

Online report sponsored by:



COLLABORATION TOOLS

Let's talk about it **s2** | Status update: We own it **s3**

Can you see me now **s4** | Choosing the right service provider **s5**

My data in the clouds **s6**

Feature articles & full report available for download at:

www.GCN.com/CollaborationTools



Let's talk about it

Wikis, which are internal or external websites developed collaboratively, function as repositories of institutional information for companies and organizations. Users add to or edit wikis in a crowdsourced style, and anyone with permission can access them with a Web browser. Some might see wikis as yesterday's news given the fact that they were first developed in 1994. However, as a collaboration tool, wikis can still provide significant benefits.

"Using collaboration and social software for innovation is still a massive opportunity," says Sameer Patel, founding partner of the Sovos Group, a San Francisco-based consulting group that specializes in social and collaborative strategy and technology planning. "We're starting to realize the best ideas don't come out of research and development, and tools like wikis help more people be involved in ideation."

Collaboration is especially important, according to a Forrester Research report in March, "The State Of Collaboration Software Implementations: 2011," because today's workforce is largely decentralized. According to the report, 43 percent of information employees work from multiple locations during the course of a month. This might be why, according to the same report, 42 percent of respondents surveyed say they are spending more (as per Forrester Citations) on social tools such as blogs or wikis in 2011. There are many examples in the government world, said Geoff Weber, a principal at professional audit, tax and advisory services provider KPMG's federal practice, and all allow users to provide information to one another, collaborate and share lessons learned. Still, some agencies are concerned about wiki content, he said. "How do you control what's posted and what information is provided? Yes, wikis allow for quick online knowledge sharing, but the downside is that it allows anyone to post and share," said Weber. In some cases, wikis can also lead to a consensus of opinion — right or wrong — being seen and disseminated as fact.

A measured approach

For these reasons, said Claude Baudoin, a senior consultant at Arlington, Mass.-based IT consulting firm Cutter Consortium, organizations must put controls in place before implementing any wiki. To start with, the software, whether it is installed on premises, in the cloud or on an existing software installation such as SharePoint, should be set up so entries cannot be made anonymously. "They should be identifiable by contributor because, in doing that, it creates a sense of responsibility," he said. This means that new entries as well as edits of existing entries should have author information attached. The lack of authorship data has, in the past, scared some

corporate and government users away from implementing wikis.

"This was fueled by Wikipedia, where anything confrontational, such as entries about politics, had to be locked because you'd have people deleting and editing each other's input with negative results," Baudoin said.

Organizations might also want to assign someone to oversee the wiki as its site editor. A previous employer of Baudoin assigned leaders to its wikis. These people took a governance role, checking the site to make sure new entries were categorized correctly, well-written and factually correct. Employees felt comfortable using the platform, so participation soared, said Baudoin. "We ended up having a wiki that saw more than 12,000 entries over the course of 18 months, and 1,800 of those were abbreviations and acronyms," he said.

The wiki was extremely useful in that it accelerated the learning curve for new employees and helped boost the productivity of existing employees because they didn't have to stop and explain company-centric terms and knowledge, he said. "It becomes a blog about the arcane."

Another must-do for new wiki implementations: parameters about what should and shouldn't be included, KPMG's Weber said. Employees should have an explicit description about what goes into a wiki and what should be left out, and it's always a good idea to include popular and commonly-referenced links and materials. A wiki created by a health care-related government agency might define the term "CRM" very differently than one focused on education. Both might provide a similar basic definition, but then they would be differentiated based on how each uses CRM. "You might include some text that says, 'If you need an account, here are the people you need to contact, and here's the link to the user log-in page,'" Baudoin said.

Finally, there should be some incentive to get users inspired and excited about the use of a wiki, even if the only benefit is being able to save time, as is the case with a recent wiki pilot project by the General Services Administration, Weber said. That wiki, named BetterBuy, functioned as a public outreach collection tool that allowed the agency to collect feedback from potential contractors about a procurement platform in testing. It was well received because it allowed the agency to work out details about upcoming contracts and provided a level of transparency that was not possible in the past. "It was a tremendous mechanism to reach out and streamline the process," he said. ▲



Status update: We own it

The amount of time it takes for people to write something directly correlates with the responsibility and care they take with the content, or so says Mark Diamond, president and CEO of Contoural Inc., a records management and litigation readiness services provider.

