From the Chairman

JANUARY 2018

To FedEx Team Members:

Welcome to a special edition of **From the Chairman** — from both our CIO Rob Carter and me. We've co-authored this letter to address the extraordinary implications of cyberthreats and the critical importance of **cybersecurity** for FedEx, our customers, and every team member.

First, let me congratulate you on achieving a record peak season. On several Mondays during peak, we doubled our average daily volume, all while maintaining outstanding customer service levels the entire season. What a testament to your hard work and commitment to our customers! There's no team like the FedEx team when it comes to delivering the holidays. Thank you for your outstanding efforts to keep our Purple Promise front and center.

FWS: the new world of cyberthreats

The cyber world has changed dramatically — for us as individuals, for FedEx, and for companies and countries everywhere. The world's dependence on technology has created enormous risk to what was once thought very secure data. You may have experienced first-hand some of the widespread breaches that affected companies you do business with personally.

Just as the events of 9-11 changed the security protocols in air travel, recent viruses such as WannaCry and NotPetya have changed the way FedEx and other enterprises must manage their IT systems and access to them. Such changes mean you and I must modify our behaviors to protect the security of our company, customer, and employee information. **This is not optional.** Even if it feels inconvenient or involves new processes, *each of us* must cooperate to make cybersecurity a top priority.

Please read what Rob Carter has to say about how the world of technology has changed, how cybersecurity issues affect our lives, and the individual responsibility each of us has, from our senior officers to our front line team members, to protect our brand and our customers' data.

RBC: a look at the Good, Bad and Ugly

Today's technology reminds me of the old Clint Eastwood movie, *The Good, the Bad and the Ugly*. Using that title as a theme, let's explore several aspects of technology — from the terrific benefits to our business and lives to the looming threat of "bad actors."

The Good

The Good, of course, is the many positives technology brings us, particularly connectivity, speed, and convenience. With smartphones, tablets, and PCs, we can connect with friends, find the best route to drive, or simply order dinner. We can bank online, listen to the latest tunes, or make appointments. We keep our family safe by staying connected with them pretty much all the time. By talking to Siri, Alexa, or Google Assistant, we may not even have to lift a finger to get a question answered.

FedEx has used, created, and applied technology since its inception. The strategic use of information has always been a critical part of improving our quality and connecting with our customers. We are known for our innovations such as package tracking, handheld technology, customer automation, and many more "firsts" in the transportation industry. Technology is the central nervous system of our operations and the primary channel through which we serve our customers.

All these things represent the benefits of modern technology — benefits that have helped us grow our business and improve our lives.

The Bad

Technology that is deeply integrated into our business and lives is also where "The Bad" comes in. We become so dependent on those technologies that when they aren't available, for whatever reason, there are big, negative consequences.

We may have more than 650 aircraft, 150,000 vehicles, and 5,000 facilities, but they don't operate and our service suffers if our technology fails.

During peak, we processed hundreds of millions of online customer interactions every day. When our systems are running well, they provide amazing technology for our operations, our team members, and our customers. However, many parts of our technology footprint are aging and in need of modernization.

Many exciting projects are underway to make our systems leading edge and create a more nimble set of capabilities for our business. With the rapid changes in the world around us, we have to move quickly to create digital offerings that adapt easily to our customers' needs. That's where project RENEWAL comes in. It is a multi-year IT modernization project begun in 2009. It moves many legacy applications into several cross-enterprise "cloud-based" core FedEx systems such as "Shipment," "Customer," "Product," "Address," and "Pricing." These new modular cloud systems are critical to the future of our company. RENEWAL will allow us to meet the needs of the future better, faster, and more securely. RENEWAL is where speed-to-value, reliability, and security all meet.

In the meantime, we must make sure our existing systems support the business reliably and securely. That includes things like spreadsheets and programs built within the various business units. As we've scanned our vast network of systems, we've found thousands of unsupported technologies within the company — most of which are more vulnerable to outside attacks than newer cloud-based systems. This "shadow technology" is not supported by the technology teams and often has significant vulnerabilities. If such technology isn't upgraded and maintained, the entire world of FedEx technology is at risk. These "shadow" tools provide great value to helping us perform our jobs, but please be mindful of the consequences of losing critical data or capabilities in a cyberattack.

