

What is risk?

When we think of risk, we often see it in two different ways – sometimes we do not put these together in the same thought. Risk can be thought of as the *possibility and probability* of something of an adverse nature occurring. In its other use, risk can be a description of the *magnitude* of the adverse impact. In other words, what are the *odds that something bad will happen*, and *how bad would it be?*

When we think of risk, we need to understand, as well as possible, both of these aspects of risk.

What is Risk Management?

Reduce risk whenever possible.

Risk can rarely, if ever, be fully eliminated, but risk can often be reduced. Risk that cannot be eliminated, or that is too expensive to eliminate, is



often referred to as “residual risk,” or as “acceptable risk.” Why “accept” risk? Sometimes the cost of reducing or eliminating risk is greater than the potential loss. Sometimes accepted risk is mitigated by compensating controls. For example, we accept the risk of driving a car, but we mandate the compensating control of safety belts.

Managing Risk Online by...

- 1) Not opening attachments that are uncertain in any way.
- 2) Not clicking on links that are uncertain in any way. View the full link, and copy and paste it to the address field, rather than click on a link that can take you to a site with a malicious “drive-by” payload that installs on your PC without your knowledge and consent.
- 3) Not replying to outrageous offers for unearned gains, such as a percentage for transferring money into your bank account from a foreign company – your inheritance from a distant, unknown relative. If an offer seems “too good to be true,” you have 99% odds that it is a SCAM, and you are the intended victim.
- 4) Safeguarding your password from EVERYONE, even trusted friends and family. Additionally, make the password a STRONG password that has no association with family names, pet names, or anything else that someone can find out about you. Make up a phrase, such as “I sleep with my cat Trixi and my socks on,” and use a password with the first letters and some simple symbol substitution: I\$wmcT&m\$o.
- 5) Not inserting thumb drives/flash drives or CDs/DVDs with unknown content, or from unknown sources, into any device or computer.
- 6) Noticing changes in your computer’s behavior. If it acts erratically, super-slow, or otherwise changes, have it checked out for malware that could be stealing your personal information.

Be safe.

Contact us

Jim Richards, CISO
Information Security and Controls
West Virginia Office of Technology
1900 Kanawha Boulevard East,
Building 5, 10th Floor
State Capitol Complex
Charleston, West Virginia 25305
esecurity@wv.gov
www.technology.wv.gov/security



**SEE A RISK?
REPORT A RISK!**



WV - ISAC

DIVISION OF THE OFFICE OF TECHNOLOGY | OFFICE OF INFORMATION SECURITY AND CONTROLS

Where can risk be addressed?

Risk exists at work, in the form of confidential data that we collect, store, and transmit. Any activity surrounding the handling of legally protected data, such as Personally Identifiable Information (PII), and its highly sensitive subset, Protected Health Information (PHI), is inherently risky. Risk of a breach of sensitive information at rest, and during transmission, is best addressed with encryption. Such information on paper should be secured in locked locations whenever possible, and never left exposed on a desktop. Verbal communication of PII or PHI should be done only when necessary, in a private setting.

Risk exists at work in situations where the wrong person gains access to buildings, systems, or data. We can all manage risk by carefully protecting access to buildings, by securing our systems when not in use, and keeping our physical (badges) and logical (passwords) credentials to ourselves.

Risk can be managed at home by keeping computers secured, up-to-date with operating system patches, anti-virus programs, and strong passwords. Online transactions should have the <https://> at the left side of the address bar (example: <https://secure.mygov.com/login.cfm>) whenever entering a password, or entering sensitive data such as credit card numbers, social security numbers, etc.

Risk can be managed at home by educating children to know who they are chatting with, to not reveal personal information to anyone they do not know personally, to be aware that online identities are sometimes faked by malicious people, and that information put on various sites can be aggregated to form a composite of information that is more revealing than ever intended by the user.

Condition	Potential Consequence	Risk Mitigation
Leaving workstation logged on and unattended	Identify theft. Someone does some action as if they are you	Lock workstation every time you step away for any reason
Allowing someone in building using your badge or credential	Person causes harm to persons or system inside the building	Send people without badges to guarded entrances for screening
Sharing your password	Identify theft. Someone does some action as if they are you	Never share your password
Loss or theft of laptop	Loss of legally protected data. Harm to persons or company	Hard drive encryption
Revealing too much personal information online	Malicious person can profile you with increased chance to cause harm	Minimize posting to social media on various sites – composite
Succumbing to social engineering	Loss of confidentiality of credentials. Id theft, hacking	Be wary of questions that ask for too much or too personal information.
Leaving badge or id on desk	Theft and misuse of credentials	Keep or secure credentials

Manage Risk

Accept residual risk that you can't eliminate, but remember you are at risk, and act accordingly. Get help if you need it. Don't take unnecessary risks, things are hazardous enough without being casual online. A global army of bad guys is trying to steal your information 24 hours a day, 7 days a week and 365 days each year. They know more about offense than you know about defense. You cannot afford to give them more advantage than they already have. **Manage risk.**

