

SECURITY - Now ...more than ever!

Cyber Security - Disaster Recovery - Continuity of Government

**DTI eSecurity News - Unintended Information Disclosure**

“Unintended” disclosure is the malicious or accidental disclosure of confidential or sensitive information. One kind of information at risk can be confidential data, such as financial accounts, credit cards, Social Security numbers, personal medical information, or other personally identifiable information defined by law. Depending on what kind of data is exposed, it can lead to criminal activity like extortion, or it can be used for an attack on critical infrastructure systems operated by the government, finance companies, transportation departments, utility companies, chemical companies, and telecommunication sectors.

How serious is the issue?

Unintended information disclosures occur through a variety of means. Electronically, they can result from lost backup tapes, lost thumb drives, lost laptops, exposure via website attacks, or email exchanges. Non-electronic disclosures include discovering paper files in trash bins or overhearing phone conversations.

Many breaches involving information such as confidential citizen data, proprietary source code, password, or network maps occur with alarming regularity but are not always tracked or even reported.

No agency or school district is immune.

These incidents represent significant financial costs. Costs will be incurred from incident investigation, the technical response of fixing the problems, informing affected persons, credit checks, and loss from financial theft; all of which can vary. Just as importantly, such an incident can result in the loss of public confidence.

**How can I help prevent unintended disclosure?**

- Know what kind of data you are handling.
- Classify your organization’s data, and protect it according to its value and risk.
- Follow your organization’s security policies and procedures.
- Know your data retention policies – don’t store confidential information longer than necessary.
- Use privacy statements in electronic and paper documents.
- Don’t use confidential data for testing purposes.
- Store, transport, and destroy confidential data responsibly.
- Keep portable data storage devices like laptops, CDs, blackberries, flash drives, and backup tapes in secured locations.

How can I respond to an incident ?

- First and foremost, realize that we are all responsible for information security – reporting the incident is the right thing to do.
- While policies will vary from organization to organization, the State of Delaware has a law detailed in “Title 6 of the Code, Chapter 12B, Computer Security Breaches”, that provides overall guidance for response.
- Report the incident to your supervisor, and document what you know.
- If you think your personal financial information has been compromised, contact the data holder to confirm the incident, and contact your financial institution.

Remember that cyber security is everyone’s responsibility and that you can make a difference!

October is Cyber Security Awareness Month

Questions or comments?
E-mail us at eSecurity@state.de.us