By completing this module, you will be able to:

* Describe what risk is

* Describe the elements used to calculate risk

* Describe five common potential threats and vulnerability combinations that present risk to DOI  information systems.
* Explain how and why individual awareness is often the only way to lessen the risk

Risk is the impact of a threat acting on a vulnerable asset. Risks are assessed by:

* Identifying threats to a situation, and
* identifying weaknesses (vulnerabilities) of safeguards protecting particular assets that threats can exploit.

Then, estimating:

* the frequency or likelihood that the threat event could occur in a given time period (e.g., annually), and
* the financial impact the threat event would have on an asset.

The quantifiable risk can be calculated as an Annualized Loss Expectancy (ALO), which would be the frequency or likelihood of the threat event occurring in a year multiplied by the financial impact to the organization of that threat event.  
  
Information security risks are those risks that arise from the loss of confidentiality of data, integrity (correctness and accuracy), and availability of data and computer systems.  Assessing risk requires the careful, consistent, and methodical analysis of threat and vulnerability information. The analysis should be our best estimate of the extent to which circumstances or events could adversely impact our organization and the likelihood and frequency such circumstances or events may occur.    
  
The National Institute of Standards and Technology (NIST) has publications addressing this topic, including the Special Publication (SP) 800-39: Managing Information Security Risk.

Threats – Unintentional and Intentional

Information is an asset, and must be protected from human and non-human, intentional and unintentional threats.  In-house developed programs, other software, decision documents, and engineering diagrams are intellectual assets. Devices, people, buildings, and the information contained in them are also assets.  
  
This training is focused on making you aware of threats to assets you use since preventing data compromise can often be done only through your awareness.

**A. Unintentional Threats**  
  
Every day, someone, somewhere in DOI will unknowingly or unintentionally make an error with data. Examples of unintentional threats include losing a thumb drive, a laptop or other mobile device, or accidentally deleting or overwriting data.

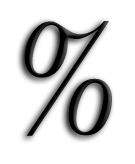
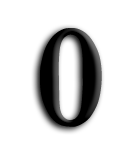
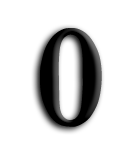
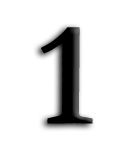
Since humans will always make errors, the risk from unintentional threats is 100% but the impact of lost data may be low due to the following factors.

* The information is not sensitive,
* it can be retrieved or regenerated with minimal effort,
* it was encrypted so there is no loss of privacy, or
* it can be retransmitted.

The vulnerability is human fallibility, the likelihood is certain, the frequency is daily, and the impact of data lost could be minimal to extreme. Two common ways to minimize the impact of lost data is to encrypt data so it isn’t revealed if lost or stolen, and to make backups of data so the information is retrievable.

Although it is a certainty that someone somewhere will unintentionally compromise data, we do not stop using computers just because there is a 100% risk of data loss.  We try to methodically and consistently evaluate the threat, determine the cost to the information services we need to provide to support our missions, and then apply cost-effective measures to control the impact of threats exploiting vulnerabilities.  It’s not worth spending more money to protect an asset than it’s worth.

This training is a security control that helps people realize that they can prevent loss of data. Other controls that mitigate (lessen) the risk are automatic temporary copies, snapshot images of databases and servers, and automatic nightly backups of data servers. Though loss of data from this threat is certain, the impact on the business that DOI performs is minimized due to the money spent annually on awareness training, and automated controls such as encryption, backup hardware, software and media. Automation reduces the personnel cost of recovering from an incident to a reasonable amount.



