SHAPING AND PROTECTING THE FUTURE OF MOBILITY

Michigan is not only the hotbed of mobility advancements—it is driving cybersecurity forward, too

A COLLABORATIVE APPROACH TO SECURITY

The future of mobility depends on software, not just hardware. Data and technology are revolutionizing the way we move from one place to another. The mobility space is ripe with opportunity for technologists and entrepreneurs.

But the digitalization of transportation and growing interconnectedness of vehicles and infrastructure also creates new vulnerabilities—or "opportunities"—cyber criminals are all too ready to exploit. The mobility ecosystem needs strategies for preventing and responding to cyber threats.

In Michigan, public and private organizations collaborate to develop these solutions. Together, they are strengthening state-level defenses, cultivating cyber talent, and creating an optimal business environment for developing security-related technologies. These initiatives help to protect the technologies that underpin mobility's future.

But, securing vehicles and infrastructure is an ongoing, complex process. Every player in the space must understand the reality of cyber threats. Let's explore the business opportunity, automotive cybersecurity challenges and solutions, and how Michigan's collaborative approach is helping businesses protect their technology—and their passengers.

planetm MICHIGAN ECONOMIC DEVELOPMENT CORPORATION | Entrepreneur PARTNER STUDIO

A TRILLION-DOLLAR OPPORTUNITY

New business models driven by such trends as shared mobility, connectivity services, and feature upgrades could add as much as $1.5 trillion in additional revenue potential by 2030, according to McKinsey predictions. Startups and small businesses can, and do, make a significant impact on the space. But entrepreneurs must understand the realities of cyber threats and consider what it means to operate in a cyber-secure environment as they scale.

This task falls on both private and public entities, as demonstrated by Michigan's unique approach. The state combines public and private resources to improve state defenses and groom future talent, while keeping business owners' interests at heart.

THE STAKES ARE HIGH

As more products that affect daily life contain and connect to computers than ever before, cybersecurity is of growing importance across industries. From 2004 to 2017, the cybersecurity market grew roughly 35x, from $3.5 billion to $120 billion, according to estimates by Cybersecurity Ventures. Experts predict continued growth through 2021—anywhere from eight to 15 percent year-over-year, depending on who you ask.

The stakes are particularly high for Automotive, explains Karl Heimer, senior technical advisor for cybersecurity for the Michigan Economic Development Corporation (MEDC), a public-partnership focused on growing Michigan's economy by building community, connecting businesses, supporting entrepreneurs, and driving the future of mobility.. Computers control a range of vehicle features, from driver assistance technologies like automatic braking and forward collision warning, to infotainment systems. Connected vehicles share vast amounts of data with one another as well as with infrastructure. All of this puts both safety and privacy at risk.

