IAEM Bulletin
Disaster Zone Column, September 2018
Topic: Cybersecurity and Emergency Management
Suggested Title: Cybersecurity, Who's job is it?

As emergency managers we have traditionally created an inventory of hazards that our community needs to become ready to mitigate, prevent, respond to and recover from. The list can be a long one with both natural hazards, technological hazards and human caused hazards on the list of "bad things that can happen."

My question for you today is what about cybersecurity as a threat to people, governments, business, industry and infrastructure? Have you added cybersecurity to your list of human caused risks in your Threat and Hazard Identification and Risk Assessment (THIRA)?

In talking to a number of emergency managers I've found that some will say, "This is not a focus for our program." Other agencies or departments are identified as having the lead responsibility.

I acknowledge that sometimes there can be turf issues within a government or organization about who is responsible for what. Your Information Telecommunications (IT) department should have this as a core function for the internal workings of your individual organization, but what are they doing for the broader community, for business, industry, utilities and individuals? It is likely that they are doing nothing at all. It is not part of their narrow mission of providing IT support to your government.

This is where your emergency management function kicks in. Cyber threats are pervasive in today's society, and when you look at your identified list of hazards, it is cyber-attacks that are present 365 days a year. While there should be internal government focused efforts, the external public education and prevention work must include cyber-readiness.

The list of attackers and methodologies continues to grow. One of the more prevalent bad-actors on the scene today are Eastern European criminals who are looking to profit monetarily from ransomware attacks that seize and hold your data, while demanding payment for unlocking your data. No one is immune from these types of cyber-attacks.

I highly recommend that you team with other public and private organizations to hold cybersecurity events and that draw attention to the issue of cybersecurity and what individual organizations can do to protect themselves. Check in with your critical infrastructure owners and operators to find out what they are doing about the cyber-threat. You should pay particular attention to the electrical utilities in your region. I

recognize that most will say that they are “compliant” with all standards but remember “compliance” means only doing the absolute minimum required.

Lastly, I recommend reading the book, Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath by Ted Koppel In our 21st Century world we are totally dependent on electricity. Without it, much of our critical infrastructures will not function due to their dependency on electricity. Our modern society will grind to a halt when the electrons stop flowing. Besides exploring the cyber threat to our electrical grid, Koppel also looks at personal preparedness from a broad spectrum of locations and perspectives.

If you were to prioritize the list of hazards for your jurisdiction or company, the size and scope of impacts would likely help influence your priorities. I recommend you also look at frequency and pervasiveness in making your list of priority hazards. When you do that, cybersecurity should move up the list, and so too your prevention, mitigation and preparedness activities associated with the hazard.

by Eric E. Holdeman, Senior Fellow, Emergency Management Magazine, he blogs at www.disaster-zone.com