# CYBER SECURITY Newsletter

## DATA PROTECTION

### Problem

A great deal of our security focuses on keeping our devices secure, such as firewalls, anti-virus, and system updates. While these are important, ultimately, most attackers are not after our organization's computers or devices, but the information residing on them. We have a tremendous amount of sensitive information that must be protected at all times.

### Solution

Technology can only do one part in protecting our data. We depend on you to protect our organizations sensitive information. To ensure our data always remains secure, you are required to take the following steps whenever handling any sensitive information:

1. Always understand the sensitivity of the data you are working with. Any sensitive data stored on authorized portable devices, such as laptops, should be encrypted. Sensitive data may not be stored or processed on any unauthorized devices.

2. Never attach sensitive files when emailing people outside of our organization. In addition, you should never forward sensitive information to personal email accounts such as Gmail or Yahoo.

3. Never store or share sensitive information on public Internet or Cloud services such as Dropbox, Apple iCloud, or Google Docs unless you have prior authorization from management.

**Data Protection**

*Our information is our greatest asset; it is also the primary target for many cyber attackers. It is critical you follow the steps provided to help protect our sensitive information.*

Idaho State UNIVERSITY

This newsletter is published by Idaho State University, for more information please contact us at:

help@isu.edu

# Advanced Threats After Our Data

*There are many different threats targeting our sensitive data. One of the most common is cyber criminals. These are individuals or organizations who know they can steal our sensitive data and use it to commit fraud or simply sell it to other cyber criminals. Unfortunately, there are several other threats targeting our sensitive data – threats even more advanced than common cyber criminals.*

*One is our competitors. Some of our competitors may be very unethical in the ways they operate. They may try to compromise our organization to gain a competitive advantage, and to do so they need our data.*

*Another threat is other countries. There are certain countries that target our data for economic, political, or military gain. Individuals launching these attacks are often supported by their government, and it is many times part of their full-time job. You may not think our data has value to other countries, but it does.*

4. Be careful responding to any emails or phone calls in which someone is asking you to send them sensitive information. Always authenticate the person first using our approved procedures.

5. Always be careful when using USB drives or other mobile media. Only use authorized mobile devices the organization has approved. Never use devices such as USB drives you may have found, received as part of a promotion, or received from strangers. In addition, whenever you connect mobile devices to your computer, make sure you scan all contents on it with current anti-virus before opening any files.

6. Any sensitive information should be backed up on a regular basis using our approved procedures. If the device is lost, stolen or the data is corrupted you will be able to recover that data via the backup device. You should also always encrypt all backup devices as they are also often targeted by criminals.

7. Sensitive information should be securely wiped, erased, or destroyed when it is no longer needed.

8. Do not install or use unauthorized software.

9. Never leave any sensitive documents unattended at your desk. Always secure sensitive documents when you leave them, such as locking them in a cabinet.

10. Always password-protect your computer. This will help to ensure unauthorized personnel will not be able to access your computer or your confidential information while you are away.