“When we used to go out and write stuff on paper, we tended to take care of what we wrote. Now, people are firing off tweets and Facebook statuses without thinking at all,” Diamond said.

That also is true for content written under the auspices of other collaboration tools and technologies, such as text messaging, e-mail messages, wikis and internal message boards, he said. When you couple the user’s lack of care with the IT department’s equally as disturbing lack of litigation readiness, it becomes fairly clear why some government entities are spending millions on e-discovery costs.

“Government entities need to be very concerned about e-discovery, or what we call litigation readiness,” Diamond said. “You need to know what you have and where it is if you’re going to be successful with litigation. A lot of people in government feel like it doesn’t apply to them because they don’t have to follow [the] Sarbanes-Oxley [law] or that litigation doesn’t happen in the public sector, but it absolutely does.”

Indeed, it’s become fairly clear that anything an employee posts in a collaborative forum, including Facebook or Twitter, might be subject to e-discovery or the Freedom of Information Act, said B.A. Boit, principal at professional audit, tax and advisory services provider KPMG’s forensic practice. “The way things are moving, SharePoint wikis and blogs are company records, and [the IT department] has to understand that they will lead to legal exposure if they are not managed correctly.”

There are several problems with the content. The first is that most IT organizations don’t know where these electronic documents reside, so they don’t have an efficient way of creating a legal hold or freezing everything in time and space so it can be produced in court.

Another problem is ownership. People don’t realize that anything they write that’s work-related can be subpoenaed. “Employees and

some employers think something like a Facebook status is private, but the courts are saying that it’s not,” Diamond said. Finally, as the amount of data that’s being stored and archived explodes, there’s a problem with IT aggressively deleting texts, e-mail messages or other documents to make more space available. In some cases, it will shut down internal access to instant messaging. “But that will only drive the use off to the employee’s cell phone or private laptop,” Diamond said. “Instead of doing that, it’s much smarter to think about how to control it.”

Reining it in

Risks can be mitigated by putting careful governance policies and procedures in place, starting with assessing the appropriate level of risk that an organization can manage, Boit said. How likely is it that something an employee or contractor says could be exposed to the world, and what effect could it have from a legal standpoint? Once you know your risk, it’s time to invest in controls.

There are products and tools that lend themselves to properly archiving, logging and retaining wikis, text messages, e-mail messages and social media postings that include what’s placed on a Facebook or Twitter page. All sensitive data should be archived and maintained in a way so it can be searched and delivered if needed. If there’s any confusion, agencies should go to their vendors for help with controlling the different types of media that include archiving, surveillance and monitoring.

The next and often more difficult step will be implementing softer controls, such as employee training and consent agreements. “Employees must be put on notice that when they access wikis and collaboration tools not only can their work computer be reviewed but also the fact that their personal devices can be subpoenaed,” Boit said. “The same thing goes for instant messages and text chats, which can be logged and stored.”

And all these controls must be done in conjunction with the oversight of an in-house counsel, Boit said. “WikiLeaks opened everyone’s eyes in a big way,” he said. “With people posting confidential material on open data sources, this is not a trend that’s going to go away.” ▲



Can you see me now?

Wireless carriers are pointing to videoconferencing as a way to differentiate their offerings. The fact that anyone at any time can engage in a video chat is proof that their networks are robust.

But marketing buzz aside, this development is big news for businesses and organizations that are spending big bucks on enabling this capability in-house: They might not need to install and maintain dedicated rooms or equipment anymore. In some cases, a mobile device and a fast connection might be all they need to stay connected.

That's not to say that IT departments aren't making the investments anyway. According to a March Forrester Research report, "The State Of Collaboration Software Implementations: 2011," 29 percent of businesses are "upgrading or building videoconferencing suites" this year as part of a broader trend to improve real-time communications. These additions will bring the number of videoconferencing-enabled enterprises to 62 percent in the next couple of years, according to the report. The bottom line is that executives place a lot of confidence and importance on video as a method of communication.

