Insurance Data Security Act Update

In soon to be released regulations, the Virginia Bureau of Insurance has reiterated that all agencies – commensurate with the size and complexity of the agency – must have a written information security program that outlines the administrative, technical and physical safeguards for the protection of nonpublic information. The regulations will provide some guidance – beyond the Code - for the conduct of a periodic risk assessments within the agency.

The Insurance Data Security Act (IDSA) was enacted on July 1, 2020 and is loosely based on the NAIC Model Law. The regulations from the Bureau of Insurance, once finalized, will seek to clarify as to how the law will be implemented. Here are just some of the highlights:

- Significant guidance is provided on what should be covered in an Information Security Program,
- Agencies should regularly conduct risk assessments that identifies "reasonably foreseeable internal or external threats',
- Agencies should train employees on cybersecurity awareness,
- What to do if a data breach is suspected and when to contact the Commissioner,
- Create an "incident response plan" that's part of the overall security program, and much more.

Having a cyber insurance policy or good "general security" practices is not the same as compliance. Many agencies today are protecting much of their data well by virtue of working with reputable third parties that take cybersecurity seriously.

But many agencies lack the "softer" aspects of a strong Information Security Program – risk assessments, employee training, procedures and so on. Securibly exists specifically to fill that void, simply and cost-effectively, for small and mid-sized independent insurance agencies. As an endorsed partner, IIAV members receive 15% off with discount code **IIAV2021**, as well.

Look for future IIAV seminars on the IDSA and proposed regulations as a part of the IIAV professional development program.