TRANSPORTATION ISSUE

SPRING 2018

Four Steps to Building a Successful Safety Training Initiative

No one wants to receive "that call" in the middle of the night, letting you know that one of your drivers has been involved in a major accident. The good news is there are steps that you can take to minimize the chances of accidents happening within your company. For starters, it is important to have a strong training initiative designed to empower your drivers with the proper tools and knowledge to keep safety "top of mind."

DRIVER BEHAVIOR: THE ROOT CAUSE OF ACCIDENTS

If you were to sit down and analyze past accidents within your company, you may notice one consistent trend—driver behavior has likely played a major role in the root cause of accidents. Safety, therefore, should not simply be delegated to one person in your company. Instead, safety must be an innate value within your company, impacting every decision made by each driver.

Implementing a strong safety training initiative, especially in an environment where a large portion of the workforce is mobile, may initially seem like a daunting task. However, online programs allow drivers to easily participate and engage in safety training, regardless of their location. The following four steps can be utilized to build a successful safety training initiative designed to create a culture of accident prevention.

(continued)

Randy Sturdivant
Director of Business Development & Strategic Partnerships
Vertical Alliance Group, Inc.

What's Inside:

STEP 1: IDENTIFY TRENDS

The best indicator of future performance is past performance. Thus, you should evaluate your insurance loss runs (history of claims) and Compliance Safety Accountability (CSA) violations to identify trends and behaviors that could lead to a major accident. Ask yourself these questions:

1. **What's the number one cause of my losses?**
2. **What are the most frequent CSA violations that could lead to an accident?**
3. **How are we training our drivers to improve these behaviors?**

Remember, just because you have not yet had a catastrophic accident does not mean the frequency of your minor accidents should be ignored. Avoiding a major accident isn't just luck. Getting ahead of the trends and understanding your problem areas are your keys to creating a safe workplace.

STEP 2: CREATE STRATEGY TO TARGET CHALLENGES

After you have identified your trends, you must create a strategy to train your drivers. Training leads to awareness, and awareness leads to reduced losses. One question companies often ask is: "How much training is enough?" The short answer is: "As much as possible." You can never conduct too much safety training. New drivers should be trained during orientation (onboarding) on defensive driving skills, Federal Motor Carrier Safety Administration (FMCSA) rules/regulations, maintenance and hours of service. Starting with training on these topics during orientation has been shown to have an extremely positive impact on the trending of violations. In addition to training during the new driver onboarding process, weekly safety and awareness training for all drivers is paramount to building a best-in-class safety culture. This weekly training can be done utilizing online micro-training videos, which can be completed in less than 10 minutes.

Online micro-training videos not only allow you to hold your drivers' attention during the training, but also keep drivers on the road, making money. Regulatory updates should also be shared with drivers to keep them abreast of new rules and regulations. Additionally, testing drivers after having watched training videos is an easy way to prove your drivers have a comprehension of the materials. As a result, you will save time and labor dollars, while your drivers improve their "top of mind" awareness of safety best practices.

(continued on page 4)

New Hires at Napa River Make Us Stronger Than Ever

Peter Mazurek
Director of Marketing & TPA Operations
Napa River Insurance Services
317.810.2029
pmazurek@napariverinsurance.com

Napa River has grown substantially in the past few years. In fact, Napa River experienced 58% growth in its transportation business alone during the past two calendar years. In order to keep up with our growing client base and its changing needs, we have appointed Peter Mazurek as Director of Marketing & TPA Operations. Peter has over 20 years of experience managing the operational and financial aspects of running a third-party administrator (TPA), and has held various positions within the insurance industry, including work in underwriting and treaty accounting. He most recently served as Vice President of Operations & Business Development at Innova Claims Management LLC, which he joined after the successful sale of Specialty Claims Management, LLC. Through his past experience at several organizations, Peter has garnered extensive knowledge in systems and work flows for claims organizations.

In addition to Peter, Carlos Lopez joined Napa River as Claim Manager for transportation. Carlos has 15 years of experience in the insurance industry, handling claims across multiple lines of business and leading process improvement and mentoring initiatives. Prior to joining Napa River, Carlos was Claims Supervisor at Protective Insurance and held positions at Liberty Mutual Commercial and Allstate. He earned his Chartered Property and Casualty Underwriter (CPCU) and Senior Claims Law Associate (SCLA) designations.

