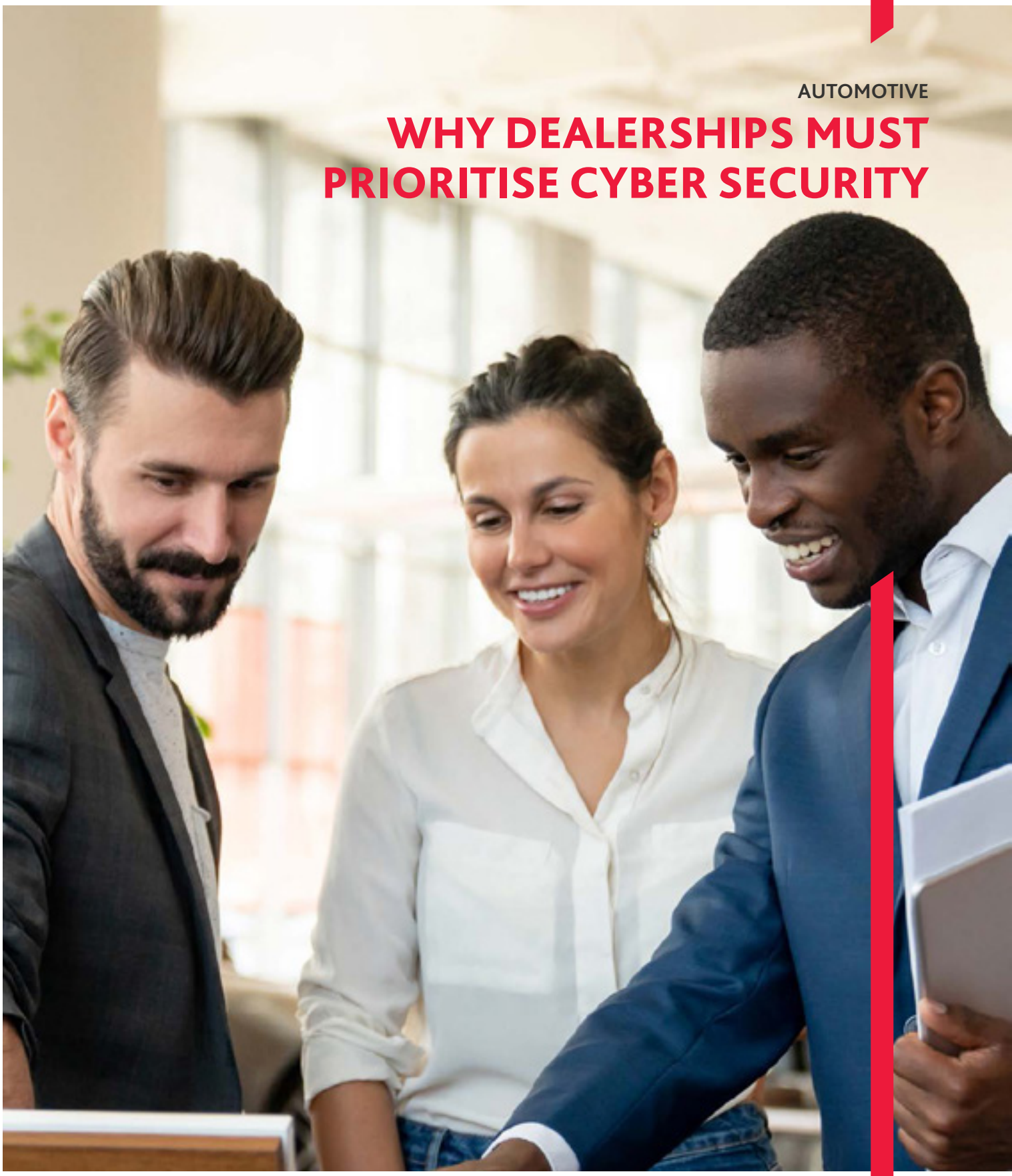
AUTOMOTIVE

WHY DEALERSHIPS MUST PRIORITISE CYBER SECURITY



While the day-to-day operations of a dealership might vary greatly from other types of businesses, they all still have one thing in common: the need for cyber security. No matter what line of work they are in, every business needs to secure their data and do everything they can to prevent accidental leakage or malicious attacks.

The threats to dealerships are pervasive. There are so many moving parts to keep track of (and we're not just talking about the vehicles here). Dealerships have relationships with financial institutions, for lending purposes, and across the supply chain. They deal with a wealth of sensitive customer data such as contact details (names, addresses, dates of birth etc.), financial information, identity documents, and credit card data. Service schedules and loan processes are typically reliant on technology, as well as revenue or lead generating marketing activities.

When talking about cyber security, the nature of business for dealerships results in exposure to a wide range of cyber threats and risks. So, how can your dealership protect against cyber threats? Here are a few tips to get started.

1 CONTINUOUS PREPARATION IS A DEALERSHIP'S BEST DEFENCE

Disruptive cyber attacks, such as ransomware, can not only halt a dealership's operations, but expose it to long lasting reputational impacts. Being unable to service customers halts critical revenue generating business activities, and a breach of customer information introduces significant reputational, legal and regulatory impacts.

