

# MiBiz Roundtable: Tech security

Monday, June 11, 2007 - MiBiz

---



**Robert Babuska**  
Data Constructs



**Keith Brophy**  
President of  
Business  
Development  
NuSoft Solutions Inc.



**John Clark**  
Wow Web  
Works LLC



**David Fideler**  
Principal  
Concord  
Communications and  
Design



**Terry Hoy**  
President  
Intersect  
Technologies



**Oliver Krings**  
Director of  
Technology  
CPR



**Julie Lough**  
President  
Micro Visions  
Inc.



**Chad Paalman**  
Managing  
Partner & VP of  
Sales  
NuWave  
Technology  
Partners



**Pranay Rajgarhia**  
SolidDesign  
software



**Chris Roerig**  
Vice President  
and co-owner  
CQSI Innovation  
Inc.



**Aaron Schaap**  
Founder  
Elevator Up



## MiBiz: What are your customers' top technology security concerns?

**Babuska:** First, spam is and should be a major concern, e-mail-borne viruses and worms, plus the damage and lost productivity of spam can be devastating for any organization. Second, providing access for distributed offices, remote support vendors, tele-workers, and road warriors is a must and needs to be secure.

**Brophy:** The top corporate worry that we see today is concern about someone accessing corporate data from outside the environment. There is fear about targeted attacks as well as random hackers, and general concern for end-to-end data security.

**Clark:** In our Web development realm it concerns mainly e-commerce issues. Our clients that are conducting business with shopping carts want to be sure their sites are hacker safe.

**Hoy:** Our customers' top technology security concerns are virus, spyware, system and firewall intrusion. Our customers are looking for the technology that will leave them confident that all of their company's pertinent information is safe from hackers or disgruntled employees.

**Krings:** Protecting the network infrastructure from external penetration attempts is still the top concern for most businesses. Protecting data assets from unauthorized access is becoming a higher priority. Protecting the organization against misuse of the technology environment is also a concern.

**Lough:** The primary fear is loss of data or unauthorized access to data via network intrusion, either internally or externally.

**Paalman:** Who is on their network? Who are they, should they be on the network, if so, should they be where they are at? This goes for both wired and wireless networks. They are also concerned about limiting access to information and giving clearance to only authorized users, preventing the theft of company electronic information and backups. More and more businesses rely on their network as a mission critical component of their business.

**Rajgarhia:** Password theft and denial-of-service kind of an external attack.

**Roerig:** We provide automation systems to pharmaceutical manufacturers, so our customers' security concerns are mostly regulatory-related. Automation systems rarely provide any offsite access. Our clients' site security measures and employee self-interest are usually sufficient to prevent unauthorized system use.

**Schaap:** A lot of our clients are new to doing online transactions and need someone to walk them through the process of setting everything up in compliance with their credit card merchant provider and VISA regulations.

**MiBiz: Are cyber criminals becoming more sophisticated and how do you advise your clients to address that threat?**

**Babuska:** Premeditated or malicious threats are evolving faster and are more sophisticated than ever. Clients can help protect themselves from these threats by ensuring that they are properly running Anti-Virus, Anti-Spyware on the Desktop and most importantly at the Gateway level.

**Brophy:** This evolution is constant! Knowledge continues to expand, and with it, so does the knowledge in the hands of cyber bad guys. We recommend a multi-layered approach that gives more layers of complexity.

**Clark:** Becoming more sophisticated? That's a given. Make sure your online presence is backed up with an insurance policy. Don't have your e-mail address on your site unless it is disguised with a Java script of some sort so the evil robots can't find and read it.

**Hoy:** We will never have 100-percent secure networks. We assist our customers with the latest technologies and strategies for securing their data, networks and potentially weak areas from intruders and help them devise a plan of attack.

**Krings:** There is a serious increase in cyber crime and organizations need to be aware of this threat. However, security expenditures have to be carefully researched and calculated to provide a return on investment to the organization.

**Lough:** While the criminals are not necessarily becoming more sophisticated, there is greater access than ever before to tools that are becoming increasingly more sophisticated. We advise up-to-date patching, frequent network monitoring, and network intrusion detection.

**Paalman:** The amount and sophistication of cyber crime increases daily. We advise our clients that there is not a "one-and-done" solution for security.

**Rajgarhia:** Yes they are becoming more sophisticated. Advice: Frequently change password (expire password in 15 days and unable to use last 6 passwords), and look into some kind of (such as fingerprint) biometric security.

**Roerig:** Cyber criminal attacks on manufacturing automation systems are far too rare to analyze "trends" in sophistication. Prevention is usually possible through network segregation.

**Schaap:** Working through a solid and tested solution helps outline the possibilities and how to continue watching for future issues. For new customers, we often recommend a feasibility study that allows for a low-cost analysis of what it going on and define a project plan for moving forward.

**MiBiz: Will endpoint security solve most or all of current IT security problems?**

**Babuska:** Any one point of security can't stop everything by itself. Endpoint security is one of the main ingredients in a comprehensive multi-layered security plan. In order to provide the most robust security, multiple layers are required.

