Governor Burgum’s State of the State Address
Takeaways (January 23, 2018)

The state of the State is one of unlimited promise and potential, provided we embrace change, diversify our economy and harness the unstoppable forces of technology.
THREE THEMES

1. Empower people
2. Improve lives
3. Inspire success

Governor Burgum’s State of the State
FIVE STRATEGIC INITIATIVES

1. Reinventing Government
2. Behavioral Health & Addiction
3. Tribal Engagement
4. Transforming Education
5. Main Street Initiative
You need to have the courage to understand that some of the things you hold true may actually not be true, be willing to let go of perceptions, and have the humility to understand that you can learn from anyone, with curiosity to drive forward with a set of questions.

Governor Burgum’s State of the State
Purpose for Initiative

• Promote a culture of safety and responsibility aligned with our core values and goals
  – Foster a welcoming, safe and inclusive campus climate
  – Community, Discovery, Diversity, Inclusivity, Liberal Arts, Lifelong Learning
• Strengthen safety due to increased reliance on information technology
  – Increased cybersecurity threats
• Recognize safety is an investment
• Recognize Safeguarding UND is a continuous process
• Recognize Safeguarding UND is everyone’s responsibility
Safeguarding UND

• Preventive Measures – Reduce the likelihood of a deliberate attack, deter an attack, introduce delays, reduce vulnerabilities, or otherwise deny the ability of the attack to be successful. (i.e., policies, lighting, public safety staff, endpoint security)

• Detective Measures – Distinguish between authorized and unauthorized personnel, help discover attacks, and trigger appropriate preventive or corrective measures. (i.e., electronic door access control, camera systems, alarm systems, Internet Watch Foundation, endpoint protection)

• Corrective Measures – Reduce the effects of an attack and restore the facility or infrastructure to normal operation. (i.e., communications systems, phishing awareness)
Preventive Measures

• Enterprise Risk Management
• SafeCampus smart phone application
• Updated Acceptable Use Policy
• Endpoint protection
  – software on all UND owned computers
• DUO multi-factor authentication for faculty and staff
• Distributed Denial of Service (DDoS) preventative software on und.edu server
• Cybersecurity education and training
Detective Measures

• Integrated Systems Platform
  – Electronic door access
  – Video surveillance
  – Building automation systems, i.e. alarm monitoring

• Internet Watch Foundation (IWF)
  – Block access to web sites with child sexual abuse material
  – Alert UND if illegal sites are hosted on UND servers
  – Unique image hashes available to integrate with software to search for child sexual abuse material on UND-owned devices (optional)

• Endpoint protection software
• Vulnerability assessment on servers
Corrective Measures

• Emergency Operations Plan
• Continuity of Operations Planning
• Information Security Incident Response Team (ISIRT)
• Functional Consolidation
• Phishing Awareness
  – Phishing Assessment **Nov 2016**
    • Phishing emails sent: 3405
    • Clicked: 86 – 2.5%
    • Submitted Creds: 27 - .8%
  – Phishing Assessment **May 2017**
    • Phishing emails sent: 5920
    • Clicked: 802 – 13.5%
    • Submitted Creds: 578 - 9.8%
Other Proposed Initiatives

- Phishing campaign
  - year long monthly campaign
- Cybersecurity education and training
  - Integrate real-time training for reinforcement
- BitTorrent
  - Protect from illegal activity such as copyright violations and sharing of child sexual abuse images
- Clean Slate
  - Identify possible vulnerabilities in UND owned computers
Other Proposed Initiatives

• UND secure wireless SSID
• DUO multifactor for students
• Encrypt devices
• Systems integration
  – Housing electronic door access
• Emergency Blue Light upgrades
• Continuity of Operations Planning
Let’s work together to promote a culture that supports a safe learning and working environment.

SAFEGUARDING UND IS EVERYONE’S RESPONSIBILITY!
BitTorrent

- 0.7% of all network traffic at UND comes from BitTorrent.
- 51% of total network traffic comes from Residence Halls. Of which, 1.3% of traffic is BitTorrent.
- Less than 20% of students live in Residential Halls.
- 67% of outbound BitTorrent traffic comes from Residence Halls. Of which, 30% is wireless and 70% wired.
- From 8/1/17 – 11/29/17, UND received 48 copyright violations in which the offender was using the BitTorrent protocol. CTS Information Security (SLA) spent 60.75 hours on these complaints, averaging more than 4 hours a week.
### Other research institutions blocking P2P/BitTorrent

<table>
<thead>
<tr>
<th>University of Tennessee Knoxville</th>
<th>Harvard Medical School</th>
</tr>
</thead>
<tbody>
<tr>
<td>Georgia College and University</td>
<td>University of Alabama - Tuscaloosa</td>
</tr>
<tr>
<td>University of Alabama - Birmingham</td>
<td>University of Missouri – St. Louis</td>
</tr>
<tr>
<td>Miami University, Ohio</td>
<td>University of North Florida</td>
</tr>
<tr>
<td>University of Tennessee Chattanooga</td>
<td>Western Illinois University</td>
</tr>
<tr>
<td>University of Oklahoma</td>
<td>UNC Pembroke</td>
</tr>
</tbody>
</table>