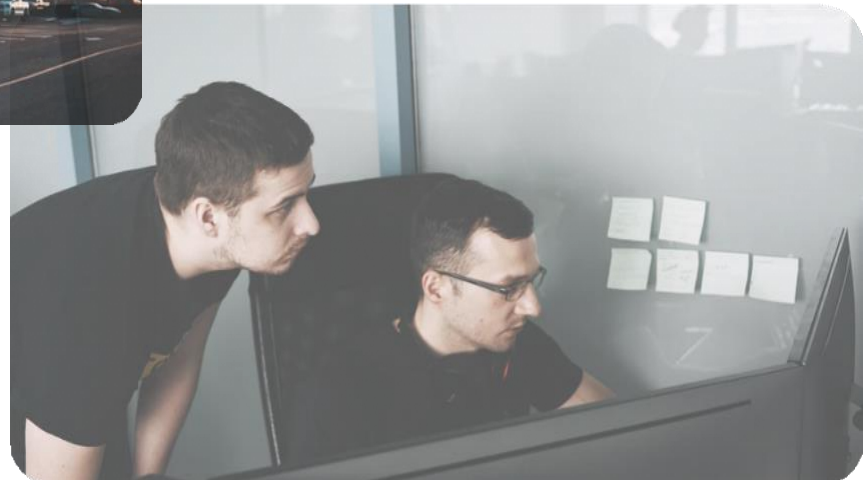


INSURING AUTOMOTIVE DEALERSHIPS.

DEALERSHIPS.

ENSURING IT SAVINGS AND SECURITY

Is it possible to find savings whilst improving the IT security within your automotive dealership? And why is Cyber insurance so essential?



This ebook will help you to see where you can drive savings with your Dealer Management System and how to lock and alarm your IT so that your Cyber Security is top spec.



hamiltonleigh
Insurance Brokers

CYBER EXPERTISE YOU CAN TRUST

hamiltonleigh
Insurance Brokers

Hamilton Leigh are very focused on ensuring that clients' key exposures are covered by insurance.

Cyber-attacks continue to rise in frequency and are having a significant impact on all types of businesses. In recent years, we have placed huge focus on discussing cyber risk with our motor dealer clients. Like so many other businesses, the cyber conversation is 'Why would a hacker attack us?'. With informative conversations, the sharing of data, claims examples (and the resultant impact), we are very pleased that most of our Motor Trade clients are now covered against a cyber attack.



RDS are particularly proud of our long-standing relationship with the retail automotive sector; it's where things began some 20+ years ago for RDS.

Through our extensive experience in dealer requirements, we understand how important it is for your IT systems to be running smoothly and efficiently PLUS be totally secure.



WHEN IT COMES TO BEING AS SAFE AS THOSE NCAP RATINGS GIVEN TO CARS WHAT DO YOU NEED TO KNOW AS A DEALERSHIP?

What follows is a cyber interview with Andrew Kays, COO of Socura, a cyber security business specialising in detection and response services.

Q: How has the cyber security space evolved in the last 3 to 5 years and have these changes heightened the risk to businesses?

A: Yes, there is now even greater focus from Organised Crime and State actors to use Cyber to achieve their aims. A whole industry has grown up in organised crime using approaches such as Ransomware to elicit money from companies. Another Industry that has evolved is the production of ready-made malware that can be purchased to run campaigns – criminals no longer need the skills themselves, they can purchase the tech. This has increased the number of potential attackers.

Q: What are some of the key change's businesses can make to their infrastructure to better protect themselves from hackers?

A: The focus for a long time has been on prevention; stopping the attacker getting in! While the technology is good in this space, there are continually new ways to exploit systems and 0 day vulnerabilities that allow criminals to gain access to systems. The focus has started to move 'detection and response' as well as prevention i.e. Security Operation Centre monitoring services. This allows us to monitor and react to suspicious behaviour, spot quickly anything that has got through the defence, and shut it down before it can have an impact on the organisation.

Q: From your perspective what are the two most potent threats (types of attacks) to businesses?

A: First is ransomware. Here the organisation's data is encrypted and therefore unusable and will only be released if a ransom is paid. This can have a massive impact on the operation of a business and its ability to service its clients. Monitoring and response are key to spot the start of an attack and close it down as quickly as possible. Secondly is probably insider threat. This is always difficult to quantify, but there is a large black market for information, and your own staff have the best access to it and know how to evade defences in place. Again, monitoring can really help here.

RISK MANAGEMENT & CYBER ESSENTIALS

At Hamilton Leigh, we continuously support our clients to enhance their risk awareness. Our specialism in the Motor Trade sector spans almost 30 years and in that time, we have successfully managed all kinds of motor and liability related claims. Through this experience, we share information with our clients through our unique and exclusive Risk Awareness Workshops, specifically designed to mitigate our clients' risk exposures.

RDS Global can offer a full cyber security audit on your business, taking a close look at processes and controls around the technical infrastructure, physical assets and documentation in your business. We can then guide your business through the necessary Cyber Essentials and ISO certifications. Our fully managed and affordable subscription-based solution will watch over your business 24/7, monitoring all network activity to your system and proactively blocking any threats ensuring IT security.

There has been a noted increase in Cyber Activity in the Automotive Sector over the last year and more recently targeted attacks on retailers which has resulted in business interruption, loss of revenue, ransom and penalty fines, loss of confidence in your customers and damage to the brand reputation.

Cyber Essentials Certification is a Government backed scheme that is designed to protect your company against a whole range of cyber-attacks and is aimed to provide the business owners peace of mind that your defences will provide protection against common cyber threats and that the basic technical requirements are in place.

The importance of the Certification has rightly risen to a prerequisite for a number of Bodyshop Approvals, Fleet Tenders and Government Tenders.

CYBER INSURANCE; LAST LINE OF DEFENCE

Many people are now up to speed on the 'Don't click a suspicious link' but it's proven to not be enough. As part of the staff induction process a modular training course to make them fully aware of the types of things to watch out for. This will empower your teams of people and allow them to feel more confident that they would know how to respond to a given scenario as well as give you more peace of mind as an employer.

RDS can support you with specific training elements to deliver to your staff from our Cyber specialists. Training is tailored to your business, your team and your requirements. It all starts with us fully understanding your dealership.

In the event of a cyber incident that has affected your customers/clients. Perhaps, their personally identifiable information was accessed by hackers and they naturally feel unhappy about it and take to various available online platforms to voice their dissatisfaction. Don't let your dealership get tripped up.

ENSURE & INSURE YOUR IT SAFETY

RDS, working in association with Hamilton Leigh, aim to ensure that you have an effective Cyber Accreditation and Cyber Insurance Policy in place for your business.

Contact Us!

If you'd like to talk about any elements included in this ebook here's how to get in touch with us:



If you are interested in learning more about Cyber Insurance feel free to contact Jason Cohen at Hamilton Leigh via email jasoncohen@hamiltonleigh.com



If you'd like to talk about a DMS evaluation or cyber security IT services feel free to contact Andy Flinn at RDS via email Andy.Flinn@RDS.Global



hamiltonleigh
Insurance Brokers