**Brophy:** Endpoint security is a great place to start. Having a firewall that allows only traffic that you want is ideal. However, nothing is foolproof. If it is a computer system, there is a chance for vulnerabilities.

**Hoy:** Endpoint security is a logical solution for organizations. This resolves a considerable amount of insecurities that companies have and allows for the option to only permit certain communication with their direct resources for business.

**Krings:** No, as the industry continues to change, new vulnerabilities will appear. Although most organizations have adequate security around the perimeter of their networks, we will see an increasing security focus toward mobile communication devices and the impact such devices have on the data assets.

**Lough:** No. User training continues to be the primary deterrent to security issues. Although the proper installation and

maintenance of endpoint security will diminish security threats, untrained users will unwittingly defeat even the best endpoint security solutions.

**Rajgarhia:** Yes, it will solve most IT security problems, but the users have to be educated on maintaining their own security with IT help.

**Roerig:** Yes.

**Schaap:** Making sure you have a strong firewall, the ability to do strong encryption of data being passed around and constantly making patches to your servers is important. Having a vulnerable machine is a large problem from the server level down to the individual machine.

#### **MiBiz: Should vendors have any liability for insecure software?**

**Babuska:** The end user or network owner bears the brunt of the cost of security, including the cost of securing the insecure software. So the correct question, regardless of open-source or commercial software, is how do we secure the software move or share the cost (liability) of security, without impacting the creativity of developers and time to market for the software itself.

**Brophy:** A vendor should be responsible for ensuring a product works as advertised. There is no such thing as a perfect system, but rather degrees of safety that depend on combinations of technologies, levels of "extra checks" coded into a system, the process and the people using a system, along with many other factors. So while vendors have high professional responsibility, like everything related to computer security, there are many layers and shades to vulnerability.

**Clark:** Yes. In general, the clients expect the software to be breach free. While larger companies may have an IT department to check this thoroughly, small- to medium-sized businesses don't. If that vendor can't accept the liability in the upfront contract, a new vendor might be in order.

**Hoy:** If a vendor knowingly installs or uses insecure software, they have a responsibility. However, if a vendor is installing or using third-party software that is represented as secure from the developer, then there should be no liability.

We believe that the vendor as well as the software manufacturer should be held liable for insecure software. Unfortunately in today's market, it is buyer beware.

**Krings:** While the vendor community is constantly reviewing existing security threats, it is always in a reactive mode for the response to such challenges. It is unrealistic to anticipate the exploitation of security related technology flaws. The way to respond to such challenges is a managed services approach to stay on top of the exploitations and react faster.

**Lough:** While vendors do have a responsibility to maintain high security standards, they should not be held responsible for hackers who would disassemble, discover, and exploit security holes that would not otherwise pose a threat.

**Rajgarhia:** Yes, vendors should be held responsible for poorly designed software that leaves security holes for hackers to exploit.

**Roerig:** If the user can demonstrate that system access is less restrictive than the specifications allow, the vendor is accountable for addressing problems under the original contract. Post-delivery, it's not practical to hold vendors accountable for evolving threats and unanticipated system connectivity.

**Schaap:** I think vendors need to stand by what they deliver and definitely be committed to fixing issues, but you can't rely on one company to solve all insecurities.

#### **MiBiz: Are your clients more concerned with attacks on their IT systems from outside or inside and which do you feel poses more of a threat?**

**Babuska:** Inside attacks pose much greater threats than attacks from the outside. But I believe most clients dealing with their IT support vendors are most concerned with threats from outside attacks.

**Brophy:** It seems that most clients are more worried about an attack from the outside. They make sure that their firewalls are locked down tight and only small amounts of traffic are let in. However, much research shows that often damage comes internally from access to data in a corporation that is not intended to be shared.

**Hoy:** While our clients are concerned about the unknown intruder from the outside via the Internet, there is a larger concern of internal secrets or documentation being stolen or compromised by employees.

**Krings:** Although external security concerns still dominate the discussions, it is a known fact that the lack of standards and policies allow for loopholes from an internal security perspective.

**Lough:** Although clients often view outside attacks as the primary concern, we recognize that unauthorized internal access to data poses the greatest threat.

**Paalman:** The trend actually seems to be that businesses are increasingly concerned about the threat from the inside. In many cases, this may actually be due to naive users versus malicious intent.

**Rajgarhia:** Clients are more concerned about attacks from outside. We believe the more likely attack will start from inside, leading to an external attack.

**Roerig:** Mostly outside. Manufacturing technicians are generally trusted to act with good intentions.

**Schaap:** Smaller companies are more concerned about outside threats. Although larger companies are equally concerned, they also worry about employee loyalty and controlled access to information and IT resources.

**MiBiz: Do you find a lot of first adopters in this area, or do businesses in this region tend to opt for the 'tried and true' technology?**

**Babuska:** Generally speaking, 'tried and true' is the preferred route. The Midwest is somewhat conservative and most clients in West Michigan would prefer to speak with another customer regarding your product or service performance, rather than being on the "bleeding-edge."

