



Safety Shorts

General Safety, Highway, & Law Enforcement

February 2024

Volume 12, Number 2

Cyber Security Keypoints from the County Network Security Cooperative

The County Network Security Cooperative released a [quick-read flyer](#) in January on the cyber security topic of phishing. A different flyer will be distributed each month throughout 2024 to provide basic information and reminders intended to keep county officials and employees cyber risk aware.

These flyers are perfect for printing/posting anywhere employees gather, such as bulletin board or on a refrigerator in a break room area.

Remember, today's safety-oriented workplace includes cyber security, as online security compromises and breaches can be both costly and burdensome.

NIRMA is dedicated to providing members with a variety of resources like this monthly flyer campaign from the Cooperative, the NIRMA Cyber Security Toolkit, and more to help avoid and mitigate potential cyber claims.

HIGHWAY DEPARTMENT

By K C Pawling, Road Safety and Loss Prevention Specialist

Stressed and Exhausted?

These last few weeks have been a challenge for many of the State's counties and municipality road and street crews. I know that I do not have to tell many of you this, because you are living it. My oldest son is a new employee of a municipality in the northeast part of the state. He recently told me he put in 81 ½ hours in a single week pushing snow.

It's been a few years since I was involved with moving snow for that many hours in one week, but that statement took me right back to that time in my life. It is amazing how just a simple statement like that can make someone recall a specific time in their life, even to the point of being almost able to physically feel how I did at that time.

While road departments don't necessarily have any production quotas or deadlines to meet, you do have the stress of getting all your roads open to the motoring public in a timely manner. The expectations for snow removal can be quite different from one county to another. But I can confidently say that most counties are expected to have the roads opened sooner than later. The press of this demand and the extra hours on the job can combine to create a lot of mental stress.

Stress can come from citizens' phone calls to the highway department office asking when roads will be opened. These usually result in the management team gently pushing the operators. The stress could come from not having the correct blend of fuel in the tanks at the optimal time, leading to the problem of gelled-up machines. Maybe, it's the stress of failing to have on hand the blades or bits you need for all your plows. Or my favorite stress that few people understand until they spend time in a plow for hours, days, and even weeks. It's just a special kind of stress... banging a machine into a snowbank for sometimes hours on end, just to get to the other side of it. Then you might have the opportunity to spend more quality time with the same drift again tomorrow.

The factors listed above create mental stress, but the mental can contribute to physical stress. Physical stress comes from pushing ourselves to the point of exhaustion, whether we are aware of it or not. The exhaustion then leads to slips, trips and falls, muscle sprains or strains and probably poor choices.

Poor choices could include not putting guards back on the machines like they should be. Maybe not picking up our tools and putting them away, causing trip hazards. Failing to put out the appropriate signage required for our road maintenance activities. Another poor decision can be getting a little short or snarky with our fellow shop mate thus resulting in the loss of someone to help us lift our heavy blades for replacement on our machine or any other type of shop cooperation needed.

I understand everyone reading this is likely quite aware of all the stress that can come with snow removal, but what I am asking of you is to yield to it. If it's possible, make some scheduling changes to give employees a little relief. Practice a little teamwork, understand that the whole crew is being challenged. Take a minute before doing something and ask yourself if it is the safest way to get the task accomplished. Give your co-workers a little grace instead of responding with additional snarky comments. Take the time and lend a helping hand. Don't contribute to the vicious circle of stress induced exhaustion.

If you have any questions, comments, or concerns that we can help you with don't hesitate to contact any of us here at NIRMA. I can be reached at kcpawling@nirma.info or 402-310-4417, text or call.

GENERAL SAFETY

By Chad Engle, Loss Prevention and Safety Manager

Safety Committee Responsibilities and Duties – Training

The third responsibility and duty of a safety committee, per NIRMA's *Safety Committee Resource Handbook*, is training. The safety committee is not necessarily responsible for providing the actual training, but the committee is tasked with developing a training schedule and topics and presenting this to management. Generally, the safety committee works on a county or agency-wide training schedule and then presents it to the board for approval. Some NIRMA members have a distinct safety committee for a specific type of county operations, such as a highway department or sheriff's office. Those committees would simply present the training schedule to whomever directs their department.

Topics for training should be easy to identify using your quarterly incident report. This report outlines the losses your county or agency has incurred in the three months prior. After investigating why and how those incidents occurred, tailor your training to address these causes. If you are fortunate enough to not have experienced any losses in the recent past, I would recommend you focus your training on preventing car crashes, slip/trip and fall and sprains/strains. These three causes of loss are consistently the most common among NIRMA members. You cannot go wrong focusing on these causes.

There are many options for loss prevention and safety training. NIRMA offers in-person training provided by any of our loss prevention and safety specialists. In addition, NIRMA offers online training resources via our Online University, the Energized Approach, as well as Streaming Videos on Demand. All these options can be found by clicking on Training under the Resources tab at www.nirma.info. Consider reaching out to local subject matter experts as well. Local fire departments and utility companies offer training as well. NIRMA members are also eligible for membership in the Nebraska Safety Council at no cost.

