NSF Office of Polar Programs, Arctic Sciences Program

Information Security 101

May 2012

Volume 1, Issue 1

Special points of interest:

- **Benefits of Security**
- **Confidentiality, Integrity & Availability**
- **Contingency planning and disaster recovery can impact all of operations**
- **Federal Information Security Management Act (FISMA) is required for all Federal agencies, including the OPP, Arctic Sciences Program**

Inside this issue:

Everything You Do …

Is connected to Information Technology (IT). It's easy to open the newspaper any day and find problems resulting from breaches of confidentiality, lapses, hacking, data mining, etc. …but have you thought about the aspects of security that you couldn't do without?

- ◊ Website security certificates have enabled online purchasing and online banking and online tax filing
- ◊ Improvements in anti-virus technology have un-cluttered our email inboxes so we can once again use email to conduct business
- ◊ Digital Rights Management technology has opened up music to personal technology, such as iPods

As technology becomes a more integral part of our day-to-day activities, the assurance that these services provide confidentiality, integrity, and availability become more and more critical. All that is considered critical infrastructure or key resources have elements that relate to cyber:

- ◊ Many people use internet phone services to dial 9-1-1
- ◊ Ability to pay federal and state taxes online
- ◊ The U.S. owns many Master DNS Servers
- ◊ Power grid has controllers online

Prague 100 Year Flood

As a result of the 100 year flood that transpired in Prague in 2002, buildings had water crest nearly two stories high. Fortunately before the flood occurred, results of a risk analysis had a bank choose to locate their mainframe on the third floor instead of the basement, which enabled them to quickly return to normal operations after the flood.

Contingency planning and disaster recovering are core components of a successful Information Security Program.

Prague in 2002

What is FISMA?

WWW.WHITEHOUSE.GOV

The E-Government Act, Public Law 107-347, passed by the 107th Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States.

Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), FISMA requires all federal agencies to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FISMA includes duties and responsibilities for the National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Division (CSD).

Some FISMA requirements include:

⇒ Plan for security

⇒ Assign security roles and responsibilities

⇒ Periodically review security controls

⇒ Security awareness training

⇒ Follow NIST guidelines

What about NIST?

NIST is a flexible framework that can be tailored to fit the needs of each agency. Agencies are required to follow NIST guidelines for implementing FISMA. NIST Special Publications detail appropriate security controls that should be in place to meet FISMA requirements.

NIST outlines three types of security controls; management, operational, and technical.

NIST is the foundation for establishing an Information Security Program.

"Information Security empowers well-informed risk management decisions to justify expenditures that are part of an IT budget."

Why the Arctic Sciences Program?

The NSF requires FISMA compliance to address Federal regulations, but more importantly to protect the confidentiality, integrity, and availability of information supporting and generated by all programs within the NSF. The *NSF Information Security Handbook* provides general guidance for supported programs to develop an Information Security program that benefits their organization.

The Arctic Information Security program is being designed to fit the Arctic Program to manage IT risk to better secure information and systems, and empower well-informed risk management decisions to justify expenditures that are part of an IT budget.

How do we address these requirements?

1. Define an IT strategy
2. Establish Information Security policies and procedures
3. Capture current state IT and security posture of the Program
4. Identify and plan for remediation of risks to the Arctic mission
5. Position the Arctic Program for success when audited by the NSF Chief Information Officer (CIO) and the Federal Office of Inspector General (OIG)

Use Behavior—Smart Phones

- 50+% don't lock devices (Passwords/PINs)
- 44% of those who don't lock devices: Passwords are "too cumbersome."
- Of those without passwords: ~90% use personal devices, 65% access work e-mail or company network.
- 10% of iPhone users use 0000 or 1234 as their password.
- Of those without passwords: 97% - e-mail, 50% - online banking, 77% - social networking, 35% - online shopping

What is at Risk?

The Arctic Program relies on many services that could be disrupted by a security incident:

- *Medical*-Ensuring medical services can be provided when needed
- *Science*-Protecting science data gathering, transfer & storage
- *Cargo*-Ensuring operational and science cargo arrives on time
- *Weather forecasting*-Availability and quality of forecasting is critical to transport and on the ground operations
- *Communications*-voice and internet communications
- *Search and Rescue*-9-1-1 and disaster response
- *Energy*-to power facilities
- *Long term data retention*-in support of the Arctic mission

Critical Services

Finance:
NSF funding requires government oversight of IT expenditures and information protection

Health:
Electronic Health Records

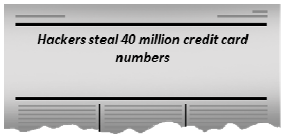
Energy:
Power and communications to Arctic sites

Public Availability:
Data sharing is mission and science critical

Air Transportation:
Flight communications and forecasting

Science Data:
Grantee Data
GIS

Threats



How Does IT Security Affect Me?

