FRONTIER SUPPLY CHAIN SOLUTIONS INC.

CYBER SECURITY ATTACKS TODAY:

KEEP FRONTIER SAFE.

1

Who Performs Cyber-Attacks?

Large criminal enterprises, staffed by intelligent people utilizing an array of techniques to gain access and spread havoc. These organizations mine social media, public databases, LinkedIn, and data harvested from other security breaches to learn about who works at what company and their function.

How do They Strike?

After they convince someone to click on a link, they'll install a malicious software. They get what they wanted, a backdoor into a a company. Then they wait. The criminals will monitor traffic, collect data within the company network but stay hidden if possible. At a point in time, usually, Friday or Sunday evening when everyone is away from the office, they launch their attack.

2

3

What do They Want?

The purpose is usually to deploy ransomware which uses exploits to get into computers and servers to encrypt data and hold it hostage. Then comes the ransom note, usually asking for Bitcoin and the amount is predetermined based on what they know about the company. The ransom also increases each hour, and they usually inform you the decryption key to recover your data will be deleted at the end of the multi-day countdown.

What's the Cost?

It's very effective and when it happens to a company it can be crippling to the point where some have gone out of business because they can’t afford to pay the ransom. The most interesting part about all this is how automated the entire operation is. Everything from the emails in your inbox, the initial malware to the ransomware deployment is all automated.

4

5

How to Avoid Cyber-Attacks:

Our hosted exchange email platform comes with some really good reporting tools to show the amount of SPAM, Phishing, and Malware emails we get daily. It's quite a bit. While Frontier IT can employ firewalls and security software that’s only one aspect of protecting the company. The best deterrent is our staff themselves. .

FRONTIER