The main reason is that video conferencing can provide financial and business benefits such as include reduced travel costs, deeper engagement between those communicating, better project management and improved user satisfaction. "Video fixes people's attention. When you're on the phone, your attention might move around; you can multitask," said Claude Baudoin, a senior consultant at Arlington, Mass.-based IT consulting firm Cutter Consortium. "You can't do that with a video conference, where you're making eye contact with the other person."

How we've arrived

A lot has transpired to make mobile videoconferencing a reality, said Catherine Clary, director of federal sales at Verizon Wireless. "The key to making videoconferencing work is 4G," she said. "You need

low latency and fast network speeds." Indeed, all wireless carriers have transitioned or are in the process of transitioning to network standards that significantly improve on the speed of 3G, with some touting speeds as fast as 10 times the rate of the previous technology. Device manufacturers have followed suit, adding features such as dual cameras that enable videoconferencing.

Now that the carriers and equipment vendors have built the underpinnings, IT managers need to do their own work before giving the go-ahead for mobile video-conferencing, Baudoin said. For one, not every employee should be able to video conference on the fly, he said. "Videoconferencing in public places can create very real, very big privacy issues. If I am an IT manager I would be very concerned about someone who is in possession of confidential or sensitive information, or someone who might be conferencing with someone who might discuss or disclose the same. You don't want someone to be sitting in an airport talking about something that should never leave the office."

There are also limitations to consider on the device side. Cameras typically don't have stands, so video quality is at the mercy of how still people can keep their hands during a discussion. "You don't want to make someone seasick on the other side because you're moving around while talking to them," Baudoin said.

Finally, there are data and network security concerns. Although the networks have encryption technologies built in, what happens if someone is connecting via Wi-Fi? That video is essentially unprotected unless controls are put in place ahead of time, Clary said. This may be why so many are making the videoconferencing investment in-house, she said. "What the IT managers are doing is taking a careful look at what the capabilities they want to enable so they can make sure it's being done securely and that nothing that is sensitive will leave their organization," she said. "It's not as simple as saying everyone has capabilities, so let's make it happen. There is no one-size-fits-all solution." ▲



Choosing the right service provider

There was a time when engaging a new service or software provider was all about cost. Now, with the various types of software — such as cloud-based and open source, to name a few — and very real differences in service offerings, cost alone just doesn't cut it anymore.

Today, what you install and which network you connect to must be based on needs first and foremost, said Sameer Patel, founding partner of the Sovos Group, a San Francisco-based consulting group that specializes in social and collaborative strategy and technology planning. “Based on the RFPs I’ve seen, people are making premature decisions without having spent enough time on the requirements, and that’s having a big impact on the success of software implementation,” he said. “People aren’t spending enough time thinking about what the chance of gaining participation are going to be. Will employees use the software or service you’re installing? How will it integrate with your existing software and services? Can your IT department handle support? These are issues that people need to be thinking about.”

One expert suggests bringing in a project manager with expertise in software and service who can help you ask the right questions. “Having a project manager on board can provide quality assurance throughout the process to make sure you’re hitting all the right points,” says Geoff Weber, a principal at professional audit, tax and advisory services provider KPMG’s federal practice.

What’s your location?

Of course, after a decision is made, some logistic concerns will pop up. The way people are making choices today might not be the best way to go about it. Figuring out which option — on premises, open source, cloud-based — is best has little to do with the actual technology, Patel said. “Really, what you need to do is have a strong

handle not on the promise of technology but on the inefficiencies of your organization. Folks love to jump into the benefits of software and the value that can come out of it without credibly laying out the problems of what’s in their systems today.”

For example, a cloud-based service might seem like the way to go. But if it will require a lot of expensive and time-consuming implementation work, especially if there’s an on-premises option available that’s compatible with your existing software, it might not be the best option. IT departments, working in conjunction with those in the line of business, must discuss what specific integration is needed between existing systems and new software. In many cases, it may even be beneficial to speak with users who typically know how they’d like to solve their problems.

