CSS441-SECURITY COMPLIANCE

Diesel Company Security Compliance

Joshua Powell

09DEC2022

Contents

Security Compliance Project

Section 1- Company Overview

The Diesel Company has a lot going on and is on top of its security considering recent events that occurred in the past year. They had to up their physical security measures due to the theft of vehicles. The company has also hired a third-party vendor to handle software and network securities that are involved with the day-to-day business that is conducted via the Service Department to upper management. They also run tests every three to four weeks on the employees via email, by sending them fake phishing emails that keep everyone on their toes to make sure they are always in a security mindset. Considering the heavy work involved in the shop, they also follow OSHA and EPA standards in the proper handling of waste and keeping areas clean as well as how clean they should be. They follow the Code of Federal Regulation standards that have been put into play over the years and it means delegating individuals to make sure that everyone is doing their part keeping areas safe and workplaces clean, as well as, staying safe.

Section 2 – Federal and State Regulations, Directives, and Act

Federal Regulations

49CFR 1910: This regulation or as OSHA puts it "standards" carries the same weight as Laws and are not to mistaken as an optional rule of thumb. In this regulation the shops that are under the company need to follow this regulation. 29CFR1910 subpart D goes into detail about how to clean walkways and workspaces should be. It describes how clean it should be and what state everything should be in (*Regulations (Standards - 29 CFR) | Occupational Safety and Health Administration*, n.d.).

49CFR: This regulation covers Transportation Workplace Drug and Alcohol Testing Programs, Hazardous material Handling, and Federal Motor Vehicle Safety Standards. This is the regulation that covers what should be inspected on trucks by the Diesel Technicians that work in the shop ie DOT inspections. This also means that if a tech in the shop were to miss a vital problem and release the truck and something bad happened the Technician would be liable given, they had proper training before the incident. This is where making sure that our Diesel Technicians are properly trained and understand the risks that are involved with the job (49 CFR - Hazardous Materials Transportation Regulations From Labelmaster, n.d.).

Fair Labor Standards Act: This act makes sure that employees are being properly paid and no underage workers are doing certain jobs that are deemed to be dangerous. It also makes sure that any such job does not conflict with their being able to go to school as well (*Summary of the Major Laws of the Department of Labor | U.S. Department of Labor*, n.d.).

Immigration and nationality act: This act applies to those aliens authorized to work in the United States under non-immigration visa programs (*Summary of the Major Laws of the Department of Labor | U.S. Department of Labor*, n.d.).

Electronic Communications Privacy Act: In this act/regulation prohibits any employer from monitoring employees' personal phone calls even if they are made on the employer's property. They are also required to disclose that they are monitoring phone call if they are (*Employee Privacy Rights: Everything You Need to Know*, n.d.).

State Regulations

South Carolina Human Affairs Law: This law protects employees against any unfair treatment or harassment, because of race, color, religion, sex, national origin, age, or disability in the workplace (Potts, 2017).

South Carolina Code Title 41 Chapter 7: This covers that employees have the right to work without having/not having a membership to a union (Council, 2014).

How Federal Regulations Apply

We have covered multiple regulations and cannot go without saying that there are a lot more but starting with the 29CFR. This regulation is important in the workplace, because it covers the necessities of having a clean environment within the workplace, along with holding employees accountable for their actions in the workplace. The next is the 49 CFR, which goes into detail about how to hold employees accountable for the misuse of alcohol and drugs while working around commercial vehicles. It also goes into detail about the proper inspection of commercial vehicles and the checks necessary to make sure that the vehicle is up to code.

The Fair Labor Standards Act is what South Carolina goes by for enforcing overtime and who can work what jobs under the age of 18 (ie whether they are too dangerous or the person is still in school). The next is The Immigration and Nationality Act, which goes into detail about authorized aliens who are allowed to work in the U.S. depending on the visa program they are on. Then there is the Electronic Communications Privacy Act. This implies that no employer is authorized to monitor employees' phone calls and is required to let the employee know that they are if they are. For if they do not, they can face lawsuits or penalization.

