

ARTICLES

How Cyber Threats Could Impact Your Courier Business

Dec 28, 2018

if you're a courier (or really any business) owner, this is an important question to ask, and even more important that you find the answer...

How and where will the next wave of cyber attacks take place? And, how can I protect myself and my business against cyber warfare?

Cyber security is a real issue for small and large businesses alike. If you're unsure of cyber security protocols and best practices, or how to protect your company and client data from attacks, it should be a top priority. Below we outline some basic cyber attack facts and key vulnerabilities your company should actively seek to safeguard.



Some Troubling Facts About Cyber Attacks

Businesses and organizations should expect cyber criminals to attack through wearable devices, employee's home systems, cloud services and automobiles within the next year, per cyber experts at **Intel's McAfee Labs**.

By 2020, individuals could receive payment for sharing their personal data and hackers could be manipulating markets in their favor through financial intelligence gathering, the experts also predict.

In fact, the future of cyber crime is now and managing potential cyber-attacks should be near the top of your risk management portfolio. The Insurance Journal put together a comprehensive look at the top cyber threats in the next five years, called the McAfee Report.

The McAfee Report

Intel Security has released its McAfee Labs which offers predictions on the cyber threat landscape and insights into what that landscape might look like through 2020. The report, which reflects the opinions of 33 of Intel Security's thought leaders, also addresses likely responses to these threats.

"The best hockey players navigate within the ice rink, grapple with opposing players taking advantage of opportunities when available, and, critically", as Wayne Gretzky said. "Always skate to where the puck is going to be - not where it has been," said Vincent Weafer, vice president of Intel Security's McAfee Labs.

Cyber Threat Red Flags and Vulnerabilities

The following is a list of common terms your company should be familiar with as they relate to cyber security.

Hardware: Analysts predict attacks on hardware and firmware will continue to expand, and the market for tools that make them possible will increase as well. Virtual machines could be targeted with system firmware root kits.

Ransomware: The world of cyber crime and its' focus on ransomware will only grow. A greater numbers of inexperienced cyber criminals will leverage (ransomware-as-a-service) offerings which could further accelerate the crime. Anonymizing networks and payment methods will continue to fuel the growing threat of ransomware.

Wearables: Wearable devices typically do not store large amounts of personal information, but wearable platforms could be targeted by cyber criminals working to compromise smart phones used to manage them. The industry will work to protect potential attack surfaces such as operating system kernels, networking and Wi-Fi software, user interfaces, memory, local files and storage systems, virtual machines, web apps, and access control and security software.

Attacks through Employee Systems: Back-door cyber infiltration will continue to be the method of choice by would-be hackers. Companies are always improving virtual security, implementing the latest anti-hacker technologies, and creating new policies. Thus, attackers shift their focus onto employees, by targeting, among other things, employees' relatively insecure home systems to gain access to corporate networks.

Cloud Services: Cyber criminals could seek to exploit weak or ignored corporate security policies established to protect cloud services. Home to an increasing amount of business confidential information, such services, if exploited, could compromise organizational business strategy, company portfolio strategies, next-generation innovations, financials, acquisition and divestiture plans, employee data and other data.

***Risk Strategies** works with nearly 2000 delivery and logistics companies of all shapes and sizes nationwide, specializing in the full range of insurance and risk management solutions for this industry: property & casualty, alternative risk solutions, employee benefits, IC risk programs, key person risk management, safety and accident prevention, executive and family risk, and financial services.*

Contact us today to learn more about using our expertise to take you further and protect your journey. To learn more please call (877) 862-4755.

TAGS:

Transportation