The Ugly

The greatest benefit of technology — our connectedness to the world — also leads to its greatest risk — inroads for criminals, political enemies, and even terrorists to exploit weaknesses in cybersecurity. That is the Ugly.

Let's take a closer look at the threat landscape.

- Black market thieves are actively stealing personal data, as we've seen in the recent past within the U.S. at Target, Home Depot, Anthem, and Equifax.

- We've also seen nation-state attacks on businesses — North Korea attacked Sony Pictures three years ago to prevent the company's release of a film North Korea deemed unflattering to its leader. A German cyber organization estimates that 53% of all German companies have been the victim of corporate espionage, the stealing of proprietary information.

- Another example is nation-states attacking political enemies such as the StuxNet malicious worm attack in Iran and the NotPetya ransomware in the Ukraine. Ransomware is a cyberattack in which hackers take control of a company's data, encrypt it so the company can't access it, then hold it hostage until the company pays for a code to unlock the data.

- Even the U.S. government has been hacked. About 18 months ago, an arsenal of weapons-grade cybertools was stolen from the National Security Agency. According to a recent *New York Times* article, "America's largest and most secretive intelligence agency had been deeply infiltrated." The hackers stole these U.S.-designed cyberweapons and then turned them against us and other countries. It's important to note that these cyber-weapons aren't just for Microsoft Windows, but span a wide variety of technologies, many of them used by FedEx.

- FedEx is considered a Critical Infrastructure Company (CIC) since our networks circle the world. As such, we are monitored more closely by the governments of nations trying to steal trade secrets.

Now let's talk about the direct impacts this wave of cyberterror is having on our business. These criminals and nation-states have launched attacks that have hurt the FedEx brand that means so much to all of us. It can affect our jobs and harm our customers. This has gotten personal.

Last spring North Korea unleashed the WannaCry virus, which affected our U.S. domestic operations, particularly in our Memphis and Indianapolis hubs. While the vast majority of our servers were protected against this attack, some older systems in our Express hubs had not yet been "patched." Here's where we found out that being 96% patched isn't good enough. We were testing these patches to make sure they didn't degrade performance of these sort control systems. The result is that WannaCry infected the systems and caused a significant operational outage. This led to a national service disruption, and the FedEx brand was used hundreds of times in the media as an example of a company that was impacted.

We can no longer tolerate delays in patching systems connected to the network. Critical patches will be applied within 10 days. Urgent patches will be applied within three days. Unpatched systems will be removed from the network. Much like waiting in security lines at the airport is inconvenient, this new requirement is time-consuming and inconvenient. The risk, however, is far too great to ignore.

Certainly the most devastating and destructive malware FedEx has experienced is the NotPetya attack on TNT last summer. As a result of the attack in the Ukraine mentioned above, a trusted software widely used in the Ukraine was severely compromised. All entities using that software were breached: banks, airports, hospitals, schools, and retail across the country. Even the monitoring systems at the Chernobyl nuclear reactor were affected.

Also hit were companies doing business in Ukraine, including TNT. NotPetya destroyed all data and software on TNT's Microsoft-based personal computers and servers around the world. It knocked out TNT phones and directories, email, call-center support, tracking, billing, clearance, and the TNT website. Fortunately, *no FedEx systems were affected, and no customer data was compromised*. The attack was so intense that, for the first half of FY18, NotPetya cost FedEx $400 million. In fact, were it not for the efforts and resources of the unified FedEx-TNT team, TNT may not have been able to recover and thousands of jobs would have been put at risk. Now that's personal.

Of course no one pulls together better than our people in the face of crisis or disaster. FedEx team members from all over the world rallied to accomplish what seemed impossible.

Within three weeks, 42,000 laptops, work stations, and desktops were restored. Hundreds of applications and their data, running on thousands of servers, were recovered from tape and paper logs. By using the FedEx network as backup throughout the crisis, we were able to continue shipping even on day one, and we announced full capabilities restored on day 100. This was an amazing accomplishment! We thank the entire team, particularly those who worked around the clock for weeks to get our systems back up and running. You inspire us because you truly delivered the Purple Promise to our customers and each other. Well done!

