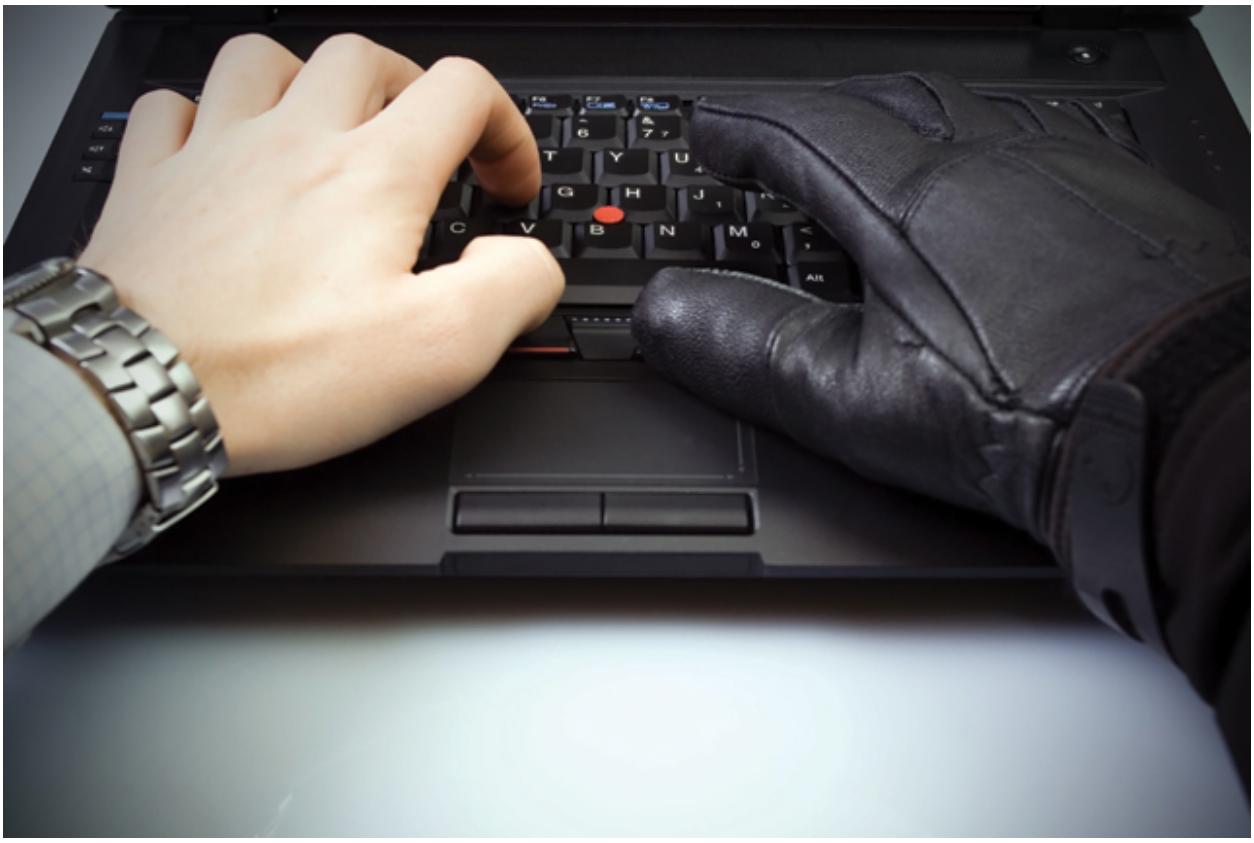
Emergency Agencies Prepare for Cyberbreaches to 911 Systems

Adam Stone | January 21, 2014



Emergency planners routinely think about the outside world: What if that building fell to a natural disaster or man-made attack, or that neighborhood flooded? What if hackers disabled that water plant or took out the power grid?

Now turn that same question inward. What if they struck against you?

Consider cybercrime, one of the fastest-growing forms of social malice. Victims in the news typically include banks, online commerce and political targets. But hackers have taken aim against government institutions as well, and it's not a far leap from there to imagine an attack against first responders themselves. It's no sci-fi scenario to posit an attack against a 911 system, an emergency response center or police resources.

In fact, the threat is very real, and today's emergency managers are tasked with ensuring not just that their systems are rock-solid, but also that their response plans are in place.

The Ohio Emergency Management Agency gives credence to the possibility that its own systems could someday come under cyberattack. The agency actively plans for such an incursion and thinks hard about remediation, said spokesperson Tamara McBride.

“We’re sitting down with our cyberworkgroup and discussing just that question. We’re very focused on the consequences of those threats,” she said. Suppose the department’s own communications systems were sabotaged, leaving no ready route to connect with citizens. “Do we go door to door? Do we go up the street with a bullhorn or reach out to ham radio volunteers? Those are all the things that are on the table.”

Maybe the bullhorn sounds excessive, but a range of experts say it would be hard to be too prepared for an attack that went to the core of emergency operations.

First of all, let’s admit there’s a threat. Starting at the top of the pyramid, the number of significant cybersecurity events against the U.S. government increased 680 percent over a five-year period, from 5,503 in 2006 to 42,887 in 2011, according to the U.S. Government Accountability Office.

So there’s clearly vulnerability within government. But does that trickle down to the state and local levels, specifically to emergency operations?