The next step is deciding which type of vendor to use. In the collaboration market, four camps of vendors are out there: pure-play software providers, enterprise resource planning vendors that build in collaboration tools, specialist vendors that sell services and software, and unified communications vendors that integrate collaboration tools with existing communication platforms.

In many cases, new collaboration implementations will also require new or expanded wireless connectivity for off-site employees or contractors. Connectivity providers should also be evaluated based on need. But in this case, IT managers must delve deeper than published speeds and feeds for a particular network. A provider might have 4G service in specific cities but have limited coverage where remote workers are located. It’s only after all of these things are addressed adequately that an organization will see success, KPMG’s Weber said. “There’s a lot of attention in the federal space to failed IT projects,” he said. “How you develop a new project is really most critical.” ▲



My data in the clouds

How do you balance the need for freedom and collaboration with a mandate to secure the network and its data? This is something that's been facing IT managers across every level of business, especially as collaboration tools and corresponding data move out of the corporate environment and into the cloud.

In the past, organizations that allowed collaboration did so in the confines of the network, blocking access to external collaboration tools. In many cases, they limited use of the tools even inside the network, allowing only managers or specific departments to instant message or create and post to discussion boards. However, during the past year, the visible benefits of collaboration tools have made it impossible to exclude specific employees from collaboration tools, and a quick look at some of the most popular collaboration tools bears this out. Programs such as OpenView Venture Partners' AtTask project and portfolio management software, Salesforce.com's Chatter, 37signal's Basecamp, and Microsoft's SharePoint Online all live in the cloud and can be used by almost anyone on staff.

However, unfettered use, especially in the cloud, creates specific security and privacy problems. For one, unless a collaboration tool has the inherent ability to create groups and specify rights, users might gain access to topics and discussions that they are not authorized to see. Considering how easy it is to copy and paste text from a browser, it's not difficult to see how such access could create a WikiLeaks-size problem very quickly.

The open nature of collaboration tools might also contribute to finger pointing. Some tools allow people to edit and change files and intellectual property without authorship. Although many wikis or group document-sharing sites have version control, there are common ways around it, which could lead to problems. Online

communities such as wikis or forums can also give rise to heated discussions or personal insults. Finally, surreptitious viewing of calendar tools might lead to employees goofing off, such as taking a 90-minute lunch when supervisors are out of the building.

It is possible to avoid those problems even when collaboration applications are open to the general population, though. One strategy is proactively enforcing a governance program, said B.A. Boit, a principal at professional audit, tax and advisory services provider KPMG's forensic practice. "The best defense is to put into place confidentiality policies and software that has an archiving capability to whichever collaboration tools you have installed can be searched across," he said.

To promote responsible posting and civility, Sameer Patel, founding partner of the Sovos Group, a San Francisco-based consulting group that specializes in social and collaborative strategy and technology planning, suggested that organizations also must have a strong identity management policy in place so employees are familiar with one another and less likely to post or interact with one another without thinking. An identity management program will also make it easier for like-minded employees to link together and collaborate on projects, he said. "When you think about having that level of rich meta data about the people who are at an agency or the external contractors you work with, it's far more likely that the best minds are going to find each other."

Finally, every organization should engage in a formal training program that encompasses best practices around collaboration tools as well as the internal and external use of social media, Boit said. "Social media and collaboration [governance] isn't a technical challenge anymore," he said. "Information flows out of the weakest link, and that link is usually an employee." ▲



Network details and coverage maps at vzw.com © 2011, Verizon Wireless.

A FAST CONNECTION HELPS A FAST RECOVERY.

Track equipment and people in the most chaotic environments so you can focus on the task at hand. With a mobile public-safety solution enabled by Verizon, you can set up a wireless network right where you need it, helping you coordinate interagency efforts on site and in the field. Clear lines of communication are critical when coordinating recovery efforts, and clear communication begins with the largest high-speed wireless network in America.



VERIZONWIRELESS.COM/GOVT

1.800.VZW.4BIZ

MOBILE BROADBAND

MOBILE PUBLIC SAFETY

MOBILE CARE

MOBILE OFFICE