We learned several lessons from the TNT breach and have made important changes. This new, more threatening cyberlandscape requires that we make even more changes to mitigate attacks or prevent them in the first place.

As a consequence, FedEx must and will exert much tighter control on what can be accessed on company machines. Some of the freedom we've allowed on our company-owned PCs and devices will have to be curtailed. We realize this will be inconvenient, but many of the current attacks are launched through personal email, social media, and public websites.

Of course we've restricted access to websites on work devices in the past, but now we'll be restricting some of them even more. The same goes for social media — expect additional limits on how and when you can access various social sites on FedEx equipment for non-work purposes. Also, we no longer allow our team members to access their personal email accounts while they're behind the FedEx firewall.

We need everyone's cooperation to combat security threats on our production systems.

The key to success in this realm is to remember that **security is everyone's business**. It's not just FedEx changing policies and processes — it is each of us being on high security alert in this dangerous cyber world where small missteps can have devastating effects. Remember that your actions online are not "cloaked"; all is visible and what you do can put business and personal data at risk. Check out From the Chairman online for how to report security issues and general cybersecurity do's and don'ts. Also, please familiarize yourself with the information security policy that dictates allowable use of company assets. See the **FedEx Guide for Information Security** (pages 6–9) at https://esso.secure.fedex.com/infosec/standards/docs/InfoSec_Guide.pdf.

FWS and RBC: teamwork and the Purple Promise

We have a great cybersecurity team and have designated major ongoing resources for enterprise-wide security day in, day out, around the world. And you're the key to making it work — your vigilance, your adherence to policy, and your willingness to report.

We'd especially like to thank Denise Wood for her outstanding leadership as chief information security officer for the past 14 years and wish her well in retirement. She and her team have made FedEx security a top priority around the globe. At the same time, we'd like to welcome Gene Sun as our incoming CISO. Gene is a 21-year employee of FedEx who has served in many positions in IT, most recently as vice president, Enterprise Infrastructure Services, and Enterprise Network and Communications Services.

Each of us committing to FedEx cybersecurity is part of our larger commitment to delivering the Purple Promise — to make every FedEx experience outstanding. Be sure to read Dave Bronczek's online discussion of why total commitment to the Purple Promise is vitally important. All of us working together with a "Purple" mindset toward cybersecurity will help create a great new year — and a more secure future — for FedEx.

All the best to you and your families in 2018!

Frederick W. Smith
Chairman and CEO

Rob Carter
EVP, FedEx Information Services, and CIO

APAC Pacific (APAC)

Innovation and accelerated growth continue in APAC

APAC continues to innovate and tap growth areas such as healthcare. At the same time, we're accelerating the growth of large, profitable customers and have already exceeded our planned goal.

Small to mid-sized businesses (SMEs) have long been our focus — the next step is adding new capabilities to acquire leads to grow SMEs faster. For example, a recent "Becoming a FedEx customer" pilot program in Hong Kong makes it easier for SMEs to open new accounts online.

Tremendous progress has been made toward the TNT-FedEx integration in APAC. Japan completed its first phase of integration last June, and the process is moving forward in China, Hong Kong, Malaysia, and Taiwan. Activities include:

- Working together to optimize the ground network
- Consolidating facilities and locations
- Combining delivery routes

The APAC team is excited as it continues its progress to accelerated growth and long-term business success.

Canada

Canada drives profitable growth through improved customer experience

In Canada, we're focusing on improving the customer experience as a key differentiator to drive profitable growth. We know that first contact resolution (FCR) can influence customer loyalty. In fact, a 1% improvement in FCR equates to a 1% improvement in customer satisfaction, a 3–5% improvement in employee satisfaction, and a reduction in our cost to serve.

As such, we are focusing on creating and monitoring key performance indicators that measure customer satisfaction and its relationship to incremental business. The newly launched Customer Experience Council is responsible for ensuring that customer experience metrics are applied across organizations.

In early 2018, we will launch an enhanced new-customer program called Welcome Support for Business. It is targeted at small and medium-sized business customers. The program will provide new customers with a single point of contact to support them throughout their relationship with FedEx.

Capturing more profitable e-commerce business remains one of our top strategic priorities, and we are rapidly expanding our retail presence to enhance the customer experience in this segment. With double-digit e-commerce growth and increasing residential deliveries, we're converting part-time routes to more efficient full-time ones. This has enabled the planning and engineering team to undertake an on-road optimization project to improve capturing more of the e-commerce business/volume with existing resources.

In addition, we launched a day-turn flight between our large hubs in Toronto and Calgary. This allows us to move deferred volumes in off-peak hours during the day.

Latin America and Caribbean (LAC)

New LAC customer experience project connects Memphis directly to Mexico

The Tijuana (TIJ) New Jet City is a new Latin America and Caribbean (LAC) project that will improve transit time and overall reliability to customers both inbound and outbound in Mexico. The project is scheduled to launch in June. Connecting Memphis directly to Tijuana, Mexico, TIJ will add value to businesses that are manufacturing products in the high-tech and medical devices industries because outbound cut-off times will be reduced by three hours and inbound transit time will be improved by at least one day.

LAC has a department dedicated to improving the customer experience. By listening to the voice of our customers and understanding their needs, we learned that our service in that area was limited. We recognized that there was a great opportunity to grow our business. This project will also position FedEx with the best offering in the market and will help our customers to succeed.

LAC is also committed to ensure that our team members embrace the People-Service-Profit philosophy and deliver the Purple Promise. Last fall's natural disasters significantly affected the LAC region, and they gave us an opportunity to bring the FedEx culture to life.

After the earthquakes in Mexico, FedEx supported the communities by turning our stations and ship centers into collection sites for relief supplies. During this time, team members volunteered more than 5,000 hours. After Hurricanes Maria and Irma in Puerto Rico and the Caribbean, LAC worked with various organizations such as the American Red Cross to deliver critical aid on more than 17 special flights. In total, FedEx moved 6,300 tons of relief and other cargo on more than 100 flights for our customers, team members, and humanitarian agencies.

____

Europe

For Europe, working together delivers for our teams and our customers

While the cyberattack that hit our TNT systems has proved to be a challenging time for our business and our team members, it has also opened up opportunities for FedEx and TNT functions to work together to deliver an outstanding experience for our customers. We've seen and heard many positive stories of collaboration and support from teams around the world, again reinforcing the close alignment of our two cultures.

Across Europe we have kick-started our next wave of country integration, including some of Europe's biggest markets: Germany, Benelux, France, Italy, Poland, and the United Kingdom. We are focusing on the areas of Operations, Sales, and Customer Experience, as they represent the largest part of our workforce and our face to our customers.

Bringing our two organizations together remains the focus for each country, though the journey for each will be different and will move at different speeds.

____

Middle East, Indian Subcontinent, and Africa (MEISA)

MEISA integration to be complete by end of May

In the Middle East, India and Southern Africa (MEISA), the integration of both our FedEx Express and TNT team members as well as operations is slated to wrap up by the end of this fiscal year.

Most team members in the region are aligned under a single structure with consistent job titles, grades, and reporting lines. Sales teams will follow, with a unified structure in place by June. Also by the end of FY18, MEISA road networks will operate as one, enabling our sales team to offer customers economy services and connect them to our Asia and European road networks.

Within MEISA integrating our Global Service Participants and Associate markets is an essential part of our service commitment. So far, 44 countries have completed this integration and we plan to integrate 14 more countries by the end of FY18.

Operations across the Middle East have been integrated, consolidating our commercial and customer experience activities. This process brings together delivery routes, stations, and depots. In South Africa and India, the largest MEISA countries, we'll complete route consolidation and co-locating our stations and depots by May.

In United Arab Emirates (UAE) rebranding vehicles with the FedEx logo has begun. Couriers in the UAE, Bahrain, and Kuwait are now wearing the FedEx uniform, and in those countries most retail facilities accept both FedEx and TNT packages, a move that will shortly expand to the other direct-served countries in the region.

Finally, many TNT managers and professionals have completed Quality Driven Management (QDM) training. It gives them the tools to ensure quality every day. Such training will expand to support our team members in achieving continuous improvement and innovation.