**Risk of**

**Data Loss**

**Mitigating Controls for Unintentional Threats**

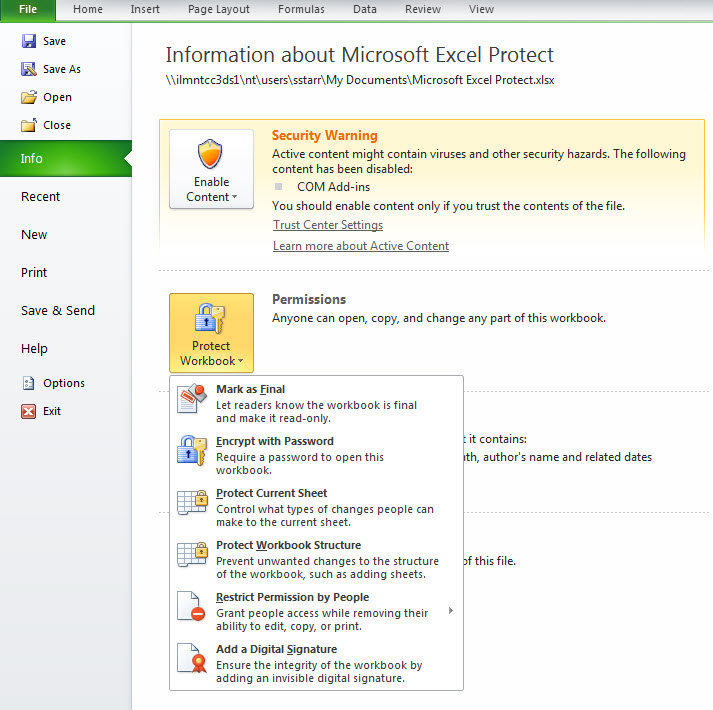
**1.  Backup**

* Make your own backups of your data, but label and properly safeguard the backups. A good rule of thumb is to have three backups of data critical to you.  This concept also applies to critical data stored in the “cloud”, since the cloud provider can go out of business, change access policies, or experience a lengthy internet outage.
* Your IT staff usually has network backups of mission critical data for catastrophic loss, but restoring lost data is time consuming, bureaucratic, and expensive. Know whom to contact for restores, what the restore time is for your backup, and how often your data is backed up.
* Label backups on mobile media and devices to reflect the sensitivity level of the information they contain, the date they were made, and the owner of the data.
* Prevent inadvertent erasures by keeping portable media such as CDs, DVDs, thumb drives and external drives away from temperature extremes (like in a hot car), and magnetic sources (such as radios).
* If the media technology for your backups will soon be outdated, make sure to transfer any valuable data to modern media.
* Keep a copy of your backups offline and physically separated from the backed up computer.
* **Mitigating Controls for Unintentional Threats** (continued)
* **2. Encryption**
* Bureaus and offices are required to ensure that all mobile media and devices containing sensitive agency data are encrypted.   
    
  There are a few exceptions to this requirement. Encryption is not required if the media or devices will never be taken outside of the agency’s secured physical perimeter. Encryption is only necessary if, for example, the devices or media will be taken to a personal residence, carried while on either business or personal travel, or transported from one controlled facility to another.  
    
  Also, an exception may be made if the Deputy Secretary (or the Deputy Secretary’s designee) determines, and states in writing, that the information contained on those media or devices is non-sensitive.  
    
  BisonConnect emails and their attachments are automatically encrypted, in transit.  However, sensitive information should be protected once it reaches the end user, and where the sensitive information is stored by the sender.

The buttons below will provide access to instructions for using McAfee Endpoint Encryption: How-to instructions and a McAfee File and Removable Media Protection User Guide.  Section 3 on page 21 of the user guide contains instructions on encrypting files and folders.

* <https://doiu.doi.gov/FISSA2016/assets/DA6BD4F9-ACBE-3A9B-6F46-A43919014F2B.pdf>
* <https://doiu.doi.gov/FISSA2016/assets/DA6BD4F9-ACBE-3A9B-6F46-A43919014F2B.pdf>

WinZip software is also an option used to store one or more files in a format that uses a compression algorithm to reduce the amount of space required to store the files.  WinZip 9.0 and higher includes an encryption feature to protect sensitive information.  A password is used during the encryption process and the same password must be used to extract files from the archive.  The WinZip program should be available by contacting your local IT Helpdesk.

You can easily password-protect Microsoft Excel spreadsheets to protect sensitive data.  While the spreadsheet is open, click on File, then Info, then Protect Workbook, then choose Encrypt with Password. Be sure to remember your password as you won't be able to recover it.  Also remember not to send the password in the email with the file.  It’s better to provide the password separately, such as with a phone call. This way, if the email communication is intercepted, the unauthorized person doesn't have the password to access the data.

