

26 August 2024

To: American Radio Relay League (ARRL),
Georgia American Radio Relay League Section,
Georgia Amateur Radio Emergency Service,
Tri-county Amateur Radio Emergency Service

From: B. Greg Colburn Jr., Technical Specialist/GA ARRL Section – N3BYR

Subject: Re: ARRL IT Security Incident – Report to Members (21 August 2024)
(<https://www.arrl.org/news/arrl-it-security-incident-report-to-members>)

I reviewed the above-mentioned report when it was sent to members on 21 Aug 2024 and published on the ARRL website the following day. I reflected on the situation for the past several days, I started my communication journey long before being a licensed Amateur Radio Operator in my early teens. I actively work in a professional capacity as a Cyber Security Researcher, IT Manager, and volunteer time to assist other organizations in these capacities when time permits. I have also given various presentations within the Amateur Radio community on cyber-hygiene practices, technology considerations as emergency communicators, and to the broader community when asked how to actively defend against cyber related incidents.

The American Radio Relay League (ARRL) is supposed to be the organization that helps unite Amateur Radio Operators within the United States. Part of the ARRL goal is preparing operators as individuals and groups to provide emergency communication during disasters. ARRL specialty groups such as Amateur Radio Emergency Service (ARES) put focus on preparation and scenarios that require operators to communicate “When all else fails”. When I was first licensed as a young teenager in the early 90’s, the various faucets of the ARRL and sub-organizations helped expand my knowledge, and in part drove myself towards the career choices I made.


I was disappointed to learn of the IT Cyber Incident affecting the ARRL. Paying a one-million-dollar ransom to recover systems that were previously played as unimportant surprised me. This also reflects on how ill-prepared the ARRL is for modern emergency situations. It appears that the ARRL did not consider cyber-related threats as a serious situation, such incidents can lead to catastrophic communication failures. Technological functionality is a huge part of the day-to-day lives to keep American society and beyond communicating. This makes cyber-actors and cyber-threats a serious topic of discussion, it has been for more than a decade now. Amateur radio operators are a failover for communication in emergencies, but the ARRL seems unprepared.

While I do not have the entire specifics on the ARRL cyber incident, much of the information already reviewed shows text-book methods to compromising any technology resource, “unique” is hardly a descriptor for the breach methodologies used. The incident puts into question whether isolated system backups were ever used or maintained and whether network policies were enacted or maintained properly. Additionally, the overall response and release of information indicates the ARRL was not prepared for cyber-related incidents. Many organizations are using proven methods within their infrastructure to include simple tabletop exercises, ‘What If’ scenarios, firewall and system monitoring, vulnerability patching, network policies, allow-by-exception limitations, and software suites designed to protect server and end-point resources. While I fully expect that the ARRL will use these tools moving forward, I am flabbergasted that there is no indicated use prior to the incident based on the response. Using such a motto as “When All Else Fails” really echoes loudly.

Among the highlights of this cyber-related incident that stick out, the wording and fact that the ARRL paid a ransom to a cyber threat actor is the worst choice and worst outcome for this type of situation. It's little consolation that the ransom came from insurance money, though members may be relieved to a limited degree. Not only does paying a ransom to cyber criminals encourage them to continue compromising systems, but it also emboldens future attempts to compromise the ARRL with the expectation of a payout. These ransoms also fund other threat actors, their causes, and other organizations throughout the world which are typically nefarious. This causes more harm to other non-profit organizations, businesses, and individuals – *IT DOES NOTHING FOR THE GREATER GOOD OF ANYONE*, only strengthens cyber threat actors.

I was ecstatic over a year ago when I was asked by our Georgia ARRL section to fulfill an important role as a Technical Specialist. That role gave me recognition within the Amateur Radio community as someone with specialized knowledge and understanding. Part of that recognition is based on my uses of digital communications, technological knowledge, weak-signal operations, and extraterrestrial-based comms (satellite and EME). This also identifies me as someone hams can reach out to for presentations, questions, troubleshooting, knowledge, and mentoring. I will continue to fulfill those roles as an individual, but I can no longer do so with the ARRL at this time. This serves as my official resignation from my Technical Specialist appointment as well as my membership with ARES organizations. I cannot, with clear conscience, support an organization that appears ill-prepared for emergencies within our modern world and decides to willingly support cyber-crime activities.

In the future, I hope that the ARRL grows and learns from this very painful cyber-incident and puts focus on preventing, preparing, and conquering cyber-crime where it involves the Amateur Radio Community. Amateur Radio is a community of individuals that prepare for emergencies like the one experienced by the ARRL, the community deserves far better.



B. Greg Colburn Jr. – N3BYR
GA ARRL Field Section/Technical Specialist
Central Georgia ARES & Tri-County ARES Member