Cyber-Attack FAQs

How was the incident discovered?
On June 28, 2022, a WSI employee received a sophisticated phishing email and opened an attachment containing malicious code, accessing personal injured employee data. The incident was immediately reported to the WSI Help Desk, then to North Dakota Information Technology. A forensic analysis was conducted by the NDIT Cyber Analysis and Response team.

What information was involved?
Primarily e-mails and voice mails that included personal information of 182injured employees. These emails contained information received and sent by a claims adjustor to process injured employee claims including e-mails to and from WSI employees and business partners.

How many individuals were affected?
The personal information of 182 injured employees was accessed which was contained in the WSI's employee's email.

Does this mean someone stole my personal information?
Currently, we know that the attackers had access to personal information in the emails. We cannot verify what information was actually taken because of the attacker's use of anti-forensic techniques. It is unknown how the attackers will use the information.

What can I do to protect myself?
WSI is offering identity theft protection services through IDX, a data breach and recovery services expert to those affected. IDX identity protection services include: 12 months of identity theft protection services, a $1,000,000 insurance reimbursement policy for identity theft losses, and fully managed identity theft recovery services. With this protection, IDX will help resolve issues if an identity is compromised.

Who was responsible for the security of my information?
Workforce Safety & Insurance and the North Dakota Information Technology are responsible for the security of the information. They take their responsibility very seriously and have multiple levels of security in place to protect your information. Just like in a home or business, even the best security systems are not a guarantee that criminals will be stopped. WSI is working closely with all appropriate authorities.

Is the accessed information still at risk of disclosure to an unauthorized person?
No, the cyber-attack was isolated to a single computer, and it did not spread onto the network. After the incident was reported to the WSI Help Desk, the computer was secured and is no longer accessible on the state network. The Cyber Analysis and Response team conducted additional evaluation to better understand the attack and to ensure protection from future threats of this nature.

How is WSI responding?
NDIT and WSI developed a strategy to identify the source of the malware and how to address it. WSI has analyzed the data accessed and will use all practical means to notify those affected by the incident. WSI is positioned to provide those affected with information and to answer questions.

Who should I contact if I have questions concerning this security exposure?
Please contact WSI Customer Service at 800-777-5033

Created August 16, 2022