INFORMATION SECURITY
EXECUTIVE BRIEF

State of Wyoming

Governor Dave Freudenthal

Office of the Chief Information Officer
2001 Capitol Avenue, Room 214
Cheyenne, WY 82002
cio@wyo.gov
http://wyoming.gov

and

MS-ISAC
Multi-State Information Sharing and Analysis Center

www.msisac.org

Information Security - Executive Summary

Government has a responsibility to serve the needs of its citizens and this is achieved through the efficient and secure collection and utilization of information. This information is often confidential and sensitive in nature. As we continue to rely on the Internet and technology to store, process and transmit this information, it is essential that we understand the associated information security risks and know how to protect the data and information systems.

As a government leader, you have the responsibility to protect your constituents by ensuring the security of their information. There are three core principles of information security that every leader should be aware of: Confidentiality, Integrity, and Availability. Information must remain confidential where appropriate (*Confidentiality*), data must retain its integrity and not be altered maliciously or accidentally (*Integrity*), and the information needed to provide services must be available to those who need it, when they need it (*Availability*).

Some examples of how your computer system would be affected by an information security incident could include your website being disabled and unavailable to your citizens; hackers breaking into your system and stealing personal and sensitive information about your employees or citizens; or disgruntled employees manipulating or destroying important government data. These and other information security incidents would certainly have a negative impact on your ability to provide services to citizens, and potentially result in a loss of public confidence.

The following Executive Brief was developed to increase awareness of the importance of information security to elected and senior government officials. By taking a proactive approach to information security, you are making an important commitment to protecting citizens and their information.

Why Is Information Security Important?

Many of our critical government services rely on the Internet and technology to function. Everything from renewing a driver's license online to submitting a tax return can be done quickly and conveniently online. This convenience does come with risks, however. The average unprotected computer connected to the Internet can be compromised in less than a minute. Thousands of infected web pages are being discovered every day. Data breaches are occurring all too often. New cyber attack methods are launched continually. These are just a few examples of the threats facing us, and they highlight the importance of information security as a proactive approach to protecting data and systems.

These rapidly accelerating and increasingly sophisticated cyber threats and the potential devastating consequences they pose to our interconnected state and local governments make it clear that **we must act now**.

It's important to note that information security is not a technology issue, but rather a management issue requiring leadership, expertise, accountability, due diligence and risk management. Information security needs to be addressed in a coordinated, enterprise approach, and factored into program decisions.

There are three core principles of information security – Confidentiality, Integrity, and Availability.

Confidentiality

Confidentiality is considered the condition when designated information collected for approved purposes is not disseminated beyond a community of authorized recipients. It is a fundamental responsibility of government officials to ensure that the necessary safeguards are in place to protect information entrusted to them. The public expects nothing less. Only authorized personnel should have access to confidential information under the stewardship of government entities. Rights and privileges assigned to personnel who administer applications and systems must be tightly controlled and limited to the minimum levels necessary to perform their jobs. Protecting the confidentiality of information is not limited to controlling access to systems, but also applies to having appropriate safeguards in place while information is stored and being transported, either electronically over a network or physically transported via tapes and mobile devices such as laptops and hand-held devices.

Some examples where confidentiality is important include medical records, confidential emails, and records containing social security numbers or credit card information and personal income tax returns.

Integrity

Integrity of information is vital to instilling trust in people who use or rely on the information. Decisions impacting the health, safety and welfare of the public are made based on the assumption that the information used is accurate and reliable. Access to information must be managed so that it cannot be accidentally or maliciously altered. Controls need to be in place regarding the creation, modification and updating of information.

Imagine a situation where a government website erroneously identifies certain professionals as licensed to work in a profession or conversely as having their license revoked when they hold a valid license. This incorrect information undermines the public confidence in the licensing system in addition to potentially causing harm to the public and the profession.

Availability

Availability means an information system or service is available and functioning correctly and providing information when needed by authorized users. All aspects of the service delivery should be protected in order for the service to function properly. Appropriate backup and disaster recovery strategies should be developed for every critical system or service.

Some examples where the loss of availability would impact government services include checking driving records during a traffic stop, processing finger prints of suspects, processing credit card transactions and loss of communications during a crisis or incident.

What Does All This Mean?

Each government official is responsible and accountable for overseeing the Confidentiality, Integrity and Availability of information with which the official is entrusted. The public expects that information provided to the government will be handled with due care and diligence in accordance with all appropriate laws, rules and regulations.

Any kind of unauthorized access or system compromise can lead to a breach of information. Compromised information can jeopardize the health, safety and welfare of the public.

Information security should be integrated at the beginning of any project or process and should never be considered an ad-hoc addition. It is far more prudent to address security at the beginning of an initiative rather than adding it in at the end, or injecting it after an event has occurred. In the end, it is an effort that is worth doing and worth doing well.

What Can You Do?

While one hundred percent security does not exist, there are steps that can be taken to manage the risks and apply due diligence in protecting information and systems.

First and foremost, embrace information security as a priority. Be a champion for the cause.

Second, designate someone to be in charge of information security, as your information security point-of-contact. This individual should be someone with a senior authority level, who has a "voice at the table" regarding information security aspects of the organization's programs, policies and any new initiatives.

Third, develop appropriate policies and procedures to safeguard the information. Be aware of the State's policies regarding security, which can be found at http://cio.state.wy.us.

Fourth, empower your information security point-of-contact to oversee the implementation of and compliance with the information security policies.

Fifth, train all staff. Ensure that all staff is trained periodically on your policies and best practices for protecting information. Ensure that technical staff has the appropriate training to implement and manage sound information security practices.

Remember, information security is everyone's responsibility!

This Brief is intended to provide a high-level, general overview of information security. If you would like information about more specific steps to enhance your organization's information security, we recommend the *Getting Started Guide*, which provides a non-technical overview of best practices. The guide is located online at http://www.msisac.org/awareness/