The cyber landscape is constantly changing, and it is important to prioritise cyber investments accordingly. All companies, especially dealerships, need to continuously evolve to keep up. They don't want anything suspicious touching their credit card transactions, supply chain relationships, and so on. Therefore, it's important for dealerships to review cyber security measures that are in place and improve upon them as needed.

2 DEVELOP AND TEST AN INCIDENT RESPONSE PLAN

The time to prepare for an emergency isn't during an emergency. Having a plan is essential, but it cannot be relied upon unless it's been tested. There are two ways to do this – in a high-stakes, real-world cyber attack, or in a low-stakes, high-gain cyber exercise. Cyber exercises are also an effective way to communicate the non-technical impacts of cyber risk. For example, rehearsing your customer service, financial, operational, legal, media and communications responses to a cyber attack can highlight the importance of cyber security for non-IT staff.

3 ESTABLISH RESILIENCE

An incident response plan will help you contain and eradicate the immediate impacts of a cyber attack, however, a disaster recovery plan will help you sustain operations with manual workarounds, and get back in business as soon as possible. A disaster recovery plan should outline a clear process to implement contingency workarounds, sustain operations, and communicate effectively when systems are down.

While an incident response plan is similar to a disaster recovery plan, there are key differences which is why each one requires a separate document.

An incident response plan will help you contain and eradicate the technical impacts of a cyber attack.

A disaster recovery plan will help you sustain operations, reduce downtime, and get back in business as soon as possible.

4 OFFERING ONGOING EDUCATION TO ALL PROFESSIONALS

In addition to having documented plans for incidents and disasters, it's also important to offer ongoing education to all employees. A dealership's people represent its first and last lines of defence against cyber attacks.

5 CYBER INCIDENT EXERCISES FOR ALL EMPLOYEES

Beyond continuing education, employees must also be prepared for any scenario that may present itself. What is the best way to make sure they're prepared? With realistic exercises. Practice makes perfect, and the more practice your employees have, the less vulnerable you'll be to cyber threats.

6 CREATING A CULTURE OF AWARENESS AND REPORTING

Creating a culture within the dealership that not only makes employees aware of cyber security but also encourages them to report incidents will only help you. Cyber security shouldn't just be a top priority among executives; make sure it's a part of the culture within your organization.

7 UNDERSTAND YOUR RISK

To protect what's important, you have to understand which digital systems keep the business running, and how they're vulnerable to cyber attack. This requires an understanding of which cyber adversaries are targeting you, what they're targeting, and how they will target you. Establishing visibility of cyber risk starts with the tone at the top and requires an enterprise-wide approach.

8 ADEQUATE INSURANCE COVERAGE

No matter how confident you are in your security posture, your mindset should never be, "what will we do if a cyber incident occurs?" But rather, you should ask yourself, "what will we do when a cyber incident occurs?" Any business can fall victim to cyber threats, and because of that, it's smart to have insurance. This can offset any financial losses that may happen because of a cyber-attack.

Most dealerships don't have people on staff that understand the current realities of what cyber risk is today. With an ever-evolving threat landscape, it is imperative that investments in cyber security are smart and pragmatic to protect your dealership.

Our cyber specialists can lend their experience and help you safeguard your dealership against cyber threats. BDO Digital's security maturity quiz provides you with an idea of how secure you are currently. Additionally, we recommend engaging in a deeper conversation around your threat landscape as it relates to cyber to find the comprehensive solution that is right for you. Contact us today to get started.

CONTACT US

KEY AUTOMOTIVE CONTACTS:

MARK WARD
National Leader, Automotive, Partner, Business Services
+61 7 3237 5744
mark.ward@bdo.com.au

RANDALL BRYSON
Partner, Business Services
+61 7 3237 5792
randall.bryson@bdo.com.au

SAM VENN
Partner, Business Services, Automotive
+61 3 9244 2025
sam.venn@bdo.com.au

GRANT CAMERON
Partner, Business Services, Automotive
Grant.cameron@bdo.com.au

KEY CYBER SECURITY CONTACTS:

LEON FOUCHE
National Leader, Cyber Security
+61 7 3237 5688
leon.fouche@bdo.com.au

ROSS WIDDOWS
Partner, Advisory, Cyber Security
+61 2 9240 9815
Ross.widdows@bdo.com.au

FAITH PAGE
Partner, Information and Technology Risk Advisory
+61 3 9603 1750
faith.page@bdo.com.au

CHRIS KORTE
Partner, Digital & Technology Advisory
+61 8 7324 6021
chris.korte@bdo.com.au

AUDIT • TAX • ADVISORY

1300 138 991
www.bdo.com.au

NEW SOUTH WALES ● NORTHERN TERRITORY ● QUEENSLAND
SOUTH AUSTRALIA ● TASMANIA ● VICTORIA ● WESTERN AUSTRALIA