Two State Regulations that tie into the company are South Carolina's Human Affairs Law and South Carolina Code Title 41 Chapter 7. The Human Affairs Law prevents the unfair treatment and harassment of anyone in the workplace due to their race, color, age, sex, nationality, or disability. The Code Title 41 Chapter 7 states that anyone wanting to work can work if the company wants them and is not required to pay for membership into a union just to do so.

Security Compliance Project

Section 3 - Compliance Plan

Policies, Standards, Processes and Guidelines

Policies – This is what the company gets a broad guidance from and can in ad-verdantly divert disaster with a good policy in place. It is used to provide a broad guidance to legal and regulatory requirements, employee conduct, information security, and financial integrity, and many other topics. Which will help in creating what is next.

Standards – These provide the rules and checks. This is what employees will have to adhere to be employed and to stay employed. Therefore, having a good policy followed by good standards is so crucial in having a company that flourishes.

Processes – This is where you want to make sure that the day-to-day tasks are laid out and that there is a significant amount of detail and exactness to what should and should not be done. There will always be changes, but the key is to make sure that and processes that a company has been updated accordingly.

Guidelines – These Supply a better understanding to the employees on what is exactly needed from them and what is allowed and not allowed. This can be a posting on the safety board and making sure that employees wear safety glasses and ear pro while in the shop per the 49 CFR allocated above (*Policies, Procedures, and Standards | BPMInstitute.org*, n.d.).

Relationship between Controls and Audits

When it comes to Policies, Standards, Processes, and Guidelines there is a lot that goes into making sure that each of these is upheld to the highest standard by managers and employees alike. Controls help set the basis for the enterprise and help make sure that they

are implemented by running audits to ensure that the standard set by the controls is what is being done. You can have controls, but with human nature the only way to make sure they are enforced from the highest level all the way down to the lowest level is by having audits and making sure audit reports are updated on a regular basis. This also will increase business by keeping employees and managers in check ethically and morally you can ensure that everyone one including customers are taken care of (*Policies, Procedures, and Standards | BPMInstitute.org*, n.d.).

The Sarbanes-Oxley Act

The Sarbanes-Oxley Act was enacted in 2002 due to a scandal within several organizations that resulted in investors and the financial market falling victim to it and so issued this act being implemented. Enron was one of these organizations that was committing financial fraud and dropped from $90.75 a share in 2000 to only $0.26 by 2002. This was because a whistleblower disclosed that Enron was hiding debts and losses using accounting techniques, such as hiding bad debt and assets from creditors and investors via off-balance-sheet special purpose vehicles. Another company was WorldCom that had done what is known as cooking the books and during the tech boom in the later part of the 90's to early 2000's had skyrocketed to a net worth over 100 billion. When tech companies started shedding sales following the boom WorldCom started sugar coating their profits by writing losses off as profits and one number was that they had reportedly had profits of $1.4billion in Quarter 1 of 2002 when it should have been -$1.4 billion. This led to Ebbers being arrested and charged with securities fraud and 25 years in jail. The next and last company I need to mention is the Tyco International scandal. This was where two people CEO and Chairman Dennis Kozlowski and

Corporate chief financial Officer Mark Swartz stole around $ 600 million dollars and cause many investors to fall victim to their outlandish behavior. This ultimately resulted in them being fined and having to pay back $ 150 million in fines and damages a piece along with jail time (*Sarbanes-Oxley Act*, n.d.).

The different implications Regulations have on Government and non-Government entities

Regulations help to maintain civil liberties and as far as government goes, they help to enforce such regulations. Whereas, with non-Government entities they force the change of regulations by means of promoting anything from transparency, free expression, equality within all aspects of regulations, and protecting the environment. They each have a part in ensuring change and enforcement in civil society. This is the basis for changes withing regulations that regulate businesses to ensure that we are protecting all things that all hold dear within ethical and moral boundaries set by the civil society and all humans (*Non-Governmental Organizations (NGOs) in the United States*, 2021).

Section 4 – Acceptable Use Policy

Global Regulations

On a global scale there are times where we will have contact with organizations that operate inside the US but are based outside of the United States. We do not have direct ties to employees working overseas, because we are based solely in the United States. We do however have to abide by the federal trade commission and any other federal laws that dictate how we are to conduct ourselves internationally if there does come a time when we must (*Privacy Shield Certification*, n.d.).