Carlos Lopez
Claim Manager
Hudson Insurance Group
317.810.2046
clopez@napariverinsurance.com

At Napa River, our strength is in our people. We are now stronger than ever, and we are ready for any and all challenges that may lie ahead. We are confident that the addition of Peter and Carlos to the Napa River team will enhance our ability to provide the exceptional products and services our clients have come to expect from us. But we're not stopping there; in the next few months, we will continue to expand our team. Exciting changes are taking place at Napa River, and we thank you for being a part of our journey.

(Continued from page 2)

STEP 3: MEASURE RESULTS THROUGH BENCHMARKING

As you implement your training strategy, you will want to monitor how well your training efforts are impacting your company's performance. Benchmarking your CSA data and insurance loss runs with scheduled ongoing evaluation points can help you implement a sustainable process. This will help you understand not only what adjustments may be needed in your training, but also on which problem areas you should focus. Measuring your success can help you realize continuous improvement until you have reached your benchmarking goals.

STEP 4: REPEAT

Finally, safety is a journey that everyone in your company must embark on together. Accidents happen, even in the safest of companies. When they do happen, it is crucial to identify the trends that caused them. Then you must develop a training strategy to improve upon them and measure your results through benchmarking. The first step towards changing behavior starts with training and communication, but note there is no last step on the training journey.

Remember, if your company has a high frequency of accidents and your training does not focus on prevention, your frequency and severity of accidents will continue to rise. Training and communication are proven ways to achieve behavioral change within your company. Implementing an online training component also helps you to ensure your safety message is in front of your drivers, no matter where they are on the road.

Randy Sturdivant is the Director of Business Development and Strategic Partnerships for Vertical Alliance Group, Inc. With more than a decade of experience working in the online training space, Randy has helped companies across the nation build best-in-class safety training programs utilizing a proven online training system. He regularly presents at industry conferences on how to avoid risk by inspiring behavioral change in employees through targeted training initiatives.

Cyber Liability: Today's Rapidly Growing Risk

John Whall
Senior Vice President
Hudson Insurance Group
816.778.0710
jwhall@hudsoninsgroup.com

This is the third article in a series. The first two parts discussed the nature of cyber liability and ways your organization can be harmed. The final article will be Part Four: *Preparing for the Time When Preventive Measures Fail.*

PART THREE:

Ways You Can Limit Exposure Through Preventive Measures

An ounce of prevention is worth a pound of cure. Network management is a highly complicated and technical function that relies on specific equipment, configurations and practices; thus, this article will focus on cyber liability at the conceptual level.

Someone in each organization needs to be in charge of information security. It should not be merely a task on their list of duties; it should be clear that they have the appropriate authority and responsibility to keep the organization's systems and information safe.

Experts say there are three legs to data security: (1) what you have, (2) who has access to it and (3) how and how long is it being kept. With that in mind, the organization should determine what are the "crown jewels" that need to be protected. In a healthcare organization, the jewels are not only limited to medical information; names and social security numbers are highly valued targets as well, as is information related to employees. (Information that would populate a W-2 form is highly desired by criminals for generating phony tax returns in order to fraudulently claim tax refunds.)

Once the jewels have been identified, the organization should consider who has access to them. Access should continuously be managed and limited in time and scope to only that which is necessary to the tasks at hand. This may reach all the way to the level of contract terms with vendors. Permission management is an organization's way of knowing not only who has access to what, but when and how those people are accessing it. Actively monitoring a network can identify abnormal activity early and allow the organization to shut down an attack before it can really get started. Larger organizations may have dedicated staff to provide this function, but for smaller providers, there are plenty of hosted options where a third party can perform this function. Costs have come way down for these services, so it is not out of reach financially. Proper implementation of this technique may be the best defense against a rogue employee incident. Not only can it catch a thief, but just knowing that the practice is in place, and the employees' every move on that network is recorded and reviewable, is a powerful disincentive.

How and how long data is kept also are important considerations. Organizations may have huge volumes of data, but does it all really need to reside on the network? If the answer is no, then remove it. You don't have to destroy or delete it; instead move it to a safe place and encrypt it. Doing so helps ensure there is one less piece of vulnerable data.

