CIOs Struggle With Social Media's Security Risks

Cindy Waxer | February 11, 2011

When a deadly tornado touched down in Cincinnati, Ark., last New Year's Eve, state officials could have relied on typical channels like TV and radio to warn citizens of dangerous road conditions and weather patterns. Instead, the Arkansas Homeland Security and Preparedness Agency chose to tweet up-to-the-minute storm reports. The result: "We were overwhelmed by the level of volunteers who came in to support our citizens in their time of need," said Arkansas CTO Claire Bailey. "We had to turn people away."

Welcome to Government 2.0. In an era of Facebook, LinkedIn, YouTube, Twitter and blogs, more government agencies are embracing these social media tools to communicate with citizens in real time and supporting internal collaboration. In fact, 66 percent of all government agencies currently use some form of social networking — from blogs and wikis to instant messaging and discussion boards, according to a recent study from the Human Capital Institute and Saba. And 31 percent of counties and municipalities surveyed have embraced social media as a more efficient customer feedback channel.

“Government’s mission for centuries has been to reach citizens on topics, whether that’s in person, at town halls, through letters or signs on street corners,” said Steve Ressler, president and co-founder of GovLoop.com, an online social networking site that connects government innovators. “Part of government’s role is to get information out to citizens and get their feedback. Social media is one of the No. 1 tools people want to use right now.”

Photo: *Steve Ressler, founder and president, Govloop*

A Heated Debate

But while social media can be used to warn citizens of an approaching tornado, another storm is brewing around government’s use of social media and the potential security risks. Phishing scams that convince users to perform a task that launches a malware attack and unwitting employees who reveal state secrets on their personal blogs are just a few ways social media presents enormous security risks.

“If you make social media available to hundreds of public employees, you have acceptable use issues, people having to be sensitive to what should be public information and what should not be, and people speaking on behalf of their agencies when they shouldn’t,” said Charles Robb, a senior policy analyst at NASCIO. “ Plus, you’ve opened up a whole new point of entry into your network.”

Even the Pentagon is grappling with what role social media should play in government circles. Despite rumors of banning sites like Facebook and Twitter altogether, and the recent dissolution of its social media office, the Pentagon is currently reshaping its social media policy format to better integrate these services.

And the Pentagon isn’t alone. As social media becomes a critical component of any communication and collaboration strategy, more federal and state agencies are rethinking their philosophy on these controversial tools. Rather than simply wring their hands, the true trailblazers are discovering a multilayered approach that maximizes social networking's benefits while addressing critical security concerns.

A Multipronged Approach to Security

At the core of any solid social media plan is training, according to Ressler. "Agencies need to start thinking about providing more training and education on proper use. There will always be that 1 percent — that person in Iraq who posts a photo on Facebook or something they shouldn't," he said. "It's about training people on proper behavior."

Bailey agrees. To get her department up to speed, she hired Boot Camp Digital, a social media and Internet marketing training agency that offers courses, seminars and workshops on managing social media. Lessons ranged from teaching public information officers the finer points of creating social media content to giving the agency's information systems personnel a crash course in more technical aspects such as network security. Through formal training, Bailey said the agency reassured technology employees who might fear the security risks of sites like Twitter and discovered how the state could better utilize social media.

For Terry Bledsoe, CIO of Catawba County, N.C., and an active Twitter user, social media education isn't something to be taken lightly. An IT governance committee comprising representatives from across the county meets monthly, supervisors participate in annual training sessions to update their skills, and new hires are informed of the agency's social media rules and regulations.

Bledsoe doesn't believe in a cookie-cutter approach to teaching safe social media practices. Because fresh-faced Millennials, or 20-somethings, make up 10 percent of Bledsoe's own staff, he says he's careful to recognize the varying degrees of understanding of social media's inherent risks among disparate age groups. "The Millennials are a lot more active on Twitter and Facebook," he said. "They've grown up with this technology, so they're able to flex as things change, whereas the baby boomers get on Facebook and they don't really know how to address security."

Promulgating Policy

Carefully crafted usage policies can help bridge this generational divide by addressing employees' behavior regardless of age and offering strict guidelines on how to mitigate social media security risks. That's not to suggest, however, that there's a standard template for social media policies. Rather, agencies must cherry-pick the controls that best meet their unique security concerns.

For example, Bailey, whose department currently is drafting a formal social media policy, has stipulated that "the only people who will have access to update our social media site, or deliver messages to it, are within my communications team." By limiting access, Bailey said she can better monitor the types of information made public while ensuring that what's being communicated represents the state of Arkansas rather than personal opinion.

Nevertheless, Bailey said agencies statewide will be encouraged to create their own social media policies versus abiding by a single set of rules. “We want to make sure the social media policy is developed by each agency so they can align it with their Internet acceptable use policy,” she said.

