TRUST

SECURITY

PROTECTING
RYDER AND CUSTOMER ASSETS

IN TODAY'S WORLD, BUSINESSES FACE NUMEROUS RISKS THAT COULD NEGATIVELY IMPACT THEIR OPERATIONS, INCLUDING CRIMINAL ACTIVITY, NATURAL DISASTERS, DATA BREACHES, OR THE WRONGFUL USE OF COMPANY ASSETS.

At Ryder, we strive to mitigate these risks for our customers by ensuring our vehicles are used for lawful purposes and providing safe and secure supply chain solutions. We can only execute this mission if we maintain systems and procedures that protect our people and our assets, and ensure business continuity for our business and our customers. By maintaining a robust security management system, Ryder is better able to serve and protect our customers, and ensure the integrity of the Ryder brand.

OUR APPROACH

We leverage a cross-functional and layered approach to manage operational risks. Individuals from Physical Security, Cybersecurity, Business Continuity, Legal, Compliance, and Corporate Communications collaborate to monitor and carry out Ryder's crisis management planning for our critical processes. Ryder's Group Director of Corporate Security is responsible for our physical security strategy. The Group Director of Global Security ultimately reports to our EVP, Chief Legal Officer and Corporate Secretary.

Ryder's VP & Chief Information Security Officer (CISO) oversees our data security program. Our data security team partners closely with Risk, Audit, Compliance, and Legal in creating and updating relevant policies, informing and training employees and leadership, and monitoring all data security-related risks. The VP & CISO reports to the Chief Information Officer, who collaborates regularly with other members of Ryder's executive leadership team, and provides reports to the Audit Committee of the Board regularly.

CROSS-FUNCTIONAL AND HIERARCHAL APPROACH

To ensure our security processes are operating effectively, our Internal Audit group tests our operating controls regularly for proper development and implementation of applications, as well as for the integrity of program, data files, and computer operations. In addition, Ryder's information security systems are continually audited by third parties, including our customers. We also conduct an annual benchmark of Ryder's security program maturity against the latest global, regional, and industry security standards. Benchmarking results are discussed with the Audit Committee of the Board, and further initiatives are implemented based on their feedback.

CRISIS MANAGEMENT & EMERGENCY PLANNING

Our business continuity strategy involves identifying our greatest risks based on likelihood and severity of impact, and implementing procedures to proactively mitigate the potential impact. We reinforce emergency procedures and evacuation plans at every Ryder facility across the globe to protect our employees and confirm they are prepared for any type of potential disruption, including natural disasters, epidemics, terrorist attacks, and/or data breaches. Each Ryder field location maintains a Business Continuity Plan (BCP) based on location, number of employees, and the type of operational processes used at the location. BCPs outline the specific security risks, procedures, resource needs, insurance plans, and network connectivity risks pertinent to the location. Our Field Operations team discusses and promotes these BCPs when leading regular meetings on disaster response.

NATURAL DISASTERS

With operations across North America and the U.K., our fleet, facilities, and customers are exposed to a variety of natural disasters, including hurricanes, tornados, earthquakes, floods, and blizzards. In addition to communicating emergency and evacuation procedures prior to an event, Ryder leverages technology to analyze where we are most likely to be impacted, and how to communicate with individual facilities before, during, and after an event. We leverage weather software to determine the geographic landscape most likely to be impacted by a storm or disaster. We use this information to strategically and proactively communicate with high-risk facilities on what needs to be done to keep our employees, customers, and communities safe. For example, during hurricane season in Florida, we regularly engage with Miami-Dade Fire Rescue to share best practices and proactively identify how Ryder can support disaster response efforts in the affected areas.

HIGHLIGHT STORY: HURRICANE RESPONSE

In 2017, when the Atlantic and Gulf coasts were hit by three massive hurricanes—Harvey, Irma, and Maria—Ryder was prepared to step in and help. Working with federal, state, and local disaster response, our maintenance and service infrastructure provided much-needed support to impacted areas. In addition, our employees donated time and resources to help those in need, and Ryder provided trucks to deliver needed goods to hard-hit areas. Partnering with the United Way and American Red Cross, Ryder supported thousands of people in need during and after these crises.

To learn more about how we help prevent disruptions for our customers, see Customer Focus.