(continued)

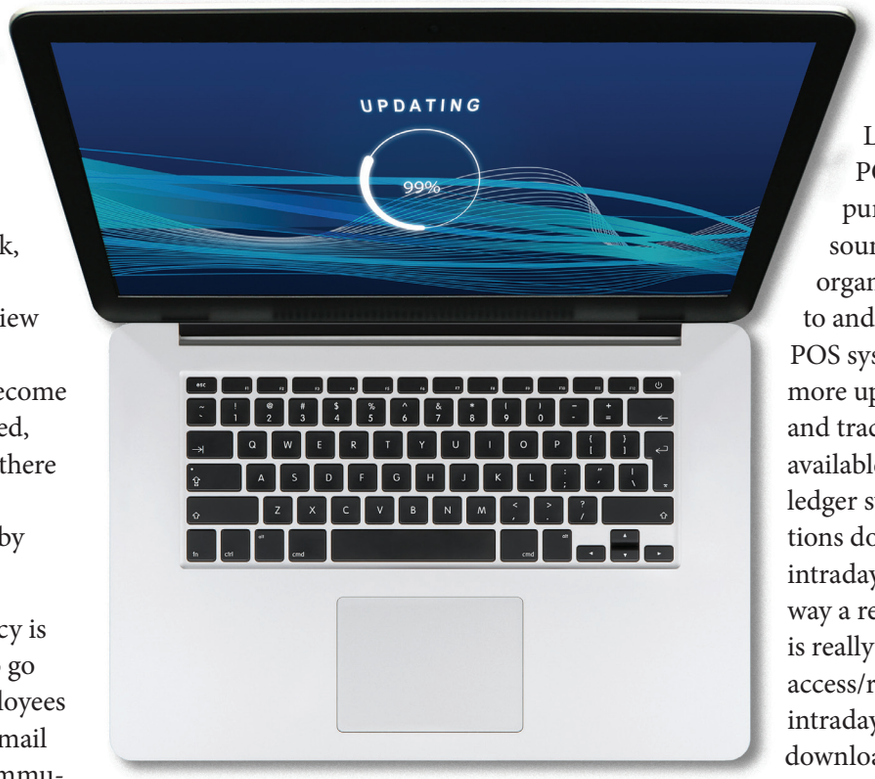
Most IT and privacy experts agree that encryption is the simplest and often most cost-effective way to mitigate privacy exposure. Privacy regulations may call for significant fines and penalties against certain organizations, sometimes in the hundreds of thousands or even millions of dollars. But if the data that a criminal seizes is encrypted, it is useless to the criminal, and regulations often take this into consideration. There may not even be a requirement to notify affected persons. While many organizations utilize encryption on some data, old records are sometimes taken off a server and moved to an external drive, but not encrypted. Implementation of encryption is not generally very difficult; it is actually built into some applications to help with privacy law compliance. Data should be encrypted while at rest, as well as while in transit.

In an ideal world, everything should be encrypted, but that isn't always possible due to system/application constraints. Some organizations use various systems, hosted both internally and by a third-party, in order to run their operations. Encryption may be accepted by some, but not all systems, or a certain type of encryption may not agree with some programs. That's a business challenge that will likely not be resolved anytime soon, but the closer one can get to the ideal of 100% encryption, the safer an organization will be.

Keeping applications and patches current can prevent as much as 85% of system intrusions.

Your employees are your front line of defense against cyber attacks. You can't read every incoming e-mail for them. Mail scanning applications are constantly improving, but the hackers are always a step or two ahead—at least the good ones are. Thus, the best-designed security system in the world is useless if someone on the inside opens the door and lets people walk in.

The best thing you can do to assist your employees in defending the network is to implement a training program to give them the tools to do so. Once established, completion should be mandatory for all current employees, and should be part of the onboarding process for new employees. Annual reminders, updates or refresher courses are also a good idea. Part of the presentation can be a review of



established corporate IT policies and procedures designed to safeguard the network, but actual training and examples on how to review e-mails is high impact. Spoofed e-mails have become increasingly sophisticated, but with careful review there are often clues that can be spotted pretty easily by an informed employee.

