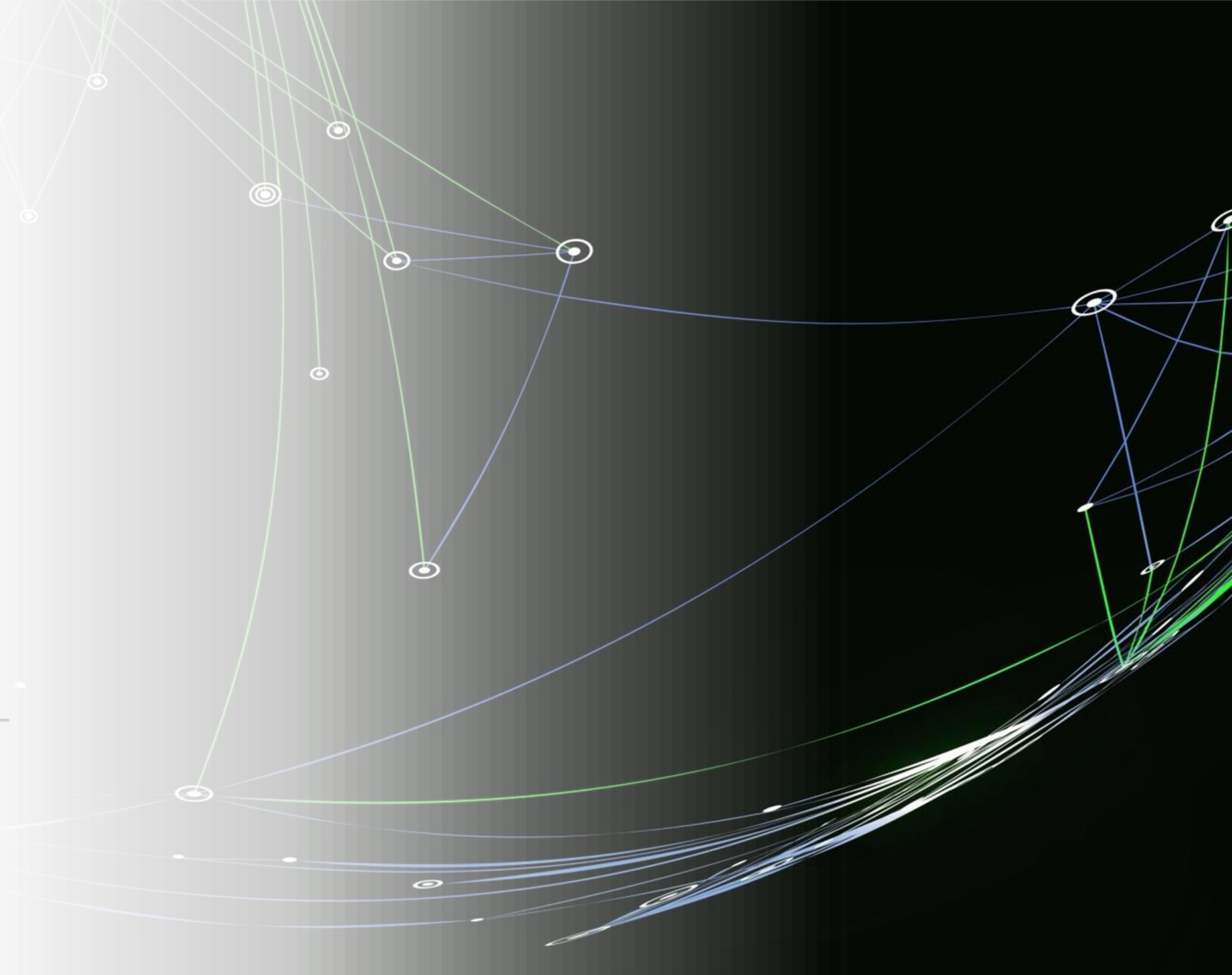
Cyber Threats to the Healthcare Ecosystem

HB333/SB691



Why Healthcare is a Target

Valuable Data: Healthcare organizations possess a wealth of sensitive data, which is highly valuable to cybercriminals and nation-state actors.

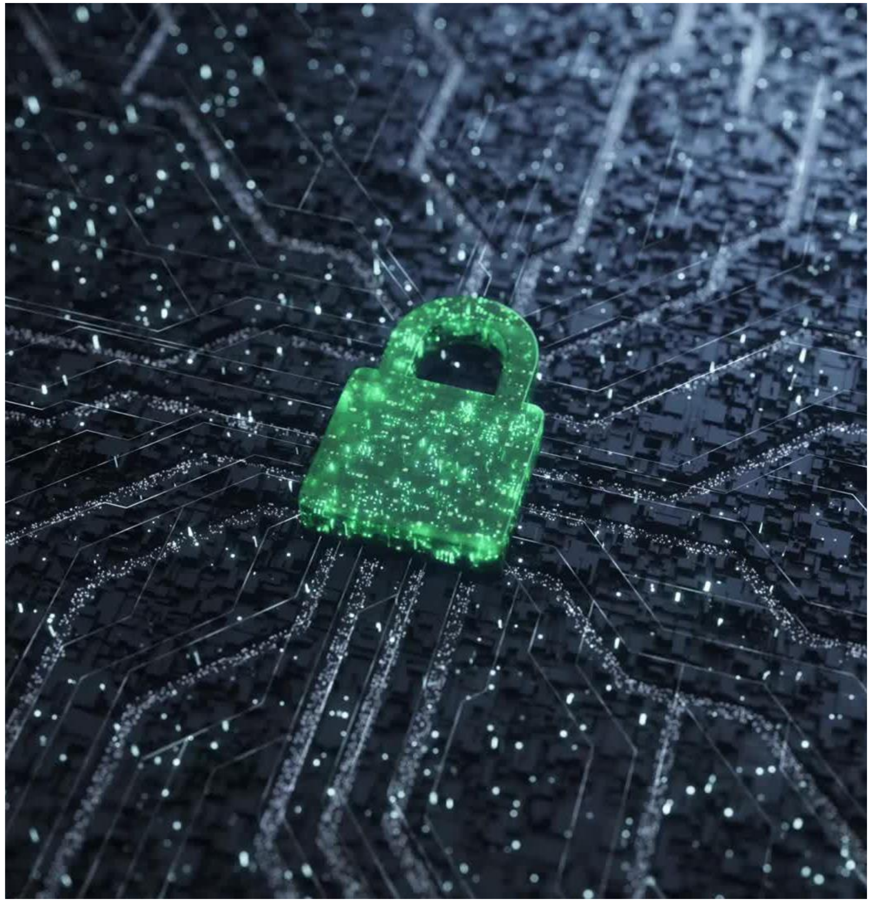
High Financial Rewards: Stolen records sell 10 times more than stolen credit card numbers on the dark web, with costs to remediate breaches also being significantly higher than in other industries.

Disruption Drives Immediacy: Disruptions to healthcare lead to proven negative impact on patient outcomes, meaning the pressure is high to pay ransoms to cybercriminals.

National Threat Landscape

- Health-related privacy breaches have gone up 256% over the past five years (OCR).
- Ransomware attacks on healthcare related organizations is up 264%. (OCR)
- ”Healthcare and Public Health” was the most affected critical infrastructure industry from ransomware attacks. (FBI Internet Crime Complaint Center)