In Spartanburg County, S.C., a recent cyberattack flooded nonemergency phone lines, pushing calls over onto the 911 system, potentially jamming the emergency system and slowing dispatchers’ ability to respond to crisis calls.

Indianapolis Public Safety Director Troy Riggs paints an even grimmer picture. Speaking with local reporters after a forum on cybercrime, he offered a scenario in which an attack on first responder systems coincided with a terror attack. Essentially the idea is to detonate a bomb, then flood 911 call systems or cripple essential computers to stop responders from heading to the scene. It’s a techno-driven version of a common terror scenario in which a second bomb goes off just as ambulances arrive to treat the victims of a first explosion.

Such a scenario is not beyond the imagination. If a physical attack is possible, and a cyberattack is plausible, it would take little creativity to coordinate the two events, punching a hole in the center of response efforts.

Why is this possible? Ironically the steady improvements in emergency communication also have made those systems more vulnerable to attack. In short, it’s all about the Internet.

It starts with connectivity, with shared infrastructure controls, with intranet components and phone systems all increasingly routed through the Internet. “Everything these days is built out of Web technologies, even systems you would not expect to be connected to the Internet,” said Shuman Ghosemajumder, vice president of strategy at Shape Security in Mountain View, Calif.

Connectivity in turn creates ubiquity. Suddenly all our information assets are available through our physical assets: police cars with video recorders and fire trucks with their own Wi-Fi access points. “We have a lot of IT moving around in incident response,” said J.R. Cunningham, director of the state, local and education practice at security program provider Accuvant.

The company has successfully poked holes in that IT, for testing purposes, and Cunningham has concerns about the fundamental stability of the IT components that underlie emergency service systems. “These systems were not designed to be highly secure,” he said. “Generally they’ve evolved over time, with security often brought in as an afterthought.”

While the risk runs through any Internet-connected system, the threat may be particularly visible in the realm of 911. Where news coverage looks at cyberattacks on institutional networks, it often overlooks the threat to telephony, and yet that threat looms large in the emergency management world, where phone systems often are the link in the chain of incidence response.

“As our 911 centers move into a more fully digital world, those 911 centers are going to be vulnerable to those same attacks that have been plaguing other networks, whether they are financial or commercial,” said Neal Puff, senior security solutions architect for the public sector at Verizon Terremark.

For those looking to spur cybermayhem among emergency responders, 911 is an especially attractive target. First, because the emergency phone system offers a single entry point. An attack on a police station may disrupt that station, but a denial-of-service (DOS) assault on 911 could impact literally every emergency responder.

It goes deeper than this. Because 911 now connects to the Internet, an enterprising hacker could in theory get inside the system and feed it bad information, dispatching responders unnecessarily or diverting rescuers to the wrong destination. While a DOS could hold up response, this kind of insider attack — in which a hacker achieves total control over the system — could have more devastating consequences.

Ultimately 911 is critical infrastructure, “and that’s what makes it a possible target,” said Jay English, director of Communications Center and 911 Services at APCO International. While 911 has for years been a “ closed loop,” virtually self-contained and therefore highly secure, “it is still public telephony, public switched networks, and we know there are potential vectors by which bad guys can get to those 911 trunks.”

The potential for damage is significant, Puff said. A hacker intercepting 911 calls could glean names and addresses, maybe personal data about police officers and judges. The location of emergency command centers or the activities of first responders could be disclosed, which could be used as compromising information, depending on the type of emergency.

Puff takes it back to Riggs’ double-punch scenario. “You could set off an explosive device and then if you know in advance where the command center is going to be set up, you can plant another device there and potentially do real harm to law enforcement,” he said.

How will the hackers get in?

There are the usual ways. Someone will leave a password taped inside a desk drawer or lose a laptop.

There are the usual ways. Someone will leave a password taped inside a desk drawer or lose a laptop.

Once they're in, the sky's the limit. An intruder can easily pilfer user names and passwords, opening up all the information contained in the system. Depending on the level of access the hacker has tapped into, he or she can issue commands as an administrator. Such access could give an attacker total control over the emergency apparatus.

It's not all doom and gloom though. For many emergency managers, an ironic touch here will come in knowing that the perpetual budget shortfalls against which they've struggled for so long, now may be saving their bacon.

Vulnerability here comes via the Internet, and widespread Internet connectivity is only a product of the additional management tools and telephone systems. In many cases, the legacy systems you've been too broke to replace are probably far less susceptible to attack. Hardly a resounding win, but some comfort nonetheless.

Another safeguard: Don't assume that connectivity is always a necessity. While it often helps to have an Internet backbone joining systems together, "you need to ensure that every system that doesn't need to be connected to the Internet is not connected to the Internet," Ghosemajumder said.

It helps to have redundancy (think of McBride's ham radio operators) and training is essential. "People need to know not to use their Gmail password on mission-critical systems. If they're not given proper training, the odds are that a lot of them will," Ghosemajumder said.

It helps to have redundancy (think of McBride's ham radio operators) and training is essential. "People need to know not to use their Gmail password on mission-critical systems. If they're not given proper training, the odds are that a lot of them will," Ghosemajumder said.

Whatever approach one takes, the prospect of a cyberattack on emergency management is one that must be faced. "If it hasn't happened yet, it's coming. It has to," Puff said. "If there's a data network, if there's information that people will find valuable or useful, some attempt will clearly happen at some point. It's just the law of averages."