National Infrastructure Protection Plan
NIPP Challenge

Cyber Risk Management Toolkit for Small Government Entities

SITUATIONAL AWARENESS

According to the National League of Cities, there are approximately 39,000 municipal, county, and township government entities in the U.S., 90 percent of which serve small populations. Another 50,000 special purpose government entities and small school districts exist. These jurisdictions face considerable threats of theft of personally identifiable information (PII) and hacking that would disrupt critical infrastructure services. Unfortunately, the basic cyber risk management tools built for the commercial and nonprofit sectors do not address the subtle but important differences that define small government cyber risks. The cyber risk management solutions that currently exist for commercial and nonprofit entities need to be updated with research, analysis, and models that are unique to small government entities. Applying cyber risk management tools with the correct underlying research, analysis, and models for small government entities will fill an important gap in cybersecurity resources and tools for small government entities.

METHODOLOGY

The project team performed fundamental research on cybercrime statistics cross-sectioned to small government entities. The raw crime data for this research was culled from Federal agencies and open source threat intelligence sources. The project team performed extensive survey work and focus group research that specifically sampled small government entities. The project team also reviewed the risk management literature across small government entities to identify the most applicable risk formulas and valuation models to establish an at-risk profile. The profile, when combined with the appropriate cybercrime statistics, forecasted the potential losses from threat actors utilizing various threat vectors.

Based on the foundational research, the team developed cyber risk management tools to help leaders of small governments address cyber risk from the management perspective. The tools are cost effective, user-friendly, and suitable for use by nontechnical executives who need to establish and integrate cyber risk management into their operational culture. The follow-on effect is that by reducing risk locally, the risk to citizens and larger critical infrastructure providers with whom these smaller entities interface will be reduced.

RESULT

Going forward, the project team hopes to include tools that can estimate each governmental entity's risk exposure by mapping back-market and legal liability estimates to the various types of data that each government agency may collect, store, process, or transmit. These values will be used to drive the results of high-level risk assessments that ultimately suggest mitigations that can reduce impact and overall risk.

Source: DHS Technology Development and Deployment Program

One direct outcome of this work was the acceleration of the adoption of the NIST Cyber Security Framework by small government entities, which aligned with federal agency adoption goals set forth by Presidential Executive Order 13800: *Strengthening the Cyber Security of Federal Networks and Critical Infrastructure*. Another direct outcome was helping small government entities adopt basic cyber hygiene controls as part of a strategy that balances prevention with resilience. A third, indirect outcome was the improved security posture of critical infrastructure sector participants that count small government entities as part of their supply chain.

Source: DHS Photo Library