ASSET SECURITY

Ryder works with our sector peers, governments, and industry associations to continuously identify solutions that reduce the risk of illegal use of transportation vehicles across our industry. We engage with our industry peers each year through the Truck Renting and Leasing Association (TRALA) in order to discuss and formulate best practices on preventing these types of activities. We work with law enforcement agencies, including the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the Transportation Security Administration (TSA) to discuss specific threats to our industry and how to make it safer.

HIGHLIGHT STORY: PROTECTING OUR COMMUNITIES WITH THE TRUCK RENTING AND LEASING ASSOCIATION

In the United States, 25 percent of terrorist attack scenarios investigated by the U.S. Department of Homeland Security employ trucks or vans as weapons. For this reason, our work with TRALA is more important than ever before.

As an industry, it is paramount that we work together to protect rental assets from errant misuse or illegal activities and to safeguard our neighbors and communities from senseless acts of terrorism. Ryder works closely with the Truck Renting and Leasing Association (TRALA) to develop and promote policies that would keep our communities safer. TRALA represents nearly 500 trucking companies throughout North America, which employ more than 57,000 people and represent almost 30 percent of all trucks and tractors on our roads. Through TRALA, Ryder and our peers work continuously with local, regional, and federal law enforcement agencies—including the Department of Homeland Security (DHS), Transportation Security Administration (TSA), and Federal Bureau of Investigation (FBI)—to ensure best practices are employed for the safe use of our assets.

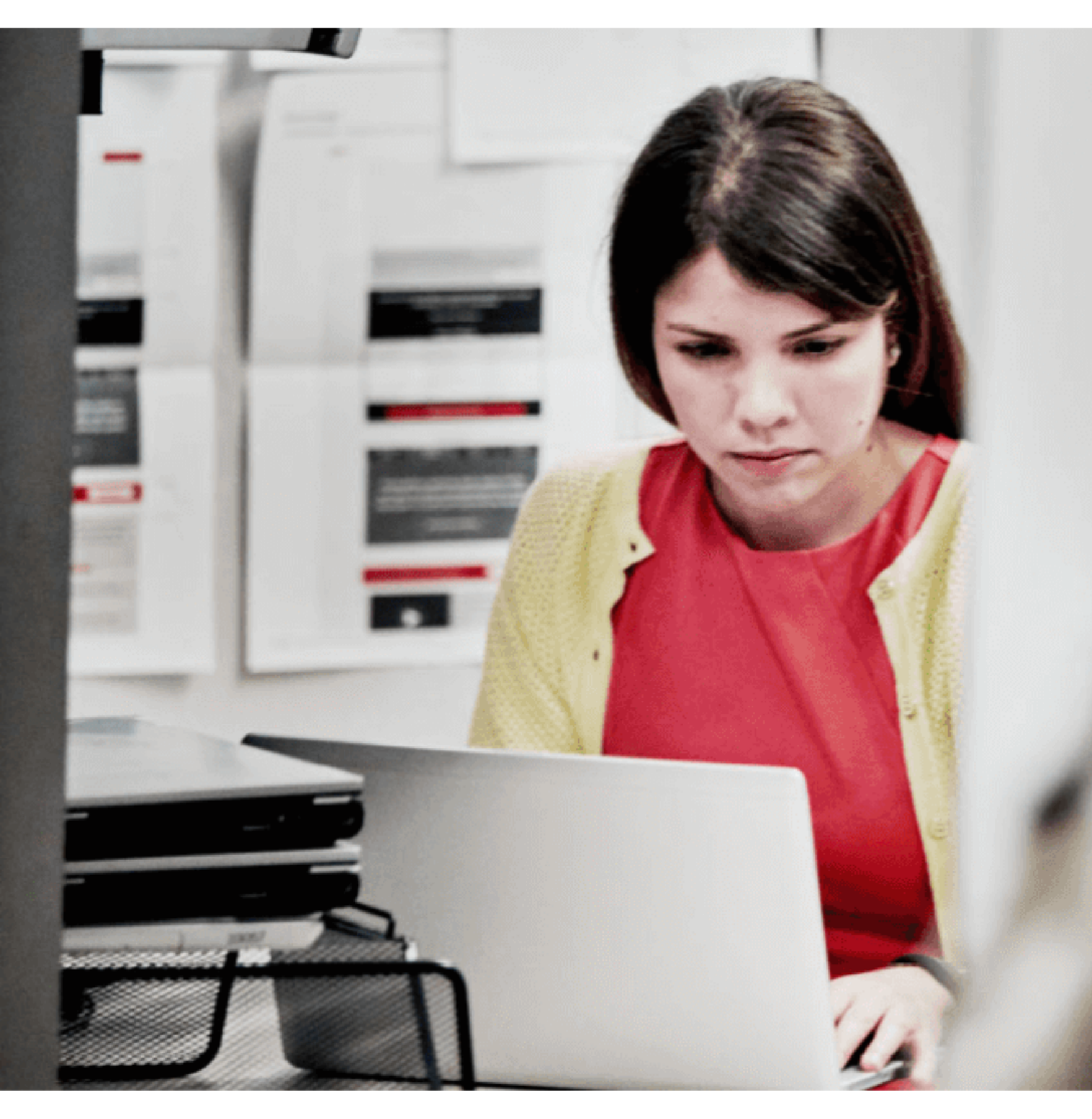
Ryder will continue to adopt the latest safety and security protocols and train our employees on the best practices in asset security. And we are committed to proactively engaging with peers, organizations like TRALA, law enforcement, and federal agencies to keep our assets out of the hands of would-be criminals and terrorists.

