Input to the Commission on Enhancing National Cybersecurity

The US government operates some of the largest networks in the world, as measured by users and endpoints. And various government branches and agencies have been the subject of some of the most disastrous data breaches, including hacks of email servers at the White House, State Department and Pentagon. Following the loss of millions of records from the OPM, the Chairman of the House Government Oversight Committee called the breach a “defining moment” in its recent report into the breach.

I would indeed say the OPM breach was a defining moment – NIST, DHS and GAO should use it to look internally. The responsibility for improving cyber security falls squarely on the shoulders of our government. It’s not acceptable for government agencies to be ‘behind the times’ (so to speak). As the stewards of society and improving citizens’ lives, the government has a responsibility and obligation to identify, define, implement and enforce the ‘best of breed’ data management and cyber security practices.

The task of recovering from over a decade of lax practices, often reflecting a naive and now dated approach that government data is public data and not highly targeted, is overwhelming. NIST and the administration can help by setting internal standards for security that at least match that of advanced private sector companies in banking and the defense industrial base. Even those organizations struggle to stay ahead of the threat actors, but their gaps in defense have been constantly addressed, whereas government agencies struggle with lax attitudes towards security, low budgets, and most importantly a lack of define responsibility.

NIST should expand on the Cybersecurity Framework to define concrete levels of cyber preparedness. Just one component of that is a comprehensive data lifecycle management regime that recognizes the importance of discovering, ranking by data type and protecting the core of value: data. Data on US citizens, government employees, intellectual property and communications should be rigorously protected.

To make this happen, I have outlined my recommendations below.

1. Immediately institutionalize a data discovery exercise. Find data stores such as OPM’s records of security-clearance issued personnel. Every agency should know its own data.
2. Explicitly catalog the protections of those data stores. Where do they reside? Who controls access? Who has access? What physical and logical protections are in place?
3. Enforce government-wide data retention policies that are already written, but rarely monitored and enforced effectively. The state, for instance, has explicit requirements for the retention of the Secretary’s documents and email. Yet, it’s apparently been very simple for several Secretaries to work around those requirements.
4. Ensure that data retention polices also call for end-of-life data erasure. By data erasure, I mean using a certified and verifiable method – and tool – to permanently erase data so that it can *never* be recovered. NIST and the GAO should ensure that effective, secure, and verifiable erasure methods be used across all of government.
5. Establish additional classes of data – including temporary files, machine logs, browsing history, free disk space, and deleted files (deleting a file does nothing to the underlying data). These are all dangerous chinks in a data security policy. To avoid inadvertent data loss/theft, these data should also be securely and permanently erased – and proof of that removal must be provided as part of an audit trail that can be submitted to government agencies, investigatory/police authorities and regulatory bodies.

6. Establish the ability to effectively audit data retention policies, data use and data erasure methods.
7. Assign responsibility for data security to a Data Protection Officer (DPO). This is a role that many countries around the world are requiring for every organization that collects and processes data – most notably, the soon to be enforced EU General Data Protection Regulation.
8. Empower the DPO to report outside the chain of command to a central data protection oversight organization, possibly GAO.

While many layers of a cyber security defense architecture need review and enhancements, it is of vital importance to think about data management from a holistic perspective across data's entire lifecycle and to create protections that account for that. If this isn't done right and first, it will be difficult to prevent future data breaches.

With many thanks,

Richard Stiennon
Chief Strategy Officer
Blancco Technology Group