Contact your bureau or office IT Helpdesk or BCISO to request these or other encryption tools used by your organization.

Threats from Peripheral Hardware

Digital information can be stored or transmitted on devices other than your desktop computer. When requested, please assist personnel with the important responsibility for maintaining accurate inventories of assets such as equipment, information, and media.  
  
Copy machines, fax machines, cell phones, laptops, thumb drives, external storage drives, CDs/DVDs, tapes, and tablets can store as much data as a computer.  Printers contain hard drives that store and transmit information without encryption. Documents can be sent to printers across the country into environments that may not be secured. No information stored or transmitted in any medium can be considered completely safe from unintended access.  Always use caution in handling information that can be considered sensitive in the present or in the future.

Because the Department has office locations in some of the most remote regions of our country, the use of modems and dial-up services may be the only option available.  Modems are also commonly used with Supervisory Control and Data Acquisition (SCADA) systems which are used to control processes in dams, oil rigs, nuclear reactors, and environmental systems such as heating and air conditioning.

If the use of a modem is unavoidable:

* Check that DOI network cables to the computer are disconnected or unplugged while the modem is in use;
* Ensure the modem is configured to never receive calls or only accept calls from specified numbers; and
* Don’t give other people the dial-in phone numbers to modems. If someone needs dial-in phone numbers to modems, they should go through authorized channels.

Insider Threats (Intentional)

Current workers (insiders) are the most common cause of deliberate information security incidents. Stress, such as financial problems, can alter a person’s normal behavior and cause that person to act irrationally or turn from a “trusted” user into an unhappy worker, having inside knowledge of data systems and the means and intent to exploit weaknesses.  
  
An example of insider threat in DOI was a procurement clerk who embezzled hundreds of thousands of dollars by directing electronic payments to her personal bank account.  She was caught when she took a week of sick leave and the person who filled in found discrepancies. The control to prevent future exploits of this type is “separation of duties” so the person authorizing payments is not also responsible for making them.  
  
The threat is theft or damage to systems, the vulnerabilities are complacency and the absence of management controls, the likelihood is possible, and the impact can be minimal to extreme but includes a damaged reputation.

Examples of insider threats include the following:

* A disgruntled employee sabotages information systems.
* A financially troubled individual provides procurement information to a “favored” bidder.
* An employee who feels “entitled” runs a wireless access point, personal website/business on federal systems, or uses unlicensed software.

Treating everyone in the organization with respect, and willingness to cooperate in work goals will reduce some sources of stress that can create insider threats. Report suspicious behavior to your management.  According to the Secret Service, other workers noticed something was amiss in 85% of insider incidents.  
  
Special attention should be given to those separating from DOI. All computer and building access must be removed immediately after an individual leaves the organization. Entrance and exit procedures are key controls, along with regular audits for “excessive access rights” for insiders and those who have moved to other jobs.

All DOI employees, contractors, and others (e.g., volunteers) are required to follow an "Exit Check-Out" on their last day that includes these steps:

* Obtain an Exit Check-Out package from your supervisor or HR if you are an employee or from the Contracting Officer's Representative (COR) if you are a contractor.
* Complete all forms and obtain all signatures on all forms in the Exit Check-Out package.  This should include your IT Support Office.
* Turn in all government property, including but not limited to charge cards, ID cards, access cards, keys, smartphones, and computer equipment and software.
* All federal records must be turned over to the supervisor and the supervisor should be made owner of files stored on Google Drive, and any Google Sites or Google Calendars.



Supervisors and CORs are responsible for ensuring that the Exit Check-Out procedures are completed and make sure access to all applications and the network is disabled.

Intentional External Threats

The breach of the Office of Personnel Management (OPM) data in April 2015 was one of the most serious breaches in the US government (22 million records), second in size only to the Veterans Administration breach (26 million records) in 2006.  Many received letters from OPM notifying that their personal information may have been compromised in the OPM breach.  The compromise was a foreign entity that accessed the OPM network and moved from server to server with stolen administrative passwords because OPM did not use Personal Identity Verification (PIV) cards for authentication.  
  
For this reason, DOI has enforced use of PIV cards for authenticating to government networks during the summer of 2015 for both administrator (privileged accounts) and for regular user accounts. The target is 100% use of PIV cards for all network users.  Over the next few years, as application software is upgraded, more and more programs will accept PIV cards to verify the right to access those systems.