Our training calendars are filling up quickly. If you are planning to utilize NIRMA for in-person training, I recommend that you reach out sooner rather than later. As always, I can be reached at: chad@nirma.info or 1.800.642.6671.

Money For Minutes Winners!

Recognizing and rewarding member county and agency safety committees for their loss prevention efforts is one of the most enjoyable parts of my job. To qualify for this year's **Money for Minutes** program, member safety committees had to do the following:

1. **Conduct at least one safety committee meeting per quarter during the calendar year.**
2. **Investigate and discuss all incidents, events, injuries, and accidents and make recommendations about how to prevent recurrence of similar incidents.**
3. **Submit minutes from each meeting, containing recommendations, to NIRMA for review.**

All member safety committees that met the requirements outlined above were eligible to win one of ten \$500.00 awards. NIRMA intends for these awards to be used by the winning member to further their loss prevention and safety efforts.

Congratulations to the following safety committees. You are 2023's **Money for Minutes** award winners!

Box Butte County Roads
Dodge County Roads
Howard County
Morrill County
Sherman County Roads

Cheyenne County
Hall County
Merrick County
Saline County
Thayer County

Thank you for your loss prevention and safety efforts to protect your employees from injury and your county from liability. Your hard work does not go unnoticed.

Budget permitting, the Money for Minutes program will continue into 2024. Remember that if you miss your first quarterly meeting you are out of luck, so get that meeting on the calendar and remember to submit your meetings to NIRMA at chad@nirma.info. Please reach out if you have any questions. Our loss prevention team is always looking to help.

LAW ENFORCEMENT AND CORRECTIONS

By Todd Duncan, Law Enforcement and Safety Specialist

Cybersecurity

On January 31, 2024, FBI Director Christopher Wray issued a [warning](#) regarding the growing threat of cyberattacks stating that foreign hackers aim to “wreak havoc” on U.S. critical infrastructure. Considering this and other similar warnings issued by the FBI in the last few months, this month’s Safety Short will focus on the importance of effective cybersecurity policies and practices within county government.

Government IT infrastructure faces a myriad of cyber threats, ranging from sophisticated state-sponsored attacks to opportunistic cybercriminal activity. These threats pose significant risks to national security, public safety, and the integrity of government operations. To mitigate these risks, robust cybersecurity measures and strategies are essential.

Threat Landscape:

- **State-Sponsored Attacks:** Nation-states engage in cyber espionage, sabotage, and warfare to steal sensitive information, disrupt critical services, or undermine government operations.
- **Cyber Espionage:** Adversaries target government networks to steal classified information, intellectual property, and sensitive data for political, economic, or military gain.
- **Ransomware:** County agencies are prime targets for ransomware attacks, where malicious actors encrypt critical data and demand ransom payments, causing operational disruptions and financial losses.
- **Insider Threats:** Malicious insiders or unwitting employees may compromise county government systems through negligence, malicious intent, or social engineering tactics.
- **Supply Chain Vulnerabilities:** Dependencies on third-party vendors and contractors introduce vulnerabilities, allowing attackers to exploit weaknesses in the supply chain to infiltrate government networks.

Recommendations for Protection:

- **Implement Robust Cyber Hygiene:** Implement a countywide cybersecurity policy, enforce strong password policies, regularly update software and systems, and conduct security awareness training to mitigate common attack methods like phishing and social engineering.
- **Deploy Multi-Layered Defense:** Employ a combination of firewalls, intrusion detection systems, endpoint protection, and encryption to safeguard county networks from unauthorized access and malware.
- **Adopt Zero Trust Architecture:** Restrict access to sensitive data and critical systems based on user identity, device posture, and contextual factors, reducing the risk of lateral movement by attackers.
- **Enhance Incident Response Capabilities:** Develop and regularly test incident response plans to detect, contain, and mitigate cyber incidents promptly, minimizing the impact on government operations and restoring services effectively.

- Strengthen Collaboration and Information Sharing: Foster partnerships between county government, law enforcement, intelligence communities such as the [Nebraska Information and Analysis Center](#) (NIAC), and private sector organizations to share threat intelligence, best practices, and resources for collective defense against cyber threats.
- Regulate and Monitor Third-Party Relationships: Implement stringent security requirements for vendors and contractors, conduct regular assessments of third-party security posture, and monitor supply chain activities to detect and mitigate potential risks.

In conclusion, safeguarding county IT infrastructure against cyber-attacks requires a comprehensive and proactive approach, combining sound cybersecurity measures, effective risk management strategies, and close collaboration among stakeholders. By prioritizing cybersecurity, county agencies can better protect critical assets, reduce risk, and preserve public trust in an increasingly digital and interconnected world.

Additional Resources:

- [NIRMA Website](#) (Member Login -> Interact)
 - NIRMA Cyber Security Toolkit
 - NIRMA eRisk Hub
 - Cybersecurity information and training
 - Model cybersecurity policies
 - Cybersecurity incident response plan template
 - Breach response guidance
 - [Nebraska State Patrol Cyber Unit](#)
 - [Cybersecurity & Infrastructure Security Agency \(CISA\)](#)