Communicating During a Cyberattack:
The Next Crisis Frontier for Cities

by Scott Summerfield, Principal, SAE Communications

California is in the midst of one of its most crisis-filled periods on record, and it seems as if we're perpetually managing fires, mudslides, drought, and more – at the same time we're focused on community resiliency. But one "crisis of confidence" lurks within every city and has the potential to cripple operations and destroy public confidence – cyberattack.

Local agencies are a favorite target since they often haven't created safeguards. Think about what can happen if a cyberattacker seizes control of your data and your systems, whether it's theft and public release of information or a ransomware hostage situation. Resident/customer information, billing and payment systems, 911 dispatch, human resources and payroll records, legal documents, traffic controls, and countless others can go offline or become inaccessible in an instant.

Your network and systems are only as strong as their users, and most attacks are the result of staff members inadvertently clicking on a dangerous email rather than organized internal or external system breaches. Suddenly your most-sensitive information is open to the world, with your internal and external stakeholders blaming you for allowing it to happen.

How much risk do we face? A few recent numbers tell the story:

- **$8 billion** in damages caused by ransomware
- **3 billion** records leaked or stolen
- **$8 million** average cost of a US data breach

The risk is clear. The responsibility for councilmembers and staff leadership is to reduce it through strategic planning and effective communication.

We recently were invited to participate in an IBM Security Cyber Range simulation in a Cambridge, MA facility designed specifically to help organizations recognize what happens when cyberattackers strike. Along with a small group representing some of the world's largest financial and insurance services companies, we experienced how a cyberattack unfolds and how to manage organizational and media responses. Using a broadcast TV studio, a social media simulation platform, and other eye-opening resources, IBM's experts stressed that we must consider our actions to be a business response tied to a security culture, not a technology response. And leadership is a vital part of keeping our businesses – our cities – operating in the wake of an attack while every aspect of our organization is scrutinized.

Communications is at the top of a successful cyberattack response – along with a clear pre-crisis understanding of all city database vulnerabilities – and city leaders and communicators are just as important as those who investigate what happened and restore services. Cybersecurity experts consistently note three inviolable communications guidelines:

- **Openness with those affected**
- **Transparency in explaining what happened**

- **Honesty about the attack's scope**

Sadly, those tenets are frequently missing from cyberattack responses, and bad situations are made worse by a communications vacuum, rumor, innuendo, and fear.

Your stakeholders will express a range of feelings – outrage, disappointment, worry, and confusion – and will ask pointed questions. How did you let this happen? Are my kids safe? Is my credit impacted? How are you going to get services re-started? When will things be back to normal?

The City of Atlanta has budgeted nearly $10 million to recover from its ransomware attack last year which shut down most City operations for two weeks. Considering the attackers' first ransom request was for about $50,000 and the City had warnings for several months before the attack, we have a lot to learn from how this crisis was handled and how it could have been prevented.

Analysis of the Atlanta case reveals several important considerations for city leaders who will someday face their own nightmare:

- **Risk Builds Over Many Years** – City officials were warned by an independent auditor eight years before the attack that insufficient funding for business continuity and disaster recovery plans; attackers often have access to systems for several months before taking action
- **It Won't End Soon** – Several months after the initial attack, more than a third of the City's software programs were still offline or partially disabled, and nearly a third of those were considered "mission critical"
- **Finger-pointing Will Linger** – City officials continue to blame each other for the attack, undermining public confidence in City operations; pundits throughout your community will also second-guess your security measures and response efforts
- **Paying Ransom is a Tough Call** – It's easy to armchair quarterback the City's decision to not pay ransom (especially given the relatively small initial request vs. the amount spent on recovery), but refusal to give in to criminals is an understandable reaction
- **Contact with Hackers Can End Quickly** – Once law enforcement agencies get involved, criminals may abandon their ransom request in an attempt to elude identification and capture; this leaves the city with no choice but to rebuild its systems from backups – if they exist
- **Explaining "What Happened" May Be Difficult** – Investigating agencies may limit communication about the cause, especially if known international hackers are suspects; this information void feeds the rumor mill and impedes the city's ability to fully inform its stakeholders

This list of Top 10 tasks can help your city prepare for and respond to an attack:

1) **Know Your Exposure** – meet with your information management staff and department heads for an in-depth and brutally honest discussion about your city's cyberattack vulnerabilities
2) **Be a "Nudge"** – communications is one of the most important elements of a viable cyberattack response, and as a city leader (whether elected/appointed or staff) your input must be part of the response, even if it means sometimes being a pest; continually ask tough questions about the attack's scope and recovery progress

3) **Prevent An Attack From Happening** – craft an education program for staff centered on spotting phishing and other attack triggers in personal email accounts; this behavior will carry into the workplace
4) **Highlight the Risk** – ensure that staff understands the potential damage to your city and those you serve, recovery costs, and the hit to your credibility when information is stolen or held hostage
5) **Focus On New Hires** – include cybersecurity in orientation materials and briefings, and emphasize your city's commitment to the protection of its information
6) **Plan Your Response** – make sure your emergency response and crisis communications plans include cyberattack; don't forget about your staff, which will be affected in many ways
7) **Identify Your Team** – chaos will likely ensue when you're attacked and you'll need to immediately gather your designated crisis response team, including your local FBI, DHS, Secret Service, and other partner agency contacts; pull your team together and build relationships now, as you won't have time when the attack hits
8) **Anticipate Outrage** – your stakeholders will be angry and confused…and communicating with heartfelt empathy will help you tell your city's response story more effectively
9) **Prepare For Questions** – though each attack is different, you can begin drafting your answers to questions you're most likely to be asked by your stakeholders and the media and then modifying as necessary when you become a victim; identify your attack-related spokesperson and train them for a high-visibility response
10) **Create Response Documents** – develop cyberattack holding statements, pre-prepared social media posts, news releases, and staff communication scripts that are written in plain language and can be deployed quickly

Don't forget to tell your resiliency story whenever possible. Our stakeholders expect us to anticipate bad things, and we can increase confidence by noting our challenges, highlighting what we're doing to keep information safe, and committing to honesty when something happens. You have a variety of tools to build confidence, such as scheduling a policy leader update, holding community and staff forums, spurring an online discussion, and pitching a media story. The more we focus on cybersecurity, the less likely we are to become victims.

We all know that good planning is the foundation for a good response. With just a bit of effort – and a deep understanding of our vulnerabilities – we can take the necessary steps to keep our cities safer when the data thieves pay us a visit.

Scott Summerfield is a principal of California-based SAE Communications and has provided communications counsel, media relations, and Joint Information Center management for many of California's most challenging recent disasters and crises of confidence.