Bledsoe also established tight controls on social media that require employees to gain approval before joining the social media sphere. “Any department that wants to set up a Facebook page, Twitter account, or even a Web page has to go through the public information officer’s office,” he explained. “We don’t just set up a profile because somebody would like to have one. We make sure that there is a benefit to the organization.”

Separation of Self and State

However, as more employees bring their BlackBerrys to work and their laptops home, the line between personal and business is becoming increasingly blurred. As a result, many employees risk exposing an agency to major security breaches by divulging seemingly innocuous details about the workplace via Facebook or LinkedIn. Take, for example, the disgruntled state worker who expresses his frustration on Twitter about a network that’s been down for hours. Although it’s a public airing of a common occurrence, for a government agency, it’s an open invitation to hackers.

To keep employees’ priorities in check, Bailey said that all employees in her Department of Information Systems sign annual confidentiality agreements. “The day-to-day things that we do in our jobs are bound by the confidentiality agreement, and I trust and educate my employees.” Still, she admits, “people can make mistakes.”

Making matters even more difficult is striking a balance between agency security and employee freedom. “You have to respect the privacy rights of the individual and their basic individuality,” Robb said. “At the same time, government employees need to consider who will see what information.”

Software Solutions

Luckily managing technology is much easier than curtailing human behavior. Today there are countless network security technologies available that provide a secure line of defense against ill-intentioned intruders. From monitoring and threat-detection tools to blocking and Web filtering technologies, state and local agencies now have a growing arsenal of weapons to choose from.

That’s good news given the network and system vulnerabilities that social media tools can create. After all, just as a single tweet can reach millions of people at once, a single worm or stolen password can rip through an agency’s computer infrastructure like a wildfire.

“Social media is an opportunity for malware to come into an enterprise, as well as an opportunity for spear phishing attacks where a message is crafted to a specific agency and an individual is targeted to obtain certain information,” warned David Thompson, group president and CIO at Symantec Services Group, a security software and services firm. "Data loss can also occur where someone inadvertently attaches a file that he or she thinks is their resumé but, in fact, it's a list of confidential missions or programs."

But that's not all. Because computer viruses are best known for spreading via e-mail, employees using social media tools may be likelier to "let their guard down or wear their consumer-at-home hat when they're actually in the office," said Thompson.

For this reason, Bailey admits to "constantly looking for a best-of-breed tool so that if my computer gets infected, and I send someone a link that says 'Check this out,' and she clicks on it, we have technology in place that blocks that infection." Besides, she added, "Today's security tools have to keep up with the hackers and malware providers who are out there working 24 hours a day, 365 days a year to bring us down."

In fact, some would argue that without anti-virus, data loss prevention and scanning tools, a social media presence simply wouldn't be possible for a public agency. And that, Thompson fears, would have a disastrous impact on the government's ability to recruit skilled professionals, especially Millennials.

"I would hate to see us lose talent or not be able to attract talent into our armed forces because we restricted it so much that they can't actually communicate," Thompson said. "There's some great talent that, with the right training and the right protections, can use these social media tools and still accomplish the mission."

The Importance of Teamwork

Working alongside social media providers is another tack government agencies are adopting to safeguard their systems and data while delving into Web 2.0. In early January, NASCIO and the National Association of Attorneys General (NAAG) struck a deal with Facebook that required the social networking giant to revise its service terms for state government use. After months of negotiations, Facebook agreed to modify the provisions of its terms and conditions regarding dispute resolution and indemnity clauses.

"It's critical that providers of social media tools understand their responsibility in how their tools can definitely impact a government agency," said Bailey, who is also a NASCIO executive committee member. "From a public-service perspective, we were very happy for Facebook to work with us because these are tools that not only help their company but also the delivery of government services when used effectively."

So too must an agency's human resources and IT personnel work collaboratively to ensure that the right policies and technologies are in place to minimize security risks. After all, intrusion detection software is only as effective as the employees who use it. "Human resources and IT have to work together," Robb said. "It's often a partnership, but a joint governance structure needs to be established to do that most effectively. There are certainly aspects of human resources policies and procedures that CIOs are not going to have comparable expertise in, but they can still contribute a lot to the knowledge of [social media] tools and how they'll be used or misused."

In the end though, the greatest risk of social media technologies may not be a breach of security, data loss or a denial-of-service attack. Rather, the most significant threat is not using social media at all. "There's a huge risk if you're not active in social media channels," Ressler said. "For example, if your brand is being beaten up or if there's a great conversation going on and you're not a part of it." By banning social media outright, federal and state agencies risk frustrating their constituents, alienating potential recruits, and stepping away from an opportunity to set the record straight or better inform the general public. And that's a conversation worth having despite the security risks. ¨

Cindy Waxer is a journalist whose articles have appeared in publications including The Economist, Fortune Small Business, CNNMoney.com, CIO *and* Computerworld.

http://www.govtech.com/pcio/CIOs-Social-Media-Security-Risks-021111.html