A corporate e-mail policy is essential, but it needs to go beyond just telling employees not to use their work e-mail address for personal communications. That is a sound policy, but they need to apply what they learn in the e-mail spoofing training with corporate communications as well. What better way to get employees' attention than to spoof an e-mail that looks like it is coming from ADP, a payor, etc.—organizations from which they undoubtedly get legitimate e-mails. Employees should be taught that if there is the slightest doubt, they should not click on any link in the e-mail nor open any attachment. Have IT check it out. All it takes is one click on the wrong e-mail and malware can be on its way in the door.

The easiest way to stave off spear phishing attacks is to have pre-established protocols. Procedures like multiple- party sign-off, requiring specific language or authorization codes from an executive when funds are to be disbursed, or requiring actual verbal or face-to-face confirmation can prevent diversion of corporate assets to criminals. Having a clear set of guidelines governing who can access and request sensitive data can have the same effect. You don't want to create a bottleneck, but the more people who are involved, or at least aware of a request for money or sensitive information, the greater the likelihood of foiling a scam.

The most widely-publicized breaches have been at retail establishments such as Target, TJ Maxx, Home Depot and so on, but lessons can certainly be learned and are transferable to other sectors. We have learned repeatedly that when an organization has multiple locations, it is not a great idea to aggregate all point-of-sale ("POS") operations. A separate system for each location reduces the amount of data potentially available to a criminal. If you have six locations with six separate data troves, the hacker will have to get into six different networks in order to get the same amount of data they would get from a single aggregated source.

Limit access to the POS system to sales purposes only. This may sound odd, but many organizations allow access to and reporting from their POS system in order to allow more up-to-the-minute data and tracking than would be available from their general ledger system. Most organizations don't need to review intraday transactions the way a retailer might, so there is really no reason to allow access/reporting on an intraday basis. A nightly download to the general ledger ought to yield adequate information with only a minimal delay. It was sloppy access to the POS system that led to the Target breach. Keep it locked down. Actively monitoring updates and patches will not only help prevent a breach, as we have discussed previously, but it is also a requirement in order to remain Payment Card Industry ("PCI") compliant. If you are out of compliance and a breach occurs, it can result in significant fines and penalties assessed by PCI. It can also result in additional expenses to regain PCI-compliant status and place additional burdens on the organization going forward.

John Whall is senior vice president of Hudson Insurance Group and leads the underwriting group tasked with insuring clients against cyber liability and other errors and omissions exposures.

Dashcam Video Retention — What's Your Policy?

Pat Lennon
Senior Loss Control Representative
Napa River Insurance Services
317.810.0062
plennon@napariverinsurance.com

Of all the technologies that have emerged in the trucking industry, perhaps the most significant is the use of dashboard cameras. Only a few years ago, it was rare to have video evidence of a crash. Now, as more fleets continue to add dashcams, the likelihood of getting such evidence is higher than ever.

A commonly cited statistic in car-truck crashes states that car drivers are at fault around 80% of the time.[1] But, as most anyone involved in trucking or truck insurance can confirm, before the use of dashcams, truckers were held responsible far more than 20% of the time; some say it's more like 50% to 75%. Now that is all changing. It's no longer a matter of both parties simply claiming the other was at fault; there is now video proof of what happened.

What's more, many systems allow the videos to be viewed by the officers at the scene. Longtime users of dashcams can share many success stories, such as when police tell the other party involved, "I just saw video of the crash. Would you like to revise your version of what happened?" Some have told of crashes where the mere presence of cameras has led the other parties to admit fault.

Fleet owners and safety professionals routinely claim that dashcam systems pay for themselves, often many times over. Not only do they provide exonerating evidence when not at fault and/or show the identity of hit-and-run vehicles, they also influence driver behavior, since they know the incident has been recorded.

Most also believe it's better to have video footage even in cases where their driver was at fault, a common concern that is heard about dashcams. They agree it's better to know the facts up front in such cases so that efforts can be directed at settling the claim rather than the costly, and often lengthy, process of investigating crashes. And, as noted previously, without dashcams, the odds were that the trucker was going to pay regardless of fault. Thus, having video footage also results in claimants being paid much sooner.

Once the decision has been made to add dashcams, there are other key steps that need to be taken. Policies need to be established on what to do with the videos that are recorded. First and foremost, there must be set procedures to follow when videos show drivers not following company policies. These can include acts of unsafe driving, not wearing seatbelts, having unauthorized passengers or using handheld cell phones. If a driver has a serious crash, you can expect the plaintiff's lawyer to demand access to those prior videos, to which they are likely entitled. It's essential that those prior incidents recorded result in appropriate actions, such as remedial training, counseling or formal reprimands, all of which MUST be documented.