Criminal elements target databases and other places where they can get large numbers of email addresses, names and either credit card numbers or Social Security numbers (SSN) to sell or to use for identity theft. Email addresses are used to send spam or phishing attacks. Criminal elements can work with disgruntled or dishonest insiders to gain access to networks and steal information from the inside.

One of the most common deceptions in enticing users to download malware (malicious software) is fake antivirus popup screen offers that can appear on legitimate websites that have been compromised.  
  
Not only do the thieves get your payment information for that transaction, they install malware that can steal other personal and financial information.  A related threat is Ransomware in which the malware will hide or encrypt your files and a payment will be required for recovery.  These activities are so profitable that attackers will create fake call centers to make people think that these scams are legitimate.  
  
Organizations shouldn’t request your personal information via e-mail.  If in doubt, give them a call (but don’t use the phone number contained in the e-mail since that’s usually phony as well).

Additionally, many of the latest web browsers have phishing filters built in or offer them as plug-ins. Any emails requesting you to “enable” Macros before opening an attachment is a red flag. One reason Macros are disabled is so computer code can’t run unless the user allows it.  Use a combination of good judgment and appropriate technical controls to safeguard your personal information.    
  
Click [here](https://doiu.doi.gov/FISSA2016/index.html#167869_1) to view an actual phishing email sent to some DOI employees.

<https://doiu.doi.gov/FISSA2016/assets/7A90943B-D1E4-A805-4D99-013A4577FA28.pdf>

**Phishing Clues**

Phishing**:** a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly.

Due to a multitude of recent events and other factors, chances are you will receive one or more phishing messages in your lifetime. In fact, DOI employees have already received Help Desk warnings of specific Phishing/SPAM messages targeting government employees. One of these warnings - the April 8, 2014 message-contains clues that will help you spot future phishing messages and can help you avoid being hooked.

*How many phishing clues can you spot?*

*On April 8, 2014 the message read*: “We have received notification of an active Phishing / SPAM campaign targeting users in BSEE, BOEM, and ONRR. The format of the messages may vary, but they are generally arriving to users’ Gmail inboxes as “Friend Requests” from valid BSEE, BOEM, or ONRR employees ….”

Here’s the phishing email sent with the April 8th message. How many clues do you count? (The answer and explanations are on the back page)

How can you spot a phishing message?

1) Approach each email message knowing you ARE definitely a phishing target. Recent cyber attacks make this a known issue for you, a government employee. But even before recent attacks, you were a high phishing risk if your work email was posted on public sites such as doi.gov, conference presentors/attendees, social media sites, or working group public member lists. “Public” means everyone in the world.

a. To minimize your risk, ask that your official email address be provided to only those who need to know and preferably behind access controls-- not be posted on public websites and documentation available to everyone in the world.

2) Before you open emails: Stop- Look-Think about the sender’s name, subject, date/time, and sender and reciever email address. Are there:

a. Unsolicited requests for protected information; such as User IDs, passwords, bank account or credit card information, or detailed personal or organizational information.

b. Unrecognizable or unknown sender addresses formatted differently or with slightly altered domains. Examples include .com when you expect .gov, like irs.com vs irs.gov or additional characters in the email addresses.

c. Is the subject irrelevant, full of hype/emergent/urgent, or totally unexpected?

3) Look at the message format. Are there:

a. Discrepancies, such as email banners or footers with physical addresses that don’t make sense or a date sent outside normal timeframes for the buisness or individual (such as after business hours or after midnight).

b. An overabundance of clicking opportunities, including many buttons or clickable links.

c. Spelling or grammatical errors

4) Do not automately open emails without reviewing them: Look for anything odd or out of context about an email subject line, sender name or email, or subject line format. Hover your mouse over sender name to see their email address.

5) Do not click on links without looking deeper:

a. Hover your mouse over the link and look at what is displayed-You should see the entire link address. Is it consistent with the message and sender? Is it what you expected?

b. Right click and copy the link and paste it in a new browser window so you see the full link/URL address. Is it what you expected and consistent?

c. Type in a link to the website yourself. If you need to look up the website first, search for the published company website, then type the URL in yourself, and do a search for on that site for the item you are looking for.