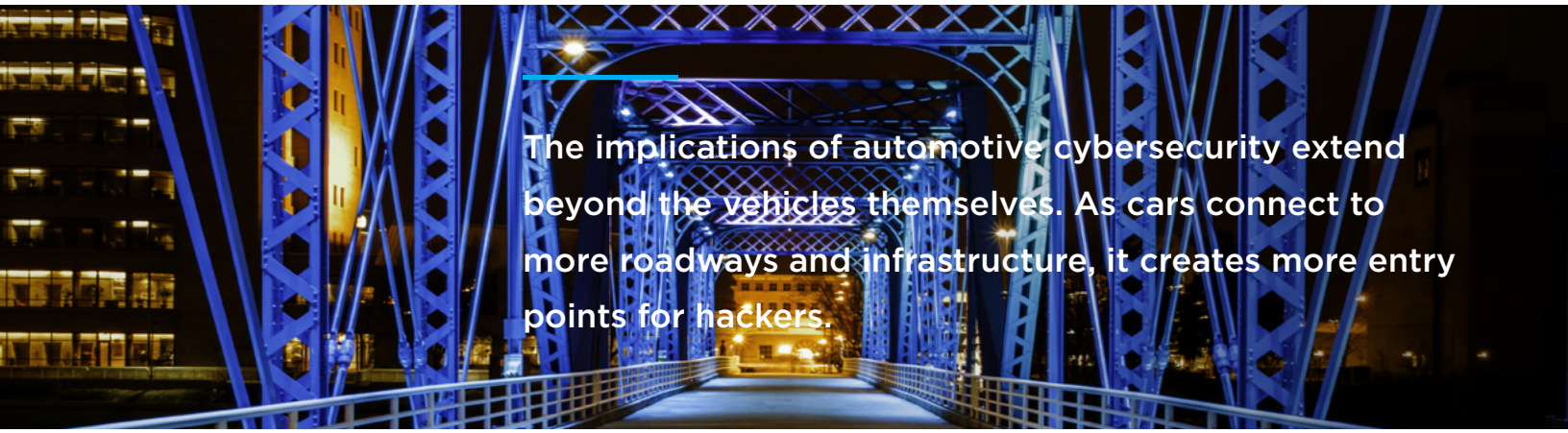
Security breaches are also bad for business. The average cost of a data breach is $3.9 million, according toresearch from IBM and the Ponemon Institute. Comparitech, a UK-based research firm, analyzed 24 publicly traded companies that had experienced a data loss of exposure of at least one million records. It found breached companies underperform the market. Even three years after an attack, the average share price was down against the NASDAQ by -15.58%.

GAIN A LEG UP WITH BEST PRACTICES

As an industry, Automotive is making progress in its ability to detect and prevent threats, says Sarah Tennant, strategic advisor of Cyber Initiatives at MEDC.As part of its commitment to mobility, MEDC runs PlanetM, an initiative to foster, retain, and grow the mobility sector and position Michigan as the global epicenter for future transportation. Entrepreneurs in the space can give themselves a leg up by considering these automotive cybersecurity best practices.

Consider security during R&D. Innovators must consider cybersecurity from the get-go, not as an afterthought. The industry's best chance at keeping up with—or better yet, ahead of—threats is working together. At the PlanetM Landing Zone, a coworking space for startups with autonomous, connected, electric, or shared transportation technologies, mobility startups work side-by-side with cybersecurity providers. This allows entrepreneurs to consider security in the research and development stage, rather than tacking on security solutions after the fact, explains Tennant.

Find the right talent. Automotive cybersecurity is significantly different in implementation than IT cybersecurity. It spans various domains and is thus intrinsically complex. The faster you realize this, the better, stresses Heimer.



The implications of automotive cybersecurity extend beyond the vehicles themselves. As cars connect to more roadways and infrastructure, it creates more entry points for hackers.

This complexity can make it hard to secure the skillsets you need to solve cybersecurity challenges. By 2021, there will be as many as 3.5 million unfilled cybersecurity positions across the globe, according to estimates by Cybersecurity Ventures. To help bridge the gap, Michigan is doubling down on specialized training programs. It is part of the reason the state ranks third in the nation for cybersecurity growth potential.

