KYND

Cyber risks in the automotive industry

As the motor trade industry accelerates into the digital age, cyber risks are becoming increasingly more prevalent. Vehicles are more connected, some being fully electric and many having internet based in-built systems. Companies selling and manufacturing cars are having to factor in significant security risks.

Automotive companies carry extensive amounts of sensitive information. Many customers purchase vehicles by taking out a loan, and their financial information presents an attractive prospect to cybercriminals. As well as this, personal details such as customers' addresses, emails, and vehicle identification numbers are stored by these companies, all of which are an appealing target for cybercriminals.

An automotive company can also face substantial GDPR fines over a failure to protect the personal and financial details of its customers. These fines can be up to £18 million or 4% of an organisation's annual global turnover - whichever is greater.

Furthermore, even if personal data isn't targeted, the disruption of business and operations can be extremely costly and time-consuming for a company. With many automotive companies having global operations, the halting of production processes can deal significant financial damage.

Business exposure and implications

Ransomware

Ransomware attacks can be an exhausting ordeal for automotive companies of all sizes. If a cybercriminal holds sensitive data to ransom, or prevents systems from being accessed, a large company could suffer a massive cost in the braking of operations, and a smaller one could be driven into the ground by the hefty resultant GDPR fines.

Phishing attacks

The amount of valuable and sensitive customer data that is stored by automotive companies can prove very useful for anyone conducting targeted phishing attacks. If this data is stolen by a cybercriminal, they can use financial information, knowledge of recent purchases, and personal details such as the customer's email and home address, to create extremely convincing fraudulent communications.

Supply chain cyber risk

Third-party service providers and suppliers present a significant risk. If these suppliers don't have sufficient cybersecurity measures in place, automotive companies are also vulnerable to being compromised by a cybercriminal. As more and more transactions take place online, and employees are increasingly working remotely, these vulnerabilities become easier to exploit.

Distributed denial-of-service (DDoS) attacks

Distributed denial-of-service attacks – an attempt to crash a web server or online system by overwhelming it with traffic from multiple resources – is a growing threat to car dealers and manufacturers, given the increased remote working of employees, which exacerbates existing vulnerabilities and creates more avenues for exploitation.

Key industry statistics

3.1m

is the total number of customers whose personal information was exposed as a result of a disruptive cyber-attack suffered by Toyota Motor Corporation in February 2019.[1]

£385k

is the fine issued by The Information Commissioner's Office (ICO) to Uber for failing to protect their customers' personal information during a cyber attack in November 2016.[2]

1.4m

of vehicles were recalled by Fiat Chrysler in the US in 2015 for an urgent software update; to prevent hackers from gaining remote control of the vehicles internal systems exploiting a software vulnerability in Chrysler's Uconnect dashboard computers.[3]

£24b

is the projected annual financial impact of cyber-attacks on the automotive industry by 2023.[4]

What types of risks exist?

There is a variety of different threats that the motor trade industry could be impacted by, but the most common include:

Phishing
Malicious emails designed to look like genuine emails which encourage employees to click – infecting their computers or stealing passwords in the process.

Viruses
Code which infects computer systems, corrupting or deleting data.

Hacking
An individual or group attempting to gain access to company systems with the intent to steal or destroy data.

Ransomware
A malicious programme which locks access to company files and data until a ransom payment is made, after which time access may be restored.

Case Study

Type
A major car manufacturer experienced a ransomware attack.

Scenario
The car manufacturer had its global operations disrupted by a targeted ransomware attack, including factory operations.

Sting
A variant of a new and dangerous form of ransomware was used to halt industrial control systems, factory operations, and production processes by targeting a company's entire network.

Investigation
The attack was able to have such a disruptive impact because the network of the company was so interconnected, rather than being segmented to prevent a bad actor from traversing the network and interrupting different business functions. One department being the victim of a ransomware attack can impact the operations of other departments and have a catastrophic effect on the company.

Conclusion
By segmenting its networks, the company could have prevented such a widespread impact on their global operations. As a result, even though no customer date was exfiltrated, it is a costly and lengthy process to return services and operations to full functionality, and this can result in a loss of sales as well as halting production. Furthermore, this type of ransomware has been known to exploit remote access to internal networks, which are in wide use during the pandemic, and the car manufacturer had machines with remote access publicly exposed.

KYND

KYND's analysis of key cyber risks of the top* 100 world's largest automotive companies

*by turnover

Ransomware Risk

67% of companies had at least one external internet service exposed which would place them at a higher risk of a ransomware attack.

Certificate Issues

77% of companies had at least one security certificate which had expired, been revoked or distrusted.

Vulnerable Services

67% of companies were running at least one service, such as an email server or web server, with a well-known vulnerability to cyber attack.

Out of Date Software

87% of companies had at least one service that was using software which was out of date, no longer supported and vulnerable to cyber attack.

Domain Risk

67% of companies had at least one domain registered to a personal or individual email address.

How KYND can help

- With just a website name, KYND reveals your organisation's cyber risks
- Instantly KYND lets you know if your emails are spoofable or if you're vulnerable to a ransomware attack
- KYND provides clear and easy recommendations without using technical jargon
- KYND continuously monitors and alerts you instantly if any new cyber risks are found

Get in touch

✉ broker@kynd.io

🌐 www.kynd.io

References:
[1] https://www.cpomagazine.com/cyber-security/new-toyota-data-breach-exposes-personal-information-of-3-1-million-customers/, 2019, CPO Magazine
[2] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-fines-uber-385-000-over-data-protection-failings/, 2018, Information Commissioner's Office
[3] https://www.ft.com/content/2bafe3e0-321f-11e5-8873-775ba7c2ea3d, 2015, Financial Times
[4] https://industrytoday.com/wp-content/uploads/2018/12/Upstream-Security-Global-Automotive-Cybersecurity-Report-2019.pdf, 2019, Upstream