EMPLOYEE DATA

Is your organization protected?

- *How are you protecting your employee data?*
- *How are you combating cyber threats with internal policies and procedures?*
- *How are you safeguarding your business from cyber attacks?*

Imagine finding out the reality that your employee's sensitive data has been compromised in a massive cyber attack.

The recent MOVEit File Transfer breach is another example of a data breach impacting numerous organizations and thousands of individuals due to their government's use of the system. Read about it here: https://www.hrreporter.com/focus-areas/hr-technology/nova-scotia-provides-details-on-huge-data-breach/376663

Cl0p - The group responsible for this attack is best known as a notorious hacker group that gained prominence in recent years for their involvement in high-profile ransomware attacks. They employ multiple tactics like exploiting vulnerabilities, phishing, and weak credentials. Notably, they use a "double extortion" technique by encrypting files and threatening to publish sensitive data unless a ransom is paid. Their targets range from small businesses to multinational corporations, drawing attention from law enforcement and cybersecurity firms. Here are some notable Cl0p cases:

Accellion: In December 2020, Cl0p this file-sharing software company. The attackers exploited vulnerabilities in Accellion's legacy File Transfer Appliance (FTA) software, leading to data breaches at multiple organizations, including universities, government entities, and financial institutions.

University of Miami: In February 2021, Cl0p attacked this renowned educational institution. The ransomware incident resulted in the theft of sensitive data, including student and employee information. The university was forced to shut down some of its systems temporarily to contain the attack.

ExecuPharm: In April 2021, Cl0p targeted this pharmaceutical outsourcing company. The attack resulted in the theft of sensitive data, including employee information, contracts, and other proprietary data. Cl0p threatened to release the stolen information if the ransom demand was not met.

Toshiba Tec: In May 2021, Cl0p attacked this Japanese technology company. The ransomware incident disrupted the company's operations and led to the theft of confidential corporate information. Cl0p published some of the stolen data on their leak site when the ransom was not paid.

Health Service Executive (HSE): In May 2021, Cl0p targeted this Ireland healthcare system. The ransomware attack caused significant disruptions, leading to the shutdown of IT systems and cancellation of appointments. Cl0p threatened to release patient data if the ransom was not paid, but the Irish government refused to negotiate.

It is more important than ever, in times like this, to partner with the right organization that understands the cyber threat landscape and how to combat this ever-evolving threat.
Contact an Iridium Risk Advisor today to learn more about prioritizing cybersecurity and protecting your organization.

IRIDIUM RISK SERVICES EVOLVED
NAVACORD®

Irsnavacord.com
info@irsnavacord.com

1100, 255 5th Avenue SW
Calgary, AB T2P 3G6
403.263.9654