SUPPLY CHAIN SECURITY

The security of Ryder's supply chain and those that it operates for its customers is critical to our success. The exploitation of global supply chains by illegitimate actors such as drug smugglers and human traffickers is not only a threat to the general public, but can also cause significant disruptions to legitimate trade and production. To ensure that these supply chains remain secure, Ryder maintains an extensive supply chain security program across our operations that involve international movement of goods. To achieve secure supply chains, the program leverages state of the art technologies, documented security polies and procedures, and numerous supply chain security best practices. Our supply chain operations are certified in the U.S. Customs-Trade Partnership Against Terrorism (C-TPAT), Canada's Partners in Protection (PIP) Program, and Singapore's Secure Trade Program (STP).

In 2014, Ryder's Global Supply Chain Security Program was assessed by the U.S. Department of Homeland Security and attained SafetyAct Certification. Ryder was the first company in its industry to achieve SafetyAct certification of its supply chain security program.

Ryder regularly meets with officials from U.S. Customs and Border Protection to discuss supply chain threats and strategies for mitigating these risks. In 2018, Ryder participated in the Commercial Customs Operations Advisory Committee (COAC)'s Trusted Trader Subcommittee to update and revise the C-TPAT minimum security requirements. By participating in conversations related to security in global supply chains and certifying our program, Ryder is staying in the forefront of this area, enabling our customers to not have to worry about a security issue.



DATA SECURITY

It is important that the data held by Ryder's information systems—such as key financial and operations data, employee information, and customer data—remain confidential and secure. As the data use and privacy risk landscape continues to evolve, regulations, policies, and best practices are rapidly changing across the world. We regularly monitor these trends and update our data privacy and information security initiatives, with a focus on threat identification and prevention, and employee education.

Ryder maintains an extensive set of policies covering security, privacy, and compliance risks, made available electronically to all employees via the Ryder Policy Management System. We refresh these policies annually to ensure they are relevant, targeted to the correct audiences, and include critical components. Our Policy Management System also enables us to easily track and verify that the required employees have read and signed off on relevant policies.