**Brophy:** Clients in West Michigan are what I would call "business smart progressive". They will move to technology that makes sense for the business. For example, there is high interest today in technologies like Exchange 2007 or OCS 2007 as a first step, and likewise MOSS 2007 as a collaboration platform.

**Clark:** Most of our clients simply rely on us to provide the answers. If it's on the newer cutting edge we tell them and most are eager to be ahead of the curve instead of behind it. As long as the word "iffy" doesn't enter the picture, why not?

**Hoy:** I find this area to be more conservative when it comes to the introduction of new technology. We see a lot of our customers in this area as the 'tried and true' technology users. They're not ready to be a beta tester for a newer untested technology.

**Krings:** The West Michigan business area is very careful in adopting bleeding edge technologies. The efficiencies and ROI are generally not yet clearly defined within new offerings, and organizations tend to take a more conservative approach towards them.

**Lough:** 'Tried and true' rules the day.

**Paalman:** Most businesses we work with are looking for reliable technology. There are certainly the 'pioneers' out there. However, we continually advise our clients to let us be the guinea pigs.

**Rajgarhia:** There are very few first adopters in West Michigan. Businesses tend to opt for existing technology

**Roerig:** Most of our customers are first adopters. Due to the limited installed base for manufacturing systems, 'tried and true' technologies are too often obsolete and uncompetitive.

**Schaap:** I think people are realizing that 'tried and true technology' is really a myth. Slowly but surely West Michigan business' are beginning to look at the technology around them and thinking of some extremely creative ways to use it.

**MiBiz: Look into your crystal ball. What hot new security technology and/or IT trends are you watching?**

**Babuska:** Security and Unified Security Gateway appliances that minimize the risk and maximize system availability and up-time are on constantly on our radar screen.

**Brophy:** According to one of our NuSoft experts, Phil Kane, one of the biggest IT trends is Virtualization.

**Hoy:** We are currently keeping a close eye on the handheld and Smartphone technology that is being utilized with today's email systems and cell phones.

**Krings:** Self-defending network technologies, mobile device security and its connectivity requirements – over the next 2 years, we will see an explosive growth in the usage of mobile computing environments and their associated applications.

**Paalman:** The buzz we are seeing seems to revolve around a few newer technologies such as: Network Admission Control (NAC), Unified Threat Management (UTM), Intrusion detection/Intrusion Prevention, and Disaster Recovery (DR) plans.

**Rajgarhia:** Biometrics security technology, like eye and face scanning software and software designing trends that will improve the success rate of software implementation.

**Roerig:** Pharmaceutical manufacturing systems will probably adopt more biometric authentication methods as they become more readily available. Use of RFID on the plant floor will be the norm. Local wireless communications with instruments will replace today's custom hardwired connectivity.

**Schaap:** OpenID is something we've been pretty excited about.

**MiBiz: How's business?**

**Babuska:** Business is good! Certain areas are growing faster than others. Currently our Office Technology full-service line of business is performing extremely well and appears to be what customers are looking for.

**Brophy:** We are growing, and will end the year with a strong increase in billable head count. Growth outside of Michigan is faster than growth within Michigan, but West Michigan is very strong.

**Clark:** Business is and has been great. We've grown 50 percent in the last year.

**Fideler:** Over the past year, our book design business has increased 200 percent, and that is work from other parts of the country. Over the coming year, we expect our revenues to increase another 200 percent by expanding the graphic design and marketing communications work we do for corporations and small businesses.

**Hoy:** Business is continuing to grow, although at a slow pace. The Michigan area is not enjoying the business boom that is occurring in other parts of the country.

**Krings:** We are seeing growth in the area of manage services, virtualization, storage and high end consulting.

**Lough:** Great and growing.

**Paalman:** Business is great. We have been extremely blessed with the growth that we have seen. We are definitely growing. We are right on track to opening up a new location in Grand Rapids, and we have job openings in all of our other offices.

**Rajgarhia:** The state of business is fair and we are planning on hiring in this year. There is a potential for growth.

**Roerig:** Business is stable. Our pharmaceutical clients have access to an increasingly diverse "menu" of business and automation choices, including overseas manufacturing. Customer reliance on large, complex, custom systems is gradually being reduced, forcing us to focus on more services as opposed to project execution.

**Schaap:** We've been steadily growing for the past few years and had a nice bump in growth over the past few months.

---

*MiBiz Network*

<http://www.mibiz.com/>

Please read the following information if you are interested in publishing a MiBiz article on your Web site. The following verbage must be included on your site with the article:

COPYRIGHT 2007. MIBIZ.  
ALL RIGHTS RESERVED.

This article appeared in the **Monday, June 11, 2007** issue of MiBiz, read by upper management executives in West and Southwest Michigan. Print subscriptions are free to qualified individuals who are employed in West and Southwest Michigan. For further information about MiBiz, visit [www.mibiz.com](http://www.mibiz.com). (A link to MiBiz's Web site is required).

PLEASE NOTE: Since MiBiz retains the copyright for the article, it must be published AS IS, with no revisions unless you receive permission from the publisher.