ZASIO

Hillary Clinton Email Incident: Five Lessons Learned for Information Governance

Soo Y Kang, IGP, CIPP/US
General Counsel / Director, Consulting Division
Zasio Enterprises, Inc.

March 2015

ZASIO

Have you adopted an information governance program? Do you need to?

As a concept and boiled down to its essence, information governance is the implementation of controls to manage information at the enterprise level to support its regulatory, legal, risk, environmental, and operational requirements. It creates synergy of information within the organization as a whole, rather than supporting the continuing existence of departmental silos that operate independently and in fulfillment of their own objectives. If there is doubt regarding the relevance or need for an information governance program, the recent Hillary Clinton email incident and headlines are instructive.

As first reported by The New York Times, Mrs. Clinton used a private email account to conduct official business during her tenure as Secretary of State. On the heels of that report, The Associated Press further reported that the private email account was traced back to a private email server installed in Mrs. Clinton's home, registered under a pseudonym, on her own internet domain. The full ramifications from this event are yet to be determined; however, from a business perspective it stresses the significance of a good information governance program. Below are five lessons to be learned from this incident to protect your business and avoid being the next example in the headlines.

Lesson 1: Be Proactive with Policies and Procedures

Laws overseeing the preservation of government records have long been in existence. Yet, these laws have been outgrown by technology and the use of such technology in the work environment (i.e., employees' use of private email to conduct business). This long overdue insufficiency was addressed in 2014 when President Obama signed the Presidential and Federal Records Act Amendments ("Amendment"), which now requires federal employees using private emails to either courtesy copy the official messaging account or forward a complete copy to the official messaging account of the user within twenty (20) days. Unfortunately, this postdated Mrs. Clinton's tenure as Secretary of State and, accordingly, failed to prevent this incident that otherwise might have been avoided with a more timely implementation.

In the corporate environment, policies set the overarching framework with procedures to fill in the mechanics. Where these policies and procedures focus on technical matters (such as the performance or execution of work), they should be carefully crafted to align with your workforce and how it conducts business. This serves two critical purposes: (1) policies and procedures that do not reflect the actual practice of the employees will fail to address the attendant risks; and (2) if it is not catered to the employees' practice, it will not be followed. Accepting that the use of private emails is an ubiquitous practice, the Amendment properly provides a workaround to achieve the overall objective – preservation. Where the Amendment failed is in the timing of its implementation, which paved the path for the attendant risk to come to fruition.

Lesson 2: Know Your Legal Obligations

Mrs. Clinton may not have been prohibited from using her private email to conduct official business, but her actions may still run afoul of other laws depending on whether she properly retained her official communications and whether those communications contained/transmitted confidential or sensitive information. With this in mind, it is important to understand all of your legal obligations pertaining to the various records and information kept, before deciding on a plan of action.

In the context of information governance, it is no longer a simple question ofhow long you should keep the information. Instead, the type of information, location, who you are as a regulated party, industry guidelines, contractual obligations, and so forth all play into the obligations you have with respect to the information you maintain. These obligations will inform decisions on policies and procedures, security measures, and other actions that must be undertaken to ensure compliance.

Lesson 3: Inventory Your Information

Part and parcel with identifying the obligations that impact your business information is understanding what business information you collect and maintain. The proliferation of technology creates unique challenges to accomplishing this, as information is now being generated at rates previously unimagined. Regardless, getting a handle on your information is necessary to reap the value that can be gained through its use (i.e., data analytics, predictive analysis, etc.), and also to inform your compliance efforts. Various options are available for this purpose, but companies commonly employ the following tools:

Records Inventory
A records inventory identifies records created, received, and maintained within an organization that is of an official character. The main purpose behind a records inventory is to support the creation of a records retention schedule, which categorizes the records identified under a classification scheme and assigns a proper lifecycle. While the scope of the records inventory will differ based on the needs of the particular organization, it generally contains information related to ownership, location, description, the medium in which the record is preserved, whether the record is "vital" to the organization, if it contains "personal information," and the operational needs for retaining.

