enterprise Systems Management software, without upgrade path from these legacy systems.

I examined more than 4,000 legacy scripts, each of which had unique functionality and required access by multiple users to add, modify and delete information at will. I sorted by functionality and developed a database-driven configuration management system to incorporate legacy, script-based system functionality.

The basic IBM Tivoli software was installed and configured by a third party, with which I collaborated on identifying specific requirements and documentation. Since design and configuration processes were variable and in a state of flux throughout the last hours of deployment, our new design remained fluid, flexible and changeable until the end.

The user interface required no special programming skills and the new system could be accessed by a broader range of administrators. The new system is several times more efficient and can handle at least an order of magnitude more real-time events, while meeting all of Target's expectations.

UnitedHealth Group (UHG), Plymouth, MN

UnitedHealth Group Inc. is an American diversified managed health care company based in Minnetonka, Minnesota. It is 6th on the Fortune 500. On one contract, I was tasked to engineer and implement their move to a Managed Services Model, and design and implement processes to integrate several ongoing acquisitions into UHG's new infrastructure.

Problems:

A) How can UHG best engineer the transition of existing infrastructure to a Managed Services Model?
B) How can UHG best extend its current IT infrastructure to effectively accommodate new business acquisitions?
C) How can UHG best integrate IT infrastructures from multiple company acquisitions?

Solutions:

Moving to a Managed Services model, we re-engineered IT systems in three major areas: Data Center consolidation, application consumption control and system refresh at end-of-life. New systems serve four Data Centers as well as hundreds of remote corporate and customer sites throughout the United States.

I helped design processes to determine final destination of systems and devices by answering simple questions:

1) Can this system operate in a cluster environment?
2) Can it be virtualized into one large system side-by-side with other applications?
3) Must it remain a standalone product in its own physical server?
4) What are the SAN disc location and configuration requirements?
5) What network security specifics are required?

Managed Services reduce the number of Data Centers by 50% and increase application density per unit of space five fold. It also cuts average power usage by a factor of at least two and average disk space by one third.

Health Care Service Corporation (HCSC), Waukegan, IL

HCSC is the largest customer-owned health insurance company in the US, 4th largest health insurer in the US overall, and an independent licensee of the Blue Cross and Blue Shield Association, concentrating operations in Illinois and Texas. I was asked to examine their IBM / Tivoli Systems Management software already owned by HCSC, to determine its value in solving a major problem. Subsequently, I engineered a transition to HP Enterprise Systems Management software.

Problems:

A) How can HCSC best manage its IT infrastructure that has grown so large and so fast that it was unmanageable?
B) How can HCSC preempt operating problems before customers complain about system failures and service interruptions?
C) How can HCSC effectively transition from its legacy IBM Enterprise Systems Management system to new and improved HP Enterprise system?

Solutions:

HCSC's IT infrastructure had grown so large and so fast that it became unmanageable. Operating problems occurred frequently and were not understood until after customers complained about system failures and service interruptions.

I utilized obsolete equipment and the IBM systems management software HCSC owned, but didn't know how to use. I architected, designed and customized metrics and monitoring systems to demonstrate the efficacy of alerting administrators in real-time of faults and errors. Furthermore, it also determined the root causes of those problems, simplifying problem resolution.

I taught HCSC personnel how to use these tools to respond to problems as they occurred and before they generated complaints from customers. As the collected metrics data grew, these monitoring systems evolved and became more sophisticated. HCSC became proactive, predicting and acting on problems before they occurred and before they negatively impacted revenue.

Subsequently, HCSC management decided to use HP Systems Management software. I directed the transition from the IBM systems I implemented to HP Systems Management products. I kept the IBM systems demonstrating production value, while spearheading design and development of the replacement HP systems.

I provided assessment, architecture, design, budgeting, installation, configuration, customization and testing information to management. We collaborated through release to production across the entire HCSC Enterprise.

Ameritech / SBC, Hoffman Estates, IL

Ameritech Corporation was a U.S. telecommunications company, one of the seven Regional Bell Operating Companies that was created following the breakup of the Bell System in 1984. Ameritech was acquired by SBC Communications in 1999. I spent much of 1995-2002 on contracts there. Their Y2K program started in 1998, during which I joined the Y2K Flow Through Testing team to architect, design and build a microcosm of the entire Ameritech Enterprise.

Problems:

A) How can Ameritech effectively use hundreds of different technology-driven techniques and tools to manage its varied and complex computer networks?
B) How can Ameritech best correlate data from dozens of point-specific tools, and consolidate and unify meaningful information in a single management console?
C) How can Ameritech best test and demonstrate that production systems are not susceptible to Y2K anomalies?

Solutions:

Ameritech used hundreds of different technology-driven techniques to manage its varied and complex computer networks. I entered a joint venture with IBM / Tivoli to customize its Systems Management software to meet the specific needs of Ameritech, which became a three-year commitment.

I conducted proof of concept projects to demonstrate the value of IBM / Tivoli Enterprise Systems Management software to support Ameritech's Enterprise Data Centers. I architected, designed and implemented IBM / Tivoli software to communicate and share data with other third-party point products. I leveraged Ameritech's investment in non-IBM / Tivoli tools, as well as integrated them into the IBM / Tivoli software systems, by creating custom programs to interface between software systems and to fully automate manual tasks.

In 1998, I joined the Y2K Flow Through Testing team to architect, design and build a microcosm of the entire Ameritech Enterprise. Spanning multiple Data Centers, a complete network secured and isolated from the production Enterprise, we implemented systems from numerous mainframes, UNIX and Windows servers to desktops and every Enterprise application, system and process. We successfully integrated applications testing within this infrastructure, supported it and demonstrated full Y2K functionality.

SKILLS SUMMARY

Databases: Oracle, SQL Server, DB2, SAP, PostgreSQL, MariaDB, MySQL, Informix, Ingres, SimpleDB

Enterprise software: Microsoft, Oracle, IBM, SAP, EMC, Amazon/AWS, Salesforce, Adobe

Hardware: Mainframe, mid-range, *NIX, desktop, embedded systems; SAN, NAS, gateways, routers, switches

Networks: Internet, OSPF, RMON, SIP, SNMP, TCP/IP, UDP, VoIP, VPN, Wireless

Operating Systems: Apple, Linux, Microsoft, Netware, UNIX, z/OS, various legacy

Programming Languages: Assembler, C/C++/C#, HTML/CSS, Java, PHP, Perl, Prolog, Python, Shell, WSH, XML/SGML/JSON

Security: AntiSpam, AntiVirus, Encryption, Firewall, Intrusion Detection, NMap, PCI DSS, PGP/GPG, Snort, SSH, SSL, VPN

SIEM: Accenture, Akamai Technologies, AlienVault, AT&T Network Security, AVG Technologies, Check Point Software, Cisco, Dell SonicWALL, Deloitte, F-Secure, F5, Gigamon, HP, IBM Security, Intel Security Group, Kaspersky Lab, Level 3, Malwarebytes, NetIQ, Palo Alto Networks, PKWARE, PwC, Qualys, Radware, RSA, Sophos, Splunk, Symantec, Tenable Network Security, Trend Micro, Tripwire, VMware