If you are wondering how IT Security is important to your support of the Arctic Program, consider the following:

⇒ Which mission essential functions that if stopped would have a significant impact on the confidence, reputation and financial status of the Arctic Program?

⇒ What information do you rely upon that cannot be interrupted for more than several hours?

⇒ What are the risks and threats to identified critical assets and supporting infrastructures?

⇒ At your facilities, what utilities would interrupt your operations and delivery if interrupted for more than a couple of hours? (computers, communications, electric power, natural gas, water, etc.)

Remember that a successful Information Security program addresses all of the aspects of an organization, not just the technology. Critical components include policy, operations, people, technology, and management.

"Which mission essential functions that if stopped would have a significant impact on the confidence, reputation and financial status of the Arctic Program?"

Arctic Program Privacy and Medical Data

In the course of your daily work for the Arctic Program you may encounter a wide variety of sensitive information (SI) about individuals, such as Personally Identifiable Information (PII) that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, mother's maiden name, or biometric records; and medical or financial information, or unfunded or proprietary parts of proposals. As an Arctic employee you are responsible for recognizing and safeguarding PII in the possession of the government, and preventing inappropriate access, use, or disclosure.

Recommendations for securely managing PII include:

- Ensure the information is only used for legally authorized purposes
- Appropriately dispose of information when it is no longer necessary to retain it.
- Encrypt to prevent loss, theft, misuse, or unauthorized access, for details see *Encrypting Information* on page 4.
- Upon collection or creation, check accuracy, relevance, timeliness, and completeness of data

Important: Immediately notify your supervisor if you ever suspect that PII has been intentionally or unintentionally inappropriately disclosed, as the NSF may be required to report the event to the US Government.

Arctic Sciences Program Information Security Support is provided by SPAWAR Office of Polar Programs

Jack Buchanan Program Manager, SPAWAR Office of Polar Programs (SOPP)
843.218.5583
jack.buchanan@navy.mil

Sarah Wolfe OPP Program Manager
843.529.4847
wolfe_sarah@bah.com

Heather Fiebing Arctic Information Security Lead
303.221.0396
fiebing_heather@bah.com

Dallas Jordan Arctic Information Security Lead Engineer
843.529.3524
jordan_jason@bah.com

SPAWAR
Systems Center ATLANTIC

Identity Theft

Identity theft is the fastest growing crime in our nation today. Over ten million Americans were victims of identity theft in 2008. Over $50 billion dollars has been lost to identity theft in the past five years. Fraud accounts for 25% of all credit-card losses each year. Seven million people become victims each year.

Reduce the risk of being a victim of identity theft by taking the following precautions:

⇒ Buy a shredder
⇒ Get your credit report
⇒ Protect Your Social Security Number (SSN)
⇒ Make sure Your SSN isn't on your driver's license and checks
⇒ Keep your mother's maiden name between you and her

If you are victimized:

⇒ Notify three big credit bureaus
⇒ Close or suspend compromised accounts
⇒ File police report
⇒ Complain to the Federal Trade Commission (FTC)

Encrypting Information

Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. If you email, transport, or store sensitive information on your computer or external hard drive, you may consider encrypting the data to reduce the risk of your information being accessed without your consent.

Many word processing, file management, and email applications now provide methods for encrypting a computer, hard drive, files, documents, and even email content. Common applications that provide encryption features include, Microsoft Office and PGP.

Remember: For the recipient of an encrypted file to open the document they must have the encryption key you used to encrypt the file. For the recipient to open an encrypted email you must share your digital signature configured in Outlook. For more information refer to the Microsoft Office website: http://office.microsoft.com

Important: All medical and personally identifiable information (PII) managed by the NSF must be encrypted using FIPS 140-2 *Security Requirements for Cryptographic Modules.*

Common Threats & Vulnerabilities

Major information security threats include:

⇒ Disruption of computer systems and electronic communication
⇒ Theft, loss, or accidental distribution of sensitive, personal, scientific, or confidential information
⇒ Lost productivity with the slowing of advancement of science
⇒ Identity theft

The types of most frequently attacked software in 2007 were:

⇒ Web applications - Includes RealNetwork's RealPlayer, Apple QuickTime, Sun Java
⇒ Business applications – Microsoft Office Suite: Word, PowerPoint; OpenOffice Suite; Adobe products: Acrobat; Symantec anti-virus software suites
⇒ Web pages - i.e., web defacements, system compromises, data theft

Most common IT security attack methods:

⇒ Social engineering (tricks you to open or close documents enabling system infection)
⇒ Malicious code (e.g., Worms, Viruses, Trojan Horses, Bot, Key Logger, Rootkit, Spam)
⇒ Physical theft of computing device (for resale of equipment and/or data)

Did you know?

- In 2010, 40% of all Facebook status updates have links. 10% of those links are spam or malicious.
- 3 in 10 people likely to click an unsafe link.
- 71% of teenagers have established online profiles on social networking sites. 47% have public profiles viewable by anyone.
- 26% of Americans say they are sharing more information on social networks