DMI
DISTRICTS MUTUAL INSURANCE
& RISK MANAGEMENT SERVICES
| Collaborators in Risk Management |

VOLUME 18 • ISSUE 4 • OCTOBER 2022

THE Incident REPORT

a publication of Districts Mutual Insurance and Risk Management Services
Collaborators in Risk Management

212 West Pinehurst Trail | Dakota Dunes, SD 57049 | DistrictsMutualInsurance.com | 605.422.2655

The "Hottest" Topic

Steven Stoeger-Moore, President

The commercial insurance marketplace remains quite challenging. The property/casualty (P/C) insurance rates for Q3 (July, August, September) indicated an average increase of 5.3%. The cyber liability market posted a 23% increase in rates. Overall, the Q3 results marked the continuation of moderate rate increases across all lines of coverage except for cyber liability. Cyber liability remains the "hottest" P/C market. There are several factors that are at work

- Severity remains an issue due to the increase in ransomware.
- The industry's loss ratio, while improved, needs to continue the downward trajectory.
- Markets are selective with restrictive underwriting requirements.

DMI clearly recognized the impact of the cyber liability marketplace on the Colleges. The most recognizable impact has been premium increases.

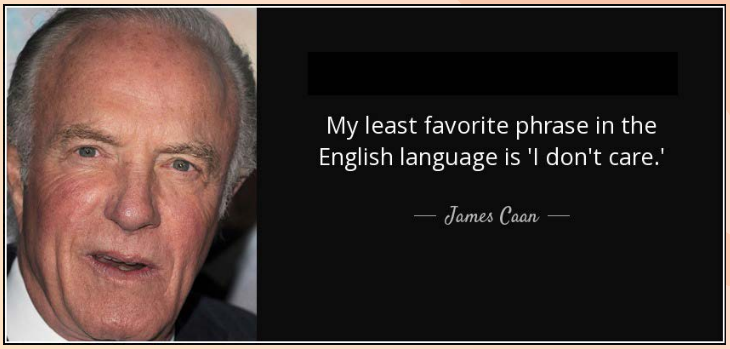
Over the last two years, DMI has dedicated the Risk Management Project Award funding to the improvement of cyber health and data protection. DMI has distributed $1.3M for college initiatives that focus on these two topics. Due to the Colleges' concerted efforts, the 07/01/22 cyber renewal retained the expiring terms and conditions (coverage limits, deductibles, sub-limits). The DMI 07/01/22 renewal, retaining the expiring terms and conditions ***was not*** the norm in higher education. Many institutions experienced significant increases in deductibles, lower coverage limits, loss of sub-limits, co-insurance, or other unfavorable terms. The Colleges' focused efforts led to a more favorable renewal result.

Looking ahead, the 07/01/23 renewal will continue with the selective underwriting that has occurred over the past several years. An application along with a supplemental questionnaire is expected. At this juncture, in the Policy Year, the College's should continue to address the "Baseline Underwriting Requirements". To read more on these requirements, Click Here

Baseline Underwriting Requirements – Cyber

If you have any questions, please feel free to reach out to this office.

Steven


My least favorite phrase in the English language is 'I don't care.'

— James Caan —

DMI Presents... Topical Snapshots

"Crime Prevention Through Environmental Design"

To view the video click here.

presented by Brooke Bahr, *DMI* Security Consultant

This month's DMI Presents...Topical Snapshots is a first from Brooke Bahr, DMI's Security Consultant. Check out her risk-mitigating feature, "Crime Prevention Through Environmental Design".

eRiskHub®

The 2022 NetDiligence Cyber Claim Study is available and NOW featured in the eRiskHub®. Just log into the eRiskHub® portal from DMI's website or through your personal account and look under Featured Articles in the Learning Center.

In honor of Cybersecurity Awareness month, NetDiligence announced adding new cybersecurity training videos to help keep you "in the know". Check the site regularly for new resources that are being added as they become available.

Empower Supervisors as Safety Leaders

Written by Willie Henning, DMI EHS Consultant

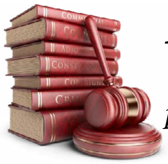
Building a strong safety culture requires active engagement from all levels of the organization. However, direct supervisors have a significant role in affecting daily safe work habits. For the colleges to be successful in safety, it is critical to empower supervisors as safety leaders. Therefore, to set supervisors up for success, provide them with strategies that enhance safety activities.

Ensure supervisors completely understand the safety mission and goals at the college and encourage them to discuss these with their teams. One option is to work with managers to include safety language in a supervisor's annual performance review, as well as in the supervisor's goals and objectives. Another important factor is to verify supervisors have been trained in all required safety training. If there is training for frontline workers, include their supervisors on the invitation list. When supervisors attend training, it shows everyone that ***safety is important***.

Take time to help supervisors become familiar with safety hazards found in their individual workplaces. When supervisors are knowledgeable of workplace hazards and how to mitigate the associated risk of these hazards, they become more confident in discussing employee safety with their teams. Promote meaningful safety conversations by providing fundamental safety knowledge and encourage supervisors to include these conversations in meetings and daily discussions.

Include supervisors in incident investigation activities to help highlight root causes and continuous improvement action items. By being part of the solution, supervisors are vital stakeholders in the implementation and monitoring of a safe workplace. Also, listening to supervisors' observations and suggestions gives them ownership of corrective actions.

Developing frontline supervisors into safety advocates sets the tone for moving toward a stronger safety culture throughout the college. Empowered, well-equipped, caring, and honest safety leaders help create a culture that fosters, accepts, and supports each employee's safety decisions.



Best Legal Report

presented by Michael Best

SEPTEMBER 26, 2022 | PRESS RELEASE

Seventh Circuit Decision Affirms Walmart's Win in Pregnancy Bias Lawsuit

Click here to read entire Press Release...

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
CYBERSECURITY AWARENESS MONTH 2022
SEE YOURSELF IN CYBER

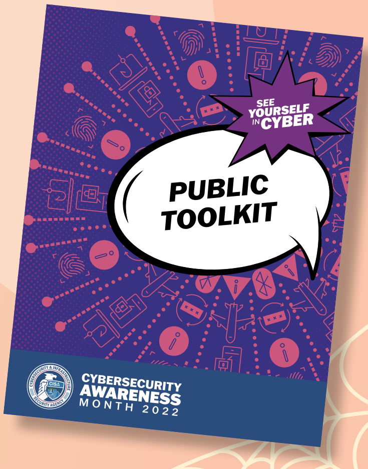
The Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) lead a collaborative effort between government and industry to raise cybersecurity awareness nationally and internationally. While CISA works to increase cybersecurity throughout the government, its regions, and critical infrastructure sectors, NCA works with corporations and the general public to raise awareness of action steps we can take to advance digital security.

This year's campaign theme — **"See Yourself in Cyber"** — demonstrates that everyone is responsible for their own online behavior. This year's focus is on the "people" part of cybersecurity, providing information and resources to help educate CISA partners and the public, and to ensure all individuals and organizations make smart decisions whether on the job, at home, or at school both now and in the future. Throughout October, CISA and NCA will highlight key action steps that everyone should take

- Enable Multi-Factor Authentication
- Use a Strong Password
- Recognize and Report Phishing
- Update Your Software

CISA/NCA's campaign shares ways to increase resilience against cyber attacks, provide easy-to-use tools to lock down private data, and keep assets secure from criminals, terrorists, and foreign entities. Check out their Cybersecurity Public Toolkit for tips and recommendations to keep yourself and the Colleges protected.

Resources: Cybersecurity Public Toolkit



The Technical Colleges are encouraged to engage in this year's efforts through cybersecurity awareness campaigns and by sharing this message. If you would like to partner with CISA/NCA in their campaign, contact Brooke Bahr or Suzette Harrell for partnership resource links to sample emails, talking points, social media announcements, presentations and templates, logos and graphics, and so much more.