It's no longer a matter of both parties simply claiming the other was at fault; there is now video proof of what happened.

Another process that should be established is a video retention policy, since it's not practical to plan on saving every video indefinitely. Instead, decisions should be made on which to save, how to save them and for how long. (Due to the possible legal consequences of such decisions, it is advisable to have an attorney with experience in such matters consult on a retention policy.) Of course, videos showing serious events, such as crashes, will need to be kept. Things get more complicated, though, when deciding whether or how long to keep other, more routine events.

The solution is to have a written video retention policy. This eliminates the need to make such decisions on a case-by-case basis. It also provides a measure of protection in the event a video is not saved, due to the company's policy, and that decision is later questioned. For example, you may no longer have prior recordings involving the aforementioned driver involved in a serious crash. Having a written retention policy can help prevent a spoliation of evidence accusation in such cases.

Customers of Napa River Insurance Services, Inc. are eligible to receive, at no charge, a generic video retention policy that has been prepared by a law firm that concentrates in trucking.[2] The policy can be customized to show the name of the motor carrier using it, although it is recommended that you have your attorney review it before you implement the policy. Feel free to contact your Napa River Loss Control Specialist if you are interested in taking advantage of this value-added service.

[1] *James Jaillet, Commercial Carrier Journal, February 14, 2013.*

[2] *Scopelitis, Garvin, Light, Hanson & Feary, P.C.*

Planning Today for Tomorrow's Catastrophic Accident

Michael H. Bassett
Senior Partner
The Bassett Firm

Whether you are a trucking company with 2 power units or 600 tractor-trailers, chances are, if you are in business long enough, one of your drivers will be involved in a catastrophic accident. When that happens, you need to already have in place a plan setting forth how you will respond.

After 30 years of representing trucking companies, I have narrowed it down to eight things that you need to gather within hours after being notified of the catastrophic accident:

1. Driver's Logs and Supporting Documents. With the advent of electronic logs, this is easier than ever.

2. Repair Records. Plaintiff's attorneys love to be able to tell juries that a trucking company put deficient equipment out on the road. Don't be one of those companies!

3. Maintenance Records. Again, Plaintiff's attorneys salivate at the opportunity to portray your trucking company as one who does not properly maintain its equipment and, as a result, endangers others.

4. Bills of Lading. We need to know where the driver was coming from, where he or she was going, and what he or she was carrying.

5. All Electronic Data. There are dozens of separate computers on the average late-model Class 8 tractor. All of them contain valuable data. Get it while it's hot. And don't forget any positioning data and dash cam videos.

6. DQ File. Because having a qualified driver on the road is pretty darn important.

7. Personnel File. Every document you have on that driver needs to be secured immediately.

8. Safety and Training Documents. Because if you cannot document the safety training you gave your driver, if it's not in writing, if it's not dated, and if it's not signed, IT NEVER HAPPENED.

Eight boxes to check. Do it right and do it quickly, and you will save yourself headaches down the road. Failing to plan today for tomorrow's accident? Well that's just catastrophic.

Jeff Davis Presented with PTDI's Crittenden Memorial Award

On March, 27, 2018, the Professional Truck Driver Institute, Inc. (PTDI) presented its highest honor, the Lee J. Crittenden Memorial Award, to Jeff Davis, Vice President of Safety at Napa River. The award ceremony took place during the 80th Annual Convention of the Truckload Carriers Association (TCA).

Jeff has been involved in commercial trucking safety within the insurance industry since 1983. In his current role at Napa River, he oversees all safety and loss prevention activities with prospective and insured clients. His role includes managing the pre-underwriting due diligence process, providing insured client safety and compliance services, as well as analyzing loss and compliance data.

The Napa River team proudly congratulates Jeff on his momentous achievement!

NAPA RIVER
INSURANCE SERVICES®

The information contained in this publication is provided for informational purposes only and is not provided as a substitute for advice from legal counsel regarding the content or interpretation of any law, regulation or rule. The information provided shall not revise, supplement or alter an insurance policy in any manner, nor is it intended as a substitute for advice from a risk management expert or legal counsel you may retain for your own purposes.

www.napariverinsurance.com