Safe Harbor

Safe Harbor is a standard that was taken out in the early part of 2015 by a ruling in Europe due to privacy laws being violated by Facebook in Australia and with that came EU|U.S. Privacy Shield Framework which was brought into play in 2017. This act is referred to as Safe Harbor 2.0. This new framework details Enhanced Dispute Resolution Systems with additional reporting criteria. A US-based privacy ombudsperson to handle complaints regarding data access by US intelligence agencies. Stricter controls on onward transfer of data once outside of the European Union and Switzerland. This entails any company in the US wanting or trying to have dealings internationally must be certified. We will have to self-certify with the federal trade commission to be able to have any dealings with outside countries when it comes to data. The Privacy Trust Privacy Shield Program provides guidance on this and lets us know what we need to do to get self-certified (*Privacy Shield Certification*, n.d.).

Work Councils

Within our company there is a lot of data being collected and used to help move the company forward. However, this also means there is other information being collected that falls under privacy laws and should not be collected unless it's for the owner's personal use or for reasonably justified for the sole use of the company and is needed for the business. Privacy Trust provides such companies as us with a dispute resolution service (independent resource mechanism) and an outside compliance review (verification) service (*Privacy Shield Certification*, n.d.).

Acceptable Use Policy and Enforcement Ethics

The ethical considerations for this are to ensure that we abide by the Framework for which the environment we are working in and sense we do not have any ties internationally there is only a brief description to be laid out. We will need to make sure that all transactions and processes that might be done internationally go through the right channels so we can move forward as a company and to make sure that any data no matter the use is used correctly and justly to protect us and our customers (*Privacy Shield Certification*, n.d.).

Section 5 – Certification and Accreditation

Certification and Accreditation

Certification: When it comes to being certified as a diesel technician dealership there is a great deal in making sure that not only are they safe but also that the technology is handled properly. When it comes to reading data from the ecu's inside the vehicle you must have a good sense of security as to hooking up to make sure that you are not damaging the customers asset. This can be prevented by making sure that there is proper voltage on the system prior to hooking up and flashing the firmware. The last thing any customer needs is an employee hooking up to a vehicle and not verifying the battery voltage and flashing the ecu only to have it disconnected and then haft to have the ecu sent off for component repair because the employee failed to take the necessary precautions to prevent the catastrophe. Thus, costing the dealership thousands of dollars on the customers vehicle because an employee failed to do what was necessary (Carnwell, 2022).

Accreditation: This is primarily what follows being certified. Meaning that to be accredited you must meet certain criteria, be verified, or get a certain certification by a certain party to obtain the accreditation. The accreditation in any standard is only as good as the criteria that back it. This means that whoever or whomever accredited the company or business must be in good standing and have a good background for the accreditation to mean anything (Carnwell, 2022).

Certification and Accreditation Frameworks

Certification Framework: One certification to guarantee that standards are held across the board when it comes to IT management is the National Institute of Technology (NIST) Cybersecurity Framework. This certification is considered nationally and

globally. It is a voluntary framework and is considered for primarily critical frameworks such as our organization as we help to keep the logistic side of our nation moving and operational. We play a part in the security and using the NIST framework will help in mitigating cybersecurity risks by using existing standards, guidelines, and best practices (Kirvan, 2021).

Second certification I want to inform you about is ISO (International Organization for Standardization) 27001, which is good for big and small frameworks. This certification framework is intended to help evaluate the application and the security around it to ensure that it is operating properly to its needs and performance to a certain security threat (Kirvan, 2021)..

Thirdly for our organization is to make sure that we follow SAE J1939-91 as a dealership we have to uphold the highest level of professionalism when working on our customers vehicles. This mainly entails the Electronic Control units in the vehicle, but every time someone hooks up to a truck, we must make sure that we are doing our due diligence to ensure that we are not further damaging our customers vehicles. With SAE's new J1939-91 standard which has not come into play yet in securing the J1939-13 connector, the green 9-pin connector that allows the hooking up of diagnostic equipment. Even though it helps in the diagnostic procedures it poses a threat to customers if used with ill intent. This means that as a dealership we need to ensure that our customers can trust us anytime, we hook up to their vehicle and that they are in fact getting the most secure and efficient service that they can get (*J1939-91 (WIP) SAE J1939 Network Security - SAE International*, n.d.).