6) Evaluate attachments: Is the attachment something you’d expect, is it in the format you expect (ie .doc vs .zip/exe). If not, don’t open it. Do not “Enable Macros” within attachments, as malware can be extracted through the Macros.

7) If in Doubt-Ask: If in any doubt about the email, links or attachments, call or email the sender at a known or publically published or previously known number/contact information. Call the Help Desk if you need help or questions.

3. Your full or partial email address in Subject

1. The From addressee is NOT “@bsee.gov” address –it’s “@infoaxe.net “

2. Somewhat urgent sounding Subject

9. Hover your mouse over the links. Does the displayed web address, (aka URL) make sense with the context? We don’t have live links for this email, but I’m betting that the site address (aka URL) that is shown when you hover over it is not a “.gov” URL . Hover 100% of the time before you click links.

4. Sent at a fairly late time (7:09 pm) for ‘bsee.gov’ offices

8. Look for good US English Grammar and content-That’s an oddly worded sentence, isn’t it?

6. Tempting sounding offers and even an emoticon. Content is odd for a work related agency contact.

7. Odd ‘bsee.gov’ physical address (PO Box in California)

5. An overabundance of click options (buttons and Links) and big, bold shading

**Phishing Clues**

Answers- Did you find all 9 clues pointing to the fact that this email isn’t legitimate?

Threats from Email

Spam:  
  
Spam is unsolicited e-mail sent to many e-mail addresses, possibly even millions of them.  Spammers use programs called “bot-nets” (robot networks) to deluge e-mail providers with spam.  If an extremely large number of these are sent, even very small percentages of responses may be very profitable.  
  
The threat from spam is that it may contain malware, links to compromised websites, and report back on valid email accounts for future campaigns. Even if spam does not contain viruses or other malware, it can clog inboxes and slow down systems.

If you receive e-mail offering to sell or give you something, and you were not expecting to receive the message, never respond to it.  Once you do, the spammer will continue to send you even more messages, possibly for additional products or services.  Delete spam messages immediately - without reading them, if possible. BisonConnect has a special “Report spam” button that you can click to identify unsolicited email as spam. Over time and with enough reports on those emails, Google will filter spam from inboxes automatically.

Chain letters are a form of spam that can transmit malware, take up space on hard drives, take up bandwidth, waste time and annoy those who get them. Do not spam others by forwarding chain letters.  
   
Similarly, insider spam comes from unnecessary emails when somebody inappropriately uses “Reply All.”  If you are going back-and-forth with emails more than three times, try another communication medium such as the telephone.

Scams:  
  
A common email scam involves using a compromised email account (that had a weak password) to plea for money from friends or family claiming an accident or robbery while on vacation. Sending private posts and photos during vacation to family and friends is alright, but posting publicly risks someone using that information for malicious activities.  
  
The state of Washington has good examples of suspicious emails about email scams. Click [here](https://doiu.doi.gov/FISSA2016/index.html#167882_2) to view them.  
  
If you are a victim, report it to the Federal Trade Commission (FTC).  Click [here](https://doiu.doi.gov/FISSA2016/index.html#167882_1) to access the FTC web site or visit the Internet Crime Complaint Center (IC3) by clicking [here](https://doiu.doi.gov/FISSA2016/index.html#167882_3).

If you must click on a link sent to you in an e-mail, whether from someone you know or not, check it out first.  Hover the mouse pointer over the link to see the “real” link behind the one in the e-mail. Try this example. Click the following link: [http://www.cnn.com/](https://doiu.doi.gov/FISSA2016/index.html#167883_1).  This link took you to Google though the address made you believe you'd be opening cnn.com. The real website was hidden. If the link and the real website don’t match, the sender may be trying to take you to a malicious site. URL-shortening services like [TinyURL](https://doiu.doi.gov/FISSA2016/index.html#167883_2) and [Bit.ly](https://doiu.doi.gov/FISSA2016/index.html#167883_3) used in [Instant Messaging (IM)](https://doiu.doi.gov/FISSA2016/index.html#167883_4) and [Twitter](https://doiu.doi.gov/FISSA2016/index.html#167883_5) are especially vulnerable to this threat.  
  