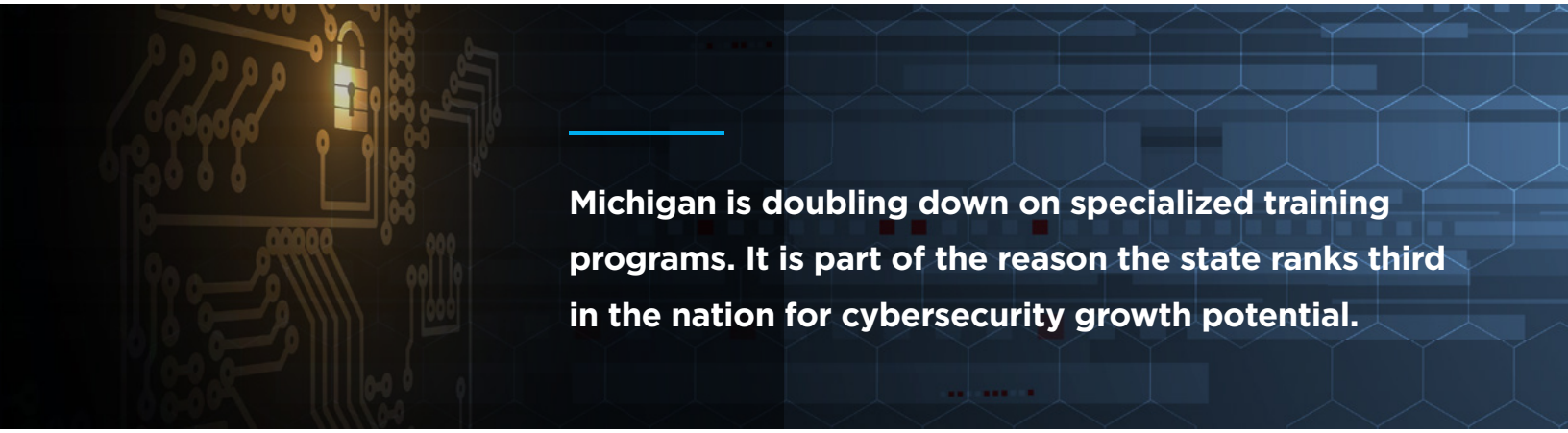
For example, Michigan partnered with Merit Network, a nonprofit governed by Michigan's public universities, to create the Michigan Cyber Range, a platform for cyber exercises, product testing, and digital forensics. The program offers more than 40 professional certifications based on the National Initiative for Cybersecurity Education (NICE) framework across Cyber Hubs throughout Michigan—not just in the Detroit area, notes Tennant.

Michigan also grooms talent with two unique initiatives. The SAE CyberAuto Challenge allows high school and college students to work side-by-side with professionals on hacking exercises on real vehicles. The first-of-its-kind CyberTruck Challenge brings college students, U.S. military academy cadets, academics, and professionals together for hands-on challenges involving infiltrating security systems in semi-trucks and military vehicles. Heimer, who founded the CyberAuto Challenge and cofounded the CyberTruck challenge, says they have helped foster collaboration between the government and industry, including OEMs.

Remember cyber criminals are living, breathing adversaries. "Secure is a verb," says Heimer. "It is not a one-time engineering exercise." Cyber criminals work hard to find chinks in companies' armor, so businesses need strategies for continually assessing threats and adapting as needed. Beyond investing in in-house capabilities, it is worth considering state cybersecurity resources. The Michigan National Guard is leading the way in developing "Cyber Warriors"—individuals who are trained in cybersecurity disciplines. The Michigan Army National Guard's 600 Secret and Top-Secret computer specialty positions are a valuable asset to the government, as well as private industry.

The state also has a first-of-its-kind Michigan Cyber Civilian Corps (MiC3), a group of cybersecurity experts who volunteer to provide assistance to all levels of government, education, and business organizations in the event of a critical cyber incident.

Michigan has long been a hotbed of automotive innovation. Now it is leading the way in automotive cybersecurity, too, by facilitating advancements that help protect technologies—and passengers.



Michigan is doubling down on specialized training programs. It is part of the reason the state ranks third in the nation for cybersecurity growth potential.

PlanetM, an initiative of the Michigan Economic Development Corporation, is a partnership of mobility organizations, communities, educational institutions, research and development, and government agencies working together to develop and deploy the mobility technologies driving the future. Available to any mobility-focused company or investor, PlanetM is a no-cost, concierge service that connects startups, businesses and communities to Michigan's mobility ecosystem—the people, places and resources dedicated to the evolution of transportation mobility. Michigan has always been the leader of the automotive industry, and as transportation technologies continue to evolve in amazing ways, Michigan continues to lead the way. Visit PlanetM.com to learn more.