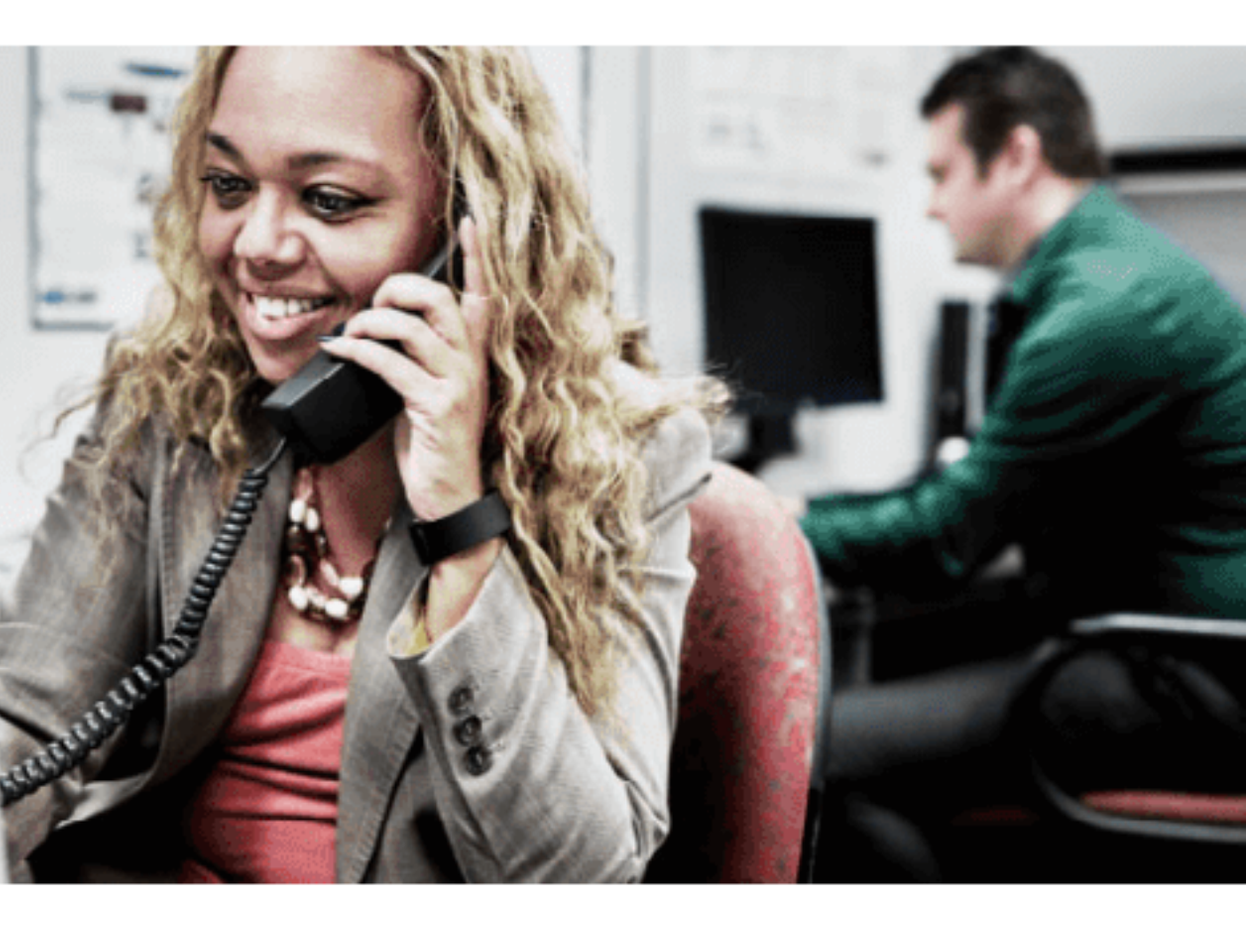
EMPLOYEE TRAINING

Employee education and security awareness are core components of our information security strategy. In 2018, our VP & CISO worked with our Ethics & Compliance group to roll out a computer-based information security training to approximately 8,000 salaried employees and administrators. We plan to roll out tailored security trainings to the entire company in 2019, as well as engage employees informally through lunch and learns, company memos, internal articles, and intranet resources to provide employees with additional knowledge and awareness of data security trends and best practices.

EMPLOYEES TRAINED
8,000

WORKING WITH VENDORS

Ryder's IT Team conducts assessments of the security systems of any vendor with access to confidential information from Ryder. Our contractual agreements with such vendors include heightened information security protocols and requirements for handling personally identifiable or other confidential information.



COLLABORATION

Our security team participates in a number of external peer groups, including the FBI partnership group InfraGard. Additionally, our VP & CISO is a member of the CISO Coalition's Governing body, and is on the CISO Corporate Membership Leadership Council of the Cybersecurity Collaborative. We also increasingly collaborate with our customers to ensure that we are aligned on and are addressing their information security-related needs and concerns.

OUR PERFORMANCE

Ryder is recognized as a leader in supply chain security management by both our customers and government partners. Ryder's various supply chain security certifications are randomly audited by U.S. Customs and Border Protection (CBP) to ensure that our written plans are being implemented at over 170 of our global sites. Over the last 5 years CBP has conducted 11 site validations at Ryder locations throughout the world. Of the 800 security items validated, Ryder has achieved an "in compliance" rating on all 800. In addition, CBP has identified and documented 29 industry best practices at Ryder's facilities.

ADDITIONAL RESOURCES

- Truck Renting and Leasing Association
- Privacy Policy

RYDER CORPORATE HEADQUARTERS
11690 NW 105TH STREET, MIAMI, FLORIDA 33178