NIGC Tech Alert

Security Incidents: Information You Need to Know

Data Breaches - Headline News?

The news headlines report data breaches, data loss, or cyber security incidents so frequently that we have become numb to the information and often just glance at headlines that report facts like:

- IRS data leak exposes personal info of 120,000 taxpayers
- Samsung discloses data breach after July hack
- The Uber Hack's Devastation Is Just Starting to Reveal Itself

The fact is most of us ignore these headlines, when we really need to be paying attention and working daily to practice good cyber security habits, personally and professionally.

Here's some information you need to know to be vigilant and combat cyber threats by being on the lookout for cyber security incidents:

What is a security incident?

A security incident is the unauthorized disclosure of sensitive information through attacks such as phishing schemes, ransomware, or malware. A security incident may also result in the loss of confidential data through theft, insider threat, or loss of a laptop /mobile device.

Examples of a security incident.

- Loss of a mobile device or laptop.
- A stolen employee's cell phone in a coffee shop, on the subway, or from their vehicle.
- An employee clicks on a malicious link, resulting in their agency being compromised by a ransomware attack.

Who is touched by an incident?

Everyone is impacted by a security incident. Whether, the root cause was an accident, poor security practices, insider threat, or phishing scheme, a security incident can affect both small and large organizations. A common myth is that only large companies are vulnerable to these types of incidents, or that a small organization is just too small for someone to take the time to launch a cyber-event. The fact of the matter is, any organization regardless of size can be impacted by a security incident.

Negative impacts from an incident

When a security incident takes place, it affects the entire agency, primarily through damage to its reputation. Often, these security incidents draw attention through local or national media, and leads to a loss of confidence in an agency's ability to safeguard its data. Restoring confidence can take years, even decades to accomplish.

What are some strategies to help avoid these incidents?

- Employ a strategy of least privilege to all accounts.
- Avoid clicking on hyperlinks from unknown sources.
- Beware of emails that asks you to act immediately.
- Do not give out information over the phone unless you know the other party.
- Use strong passwords with multi-factor authentication.
- Regularly patch your systems and update your antivirus software and firewall detection signatures.