Data Map
A data map is a tool that explains relationships between applications and systems with the objective of identifying where electronic information is stored within the organization. This is primarily driven by e-discovery; however, with new data privacy laws and consumer protection, data maps are also important in identifying where personal information resides. Due to the large number of repositories where electronic data may rest (e.g., email systems, shared drives, etc.), as well as the complexities introduced with different locations and use of third party vendors, the creation of a data map is a challenging but a worthwhile effort.

The above two identified tools are the most common methods used to capture and gain insight on the records and information retained in the organization. Regardless of what tools are used, however, taking inventory of your information is essential, as it offers invaluable insight and provides the ability for the organization to identify exposures, support compliance and discovery efforts, and provide necessary information for the organization to make management decisions.

Lesson 4: Assess Your Security Measures

Mrs. Clinton's use of her own private email and server raised questions regarding the adequacy of security measures in place to adequately safeguard her official communications. This is certainly a valid concern as we have recently been inundated with what appears to be never-ending reports of data breaches targeting information of governments, banks, retailers, and many more. These threats from external parties are only going to continue with attacks getting more sophisticated and complex. The fact of the matter is that increased connectivity brings increased risks. It is not a question of "if" you will be a subject of an external threat, but "when." Are you taking adequate measures to mitigate these risks?

The type of information being processed, transmitted, and stored, in conjunction with the degree of interaction with the network, employees, and third parties will dictate the appropriate level of security and privacy measures required. Begin by identifying your confidential information, intellectual property, personally identifiable information, and other sensitive materials. Then identify the type of tools that can be employed to protect the information and meet your legal obligations. These tools range from using modern internet security solutions, adding layers of encryption, and adopting artificial intelligence methods (e.g., machine learning, pattern recognition, fuzzy logic, data mining, artificial immune systems, intelligent agents, and so forth). In addition, with each new application or system that is incorporated into the corporate environment, assure that it has the necessary security/privacy features to suit your needs.

Lastly, incorporate effective security behavior and grow the culture of information security as part of the business process. This requires you to not only grow awareness of problems, but offer solutions to your workforce.

Lesson 5: Conduct Regular Review and Audits

Mrs. Clinton's actions occurred during her entire tenure as Secretary of State, which raises questions regarding the State Department's procedures for review and audits. These procedures are critical to assure, pertinent to an information governance program, that the workforce:

- Demonstrates awareness of company objectives and goals related to information governance
- Is properly trained in information governance policies, practices, responsibilities, and solutions
- Is securing and protecting its information
- Is disposing of information and records correctly
- Has up to date policies and procedures (that timely considers new practices and technologies)

This will also provide an audit trail to assure the reliability of information and prove that the practice to achieve compliance and quality are appropriately in place. Lastly, audits and review should occur on a regular basis and apply to the organization as a whole.

Conclusion

Played out in the headlines, Mrs. Clinton's email incident focuses on the propriety of a public officer using private email to conduct official communications. The issues highlighted by this situation, however, extend beyond proper communication and preservation processes, but go to critical aspects of a sound information governance program.

Understanding your employees' work habits, your business information and its management, as well as security measures employed to protect that information, are all considerations that every organization, whether public or private, must carefully weigh. The world and how we work have irreversibly been altered by technology, and the siloed approach is no longer capable of effectively managing information in the current business, legal, and technological landscape. Accordingly, solutions for the management of information cannot be shifted to the employee or department, but requires collaboration throughout the organization as a whole. This is information governance – breaking down silos and managing the information from an enterprise standpoint to maximize value while mitigating risks.

Take heed and learn from the mistakes brought to light by this incident. Review and assess your information governance program or, if you have yet to implement, consider implementing.

Soo Y Kang, IGP, CIPP/US
Soo Kang is General Counsel and Director of Consulting for Zasio Enterprises, Inc. In his capacity as General Counsel, Mr. Kang is responsible for overseeing all aspects of the company's legal affairs. His principal areas of focus are: negotiation of licensing agreements, consulting agreements, NDAs, and other commercial contracts; counseling on employment matters; advising on intellectual property issues; and providing strategic guidance to the company's senior executive team.

ZEICS-A-081415-1 Rev. 1 August 2015

ZASIO