Malicious URLs are usually shortened so their true destination is obscured. Use a site such as LongURL ([http://longurl.org/](https://doiu.doi.gov/FISSA2016/index.html#167883_6)) to see where the shortened link really goes.

One of the most secure steps you can take is to disable HTML in e-mail and accept text only. This will save you from inadvertently clicking on a link in an e-mail since it won’t work if HTML is disabled. Then, just type in the URL yourself. This is especially important for computers that you also make financial transactions on.

One current scam is that someone calls and claims to be a Microsoft Certified Engineer.  The scammer claims that Microsoft has detected that your computer is in a botnet (i.e., "spreading malware on the internet").  The purported engineer wants you to go to a URL to “fix” your computer.  Don’t be a victim of this scam.

**Spearphishing Threats**  
  
Spearphishing emails have targeted DOI managers and executives in the past. Spearphishing emails are common methods to trick specific people with influence into downloading malware.  Many spearphishing emails appear to be from expected senders but the email address was really to the malicious party.

Targeted spearphishing attacks come in low volume to specific individuals, (often to a specific title (e.g. CFO or Accounting, or CEO) or about subjects dealing with upcoming events or expected meetings divined through social profiling), whereas broad phishing attacks will use video, news, or celebrity lures to drive people to specific malicious websites.    
  
During disaster situations and emergencies, people tend to be more distracted and can more easily fall victim to scams and spearfishing attacks. There is often an increase in scams asking for money to support relief efforts during disaster situations and emergencies. Before donating to things such as a “relief effort”, check out the source of the request and consider donating only through well-known and reputable organizations.

Spearphishing attacks involve scams masquerading as a legitimate message from someone you know, subpoenas, FTC complaints, billing issues, or tax issues. People post much more personal information now than previously on social networking sites like Facebook, LinkedIn, Twitter, Pinterest and others.

This allows spammers and phishers to scrape or extract pertinent data from unsecured or unprotected profiles and use that data to create more personalized spam and phishing attacks, looking like they are from a friend or a peer on the social network site.

Social networks themselves have also become sources of spearphishing for the same reason, and when using a social network either in a spoof or actual source for an attack, the spammer has the added bonus of potential positive reputation to bypass security filtering.

The mobile variant of phishing is “Smishing" (SMS Phishing).  Links are sent like in an email but via a text message.  Users can send the scam message via text 7726 (SPAM) to cell phone carriers to have the sending number blocked.  Many smartphones also have a block list.

Wherever the source, be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information.   Do not provide personal information or information about your organization, including computers, structure or networks, unless you are certain of a person's authority to have the information.

There is no limit to attackers’ creativity.  Maintain healthy skepticism and report suspicious activity of any kind to your Help desk, DOI CIRC (703-648-5655/email [DOICRC@ios.doi.gov](https://doiu.doi.gov/FISSA2016/index.html#167920_1)), or your supervisor.

 Physical Threats

Of course information can also be stolen by physical means:

* Dumpster diving – going through trash cans;
* Stealing a laptop, mobile device, or thumb drive;
* Taking sensitive printouts from unattended printers or fax machines;
* Rummaging through someone else’s unsecured work area; and
* “Shoulder-surfing” to get passwords or simply accessing an unattended workstation.
* Weak building security controls are vulnerabilities that allow unauthorized individuals, including former employees, to gain access to a building or secured areas.  
     
  Visitor control is a security precaution everyone can help with by making sure all visitors are escorted, by being alert, and making it a habit to glance at badges. Be non-confrontational, friendly, and offer to help people you don’t recognize. Call the physical security people to check up on those without a badge.
* Watch for piggybacking or tailgating, which is a person without proper access credentials who tags along behind another person with proper credentials to enter a restricted building or area. This also safeguards us from physical harm as well as theft of our own belongings, and not just federal property.   
     
  If you lose your badge or facility keys or find someone else’s, contact your facility security or supervisor immediately.
* Use the Windows key + <L>  or <Ctrl> + <Alt> + <Delete> and then <ENTER> to lock the screensaver on your computer whenever you leave your work area, even if it is only for a few minutes.