Section 6 - Preparing for Certification

DIACAP (**DoD Information Assurance Certification and Accreditation Process)**

DIACAP is a department of defense process to ensure that risk management was applied to information systems. DIACAP embraced DODI 8500.2 that details information assurance controls as the pivot point for security requirements for all automated information systems. This process basically ensures that all information systems tools and techniques that were used in a DoD setting were accredited (Techopedia, 2013).

ISO27002 (International Organization for Standardization 27002)

This standardization is a collection of information security guidelines. These guidelines are intended to help implement, maintain, and improve their information security management structure. The hundreds of control mechanisms and potential controls laid out in the ISO27002 are designed to implemented with guidance provided in the ISO27001.

The framework for the ISO27002 can be applied to our Diesel Technician's computers and any other information sharing devices. This means that any j1939 device that hooks up to the trucks to how each tech views their emails. Using some of the controls laid out in the ISO27002 would be a good idea to keep things secure for our customers and keep our employees out of being centered on if something did go wrong.

This standardization would most definitely have a bit of overlap as it is an international standardization and is used in a lot of information-sharing areas. There is a need for making sure that along the step of each process for following this standardization we need to make sure that the companies and government do not rush the process to secure our information-sharing systems.

ISO27002 is an extensive standardization but allows for a company or government agency to make sure they are adhering to keeping all Pii and any other information secure from any malicious activity or person. This would be followed by making sure that the guidance laid out in ISO27001 is in fact adhered to through the controls laid out in ISO27002 (Cole, 2013).

References

1. *Regulations (Standards - 29 CFR) | Occupational Safety and Health Administration*. (n.d.). https://www.osha.gov/laws-regs/regulations/standardnumber
2. *49 CFR - Hazardous Materials Transportation Regulations from Labelmaster*. (n.d.). https://www.labelmaster.com/49-cfr
3. *Summary of the Major Laws of the Department of Labor | U.S. Department of Labor*. (n.d.). https://www.dol.gov/general/aboutdol/majorlaws
4. *Employee Privacy Rights: Everything You Need to Know*. (n.d.). UpCounsel. https://www.upcounsel.com/employee-privacy-rights
5. Potts, H. &. (2017, March 17). *The South Carolina Human Affairs Law*. Hitchcock & Potts. https://hitchcock-potts.com/blog/south-carolina-human-affairs-law/
6. Council, S. C. P. (2014, September 2). *Do South Carolinians Have the Right to Work?* The South Carolina Policy Council. https://scpolicycouncil.org/research/taxes/righttowork
7. *Policies, Procedures, and Standards | BPMInstitute.org*. (n.d.). https://www.bpminstitute.org/resources/articles/policies-procedures-and-standards
8. *Sarbanes-Oxley Act*. (n.d.). LII / Legal Information Institute. https://www.law.cornell.edu/wex/sarbanes-oxley_act
9. *Non-Governmental Organizations (NGOs) in the United States*. (2021, January 19). United States Department of State. https://www.state.gov/non-governmental-organizations-ngos-in-the-united-states/
10. *Privacy Shield Certification*. (n.d.). https://www.privacytrust.com/privacyshield/

11. Carnwell, L. (2022, March 9). *What is the difference between accreditation and certification?* Planning, BIM & Construction Today. https://www.pbctoday.co.uk/news/planning-construction-news/accreditation-and-certification-difference/32133/

12. Kirvan, P. (2021, December 21). *Top 10 IT security frameworks and standards explained*. Security. https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

13. *J1939-91 (WIP) SAE J1939 Network Security - SAE International*. (n.d.). https://www.sae.org/standards/content/j1939-91/

14. Techopedia. (2013, October 11). *DOD Information Assurance Certification and Accreditation Process (DIACAP)*. Techopedia.com. https://www.techopedia.com/definition/25825/dod-information-assurance-certification-and-accreditation-process-diacap

15. Cole, B. (2013, November 14). *ISO 27002 (International Organization for Standardization 27002)*. Security. https://www.techtarget.com/searchsecurity/definition/ISO-27002-International-Organization-for-Standardization-27002

16.