Memorandum

TO: Steve Master, CEO and acting CIO of Parts Unlimited

FROM: Kyler Kent, advisor to the CEO

DATE: October 16, 2022

SUBJECT: Voluntary cybersecurity governance frameworks for Parts Unlimited

Cybersecurity governance is of critical concern to Parts Unlimited. Being a large distributor of automotive parts across the U.S., our company and clients are subject to numerous cyber risks. To properly address these risks, we must start with a foundation of strong, coherent governance principles. We must also embrace these governance frameworks for the sake of our clients, automobile companies, as a supplier. The proposed governance frameworks include ISO/SAE 21434:2021, the NIST Cybersecurity Framework, and the DevOps governance approach.

ISO/SAE 21434:2021 is a tailored cybersecurity risk framework for managing electrically-related cybersecurity risks in vehicles (ISO, 2021, para. 1). As part of our due diligence as a supplier, we must recognize that our electrical components must be carefully integrated with an overall vehicle's architecture and prevent unnecessary vulnerabilities. If our parts lead to the successful exploitation of a vehicle's onboard systems, the results could be catastrophic: death of passengers, occupants, or pedestrians through the hijacking of vehicle safety or control systems, massive litigation due to the previously mentioned circumstances, and massive governmental and regulatory action against Parts Unlimited.

Let's take a brief detour and example of a very modest, public vulnerability involving auto parts within Kia and Hyundai vehicles. The weakness has been in the access control system of the vehicles—namely the "mechanical" ignition lock cylinder (DiLella & Day, 2022, para. 2). This vulnerability appeared patterned for over a decade from 2010-2021 vehicles (para. 2). As a result of weak access control to the vehicle's ignition system, criminals can easily steal the vehicle and engage in auto theft (para. 19). The primary impact is easy theft, not loss of life. However, the backlash has been substantial. Due to massive online publication (e.g., TikTok) of the exploits, auto theft just in these vulnerable categories has surged as much as "800%" in certain areas (para. 5). The financial and social impact are easily appreciated for the vehicle's owner. However, a dozen class action lawsuits have already been filed (para. 20). The ensuing legal and regulatory nightmare will only multiply for Hyundai and Kia. Thus, we as Parts Unlimited must remain vigilant in ensuring we are only distributing the safest and most secure auto parts, especially in regards to access control, vehicle control, and vehicle safety systems.

Thus, the need for ISO/SAE 21434:2021 cannot be understated. Additionally, the need for safety among our parts is paramount. This reality is illustrated in the crosswalk between ISO/SAE 21434 and ISO 26262 (Costantino et al., 2022, p. 86). The elements in both ISO's vehicle security and safety plans are nearly identical, and include the following steps:

1. Creation of a [security or safety] culture
2. Organization competencies
3. Responsibility definition
4. Information sharing
5. Impact analysis
6. A [security or safety] plan
7. Tailoring activities
8. Reuse activities
9. Request of audit
10. [Security or safety] assessment
11. A case example
12. A rigor level (Costantino et al., 2022, p. 86).

By utilizing this abridged version of ISO/SAE 21434 and ISO 26262, we are holistically mitigating cybersecurity and safety threats for clients and addressing governance from a much broader perspective. We are seeing the utilization of ISO 21434 from governance leaders like Deloitte within this vertical (see "Deloitte's Automotive Supplier Cyber Security Framework") (Deloitte, 2022, pp. 2-4).

Next, after consideration of our end products, we need to consider our internal cybersecurity governance processes and security mechanisms while we conduct business. The NIST Cybersecurity Framework would best serve our organization and effectively prepare and combat attacks. While this framework is involuntary to federal agencies, it is still applicable to our organization and covers the basics. NIST CSF sets the standard and will allow us to meet or exceed national cybersecurity standards. It is simple enough to be broken down into five core steps which include: identify, protect, detect, respond, and recover (NIST, 2018, pp. 7-8). Each step needs execution "concurrently" to help us achieve a "culture" of cybersecurity readiness (p. 7).

Furthermore, our goal is to become a Tier 4 organization per NIST. That is an organization that has an adaptive risk management process, "organization-wide" cybersecurity practice, and community involvement (NIST, 2018, pp. 10-11). I do not think this is a lofty, unachievable goal for Parts Unlimited. We need to have monthly meetings as well as spontaneous meetings after incidents. We can use these meetings to adapt and change our cybersecurity governance. Next, we need to involve the rest of the organization in these meetings and realize we are all contributing to Parts Unlimited's cybersecurity. Employees must voice their concerns and opinions for the CISO, John Pesche, at these meetings and not during regular work hours. This practice will allow us to come together as a whole and effectively address our cyber risks. Finally, we must engage in cyber threat intelligence, internally and externally. We must share threats with the community and the Automotive ISAC (Information Sharing and Analysis Center). This engagement will require membership with the ISAC. All of these steps are actionable and achievable now. So, let's get started today and works towards this great achievement.

The final note is briefly on DevOps. Our organization must move away from the traditional waterfall approach and must embrace DevOps with governance. By October 30th, we are to have a company-wide meeting discussing step one of all frameworks in unison. I look forward to this multi-governance deployment and secure ascension of Parts Unlimited.

References

Costantino, G., De Vincenzi, M., & Matteucci, I. (2022). In-Depth Exploration of ISO/SAE 21434 and Its Correlations with Existing Standards. *IEEE Communications Standards Magazine, 6*(1), 84-92.

Deloitte. (2022, January). UNECE – Cyber Security Management System Readiness for Automotive Suppliers. In *deloitte.com*. Retrieved October 16, 2022, from https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Deloitte_Cyber_Security_Management_System_Automotive_Suppliers.pdf

DiLella, C., & Day, A. (2022, September 10). *TikTok challenge spurs rise in thefts of Kia, Hyundai cars*. CNBC. Retrieved October 16, 2022, from https://www.cnbc.com/2022/09/08/tiktok-challenge-spurs-rise-in-thefts-of-kia-hyundai-cars.html

ISO. (2021, August). *ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering*. ISO.org. Retrieved October 16, 2022, from https://www.iso.org/standard/70918.html

NIST. (2018, April 16). Framework for Improving Critical Infrastructure Cybersecurity. In *NIST.gov* (Version 1.1). NIST Technical Series Publications. Retrieved October 16, 2022, from https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf