--- SOURCE TEXT ---

NORTH DAKOTA’S BIG

CYBERSECURITY VISION

*By Shawn Riley*

The people of North Dakota have a lot to be proud of. Our state is a leader in agriculture, energy and national defense. We’re believers in humility and modesty—strong Midwestern values that define how we go about our day at work, home and school.

But there is one thing we feel so proud of that we hope you’ll forgive us if we are uncharacteristically boastful:

We intend to be the most connected state in America.

Yes, in a country with such acknowledged technology-oriented states as California, New York, Texas and Massachusetts, we are positioning North Dakota to be a pioneer in the digital transformation of government, education, business, workforce and society. We are also planning to make cybersecurity the lingua franca of a digital North Dakota.

These goals seem lofty – maybe even a stretch – for a state that has the second smallest population in the United States, is the most rural in the nation, and has an annual budget that would be little more than a rounding error compared to California or New York.

But you don’t need to be a colossus to be a leader. You do, however, need to be smart, resourceful, innovative and deeply dedicated to excellence in strategy, execution and communication.

From the halls of the state capitol to every classroom, we’re prioritizing cybersecurity as a state in order to protect our critical systems, safeguard the data of our citizens, train our next generation to succeed, and create the digital workforce of the 21st century.

**Every Student Cyber Educated**

To get to where we want to be, we’re focused on comprehensive education in computer science. Our state’s K-20W initiative is key to bringing together 40 different public- and private-sector entities to empower North Dakota’s workforce, educators and students from kindergarten through PhD. That’s why K-20W’s mantra is: “Every student, every school, cyber-educated.”

We’re establishing an overarching goal of training 700 teachers across the state on both computer science and cybersecurity, giving us at least one cyber-trained teacher for every 160 public school students. Every student graduating school today is entering a digital society. Regardless of career path, nearly every job in the 21st century uses computer technology. It’s time that every student learns the essential tools, as well as the risks and rewards.

Cyber education isn’t just about unleashing the potential of machine learning and Internet of Things, it’s also about driving cybersecurity awareness and action on all levels, attracting and retaining businesses to fuel economic growth. This is why we’re giving parents, students, teachers and educational institutions the tools that they need to put cybersecurity front and center.

**Whole of Government Cyber Defense**

We formed a cybersecurity framework across the entire state—unifying what had once been a patchwork of silos. We embraced the concept of “whole of government” cyber defense, spanning all seven branches of public sector entities across the state: executive, legislative, judicial, higher education, K-12 education, cities and counties, helping to elevate our collective security posture for 252,000 statewide network users.

We wanted to avoid the inefficiency and inevitable gaps created by implementing cybersecurity at only opportunistic, transactional levels by departments and entities. By committing ourselves to covering every aspect of North Dakota’s public sector, we will become operationally more secure and make cybersecurity second nature to everything we do.

**A Proactive Mindset Toward Security**

To embark on our statewide security transformation, we had to avoid the death trap of simply chasing every cybersecurity fire. We needed to shed the mindset of reacting to each breach, each zero-day attack, each ransomware and DDoS attack and treating them as one-off problems.

Instead, we needed to get out in front with a proactive plan to utilize technology, people and process as part of an active defense mindset. Techniques like threat hunting, network behavior analysis and other steps have allowed us to funnel out the noise to go far beyond reacting to known threats, and instead catch attacks before they happen. Core elements of

**Zero Trust:** We committed to the Zero Trust model of cybersecurity defense from the very start; in fact, we’ve employed Zero Trust for more than 70% of our data centers. It’s a big workload, but well worth it. The way in which we utilize the Zero Trust model requires us to have a clear understanding of our resources and how they communicate with one another. By mapping the communication vectors prior to the development and implementation of the corresponding rulesets, we ask a crucial question: Should this resource be accessible and if so, by who or what? Couple that with the identity verification of every user trying to access the resource, we are truly limiting the exposure, and threat landscape, of the resource.

**IoT security:** Having a big military and defense footprint in the state, as well as massive agricultural and energy sectors, means that North Dakota was an early adopter of the IoT. Think about the use of drone radar systems for Homeland Defense and other military applications, and the future need for a billion sensors to cover our farmlands and environmental ecosystems. You can’t do the “farm of the future” without IoT, and you can’t do IoT without a specific plan to secure sensors, chip sets and other connected things.

**Cloud-first strategy:** Obviously, it’s not just small states like North Dakota that need the agility, flexibility and cost efficiency of the cloud. Every state, and every commercial entity, should move toward a cloud-first paradigm to encourage a nimbler approach to security.

**Lead by Action, and Courage**

Leadership requires many qualities, including courage, open communication, and creativity. Whether it’s embracing new technologies or prioritizing cybersecurity, our approach has been: Why not? Or how can we do this? In fact, our new information technology vision is in the form of a question: How might we deliver world-class technology and services to our state?

**We’ve done a lot so far, including:**

• The state’s Department of Public Instruction has teamed with state and industry experts to draft integrated computer science and cybersecurity standards—making us the first state in the nation to emphasize cybersecurity in such an integral manner – and we did it in just 11 months.

• We passed comprehensive legislation that allows for strategic cyber defense for every governmental entity across the state.

• North Dakota State University and Bismarck State College have been designated as Centers of Academic Excellence in Cyber Defense by the National Security Agency and the Department of Homeland Security.

• Our partnerships with local entrepreneurs and national organizations like code.org, NICERC and NCWIT are yielding tangible benefits in terms of classroom resources, coding camps and professional development.

• In our first year of participating in the SANS Institute “Girls Go CyberStart” and “College FastTrack,” we achieved the highest per-capita participation of all states taking part in the programs.

And we plan to do more, like hosting legislative technology showcases, partnering with private-sector cybersecurity leaders such as Palo Alto Networks, and promoting opportunities in computer science for women and girls.

We’re incredible lucky that the North Dakota Governor Doug Burgum, Chancellor Mark Hagerott, and my CISO colleague Sean Wiese are likeminded in envisioning the digital future. Numerous other stakeholders, as well as North Dakota citizens, have done much to help build that future.

Which brings me to a personal anecdote. My 14-year-old daughter was looking over her class roster for the new school year, and I could tell she was a bit miffed (as only teenagers can be). She handed me a piece of paper and plaintively asked, “Where are my technology classes?”

Now, my daughter is not necessarily going to be a coder or a bug-hunter, but she certainly has experienced enough technology in her short life to know what has taken years for many of us to learn: You can’t have a digital society unless you start very early. And that means having a strategic plan for cybersecurity that doesn’t wait for you to graduate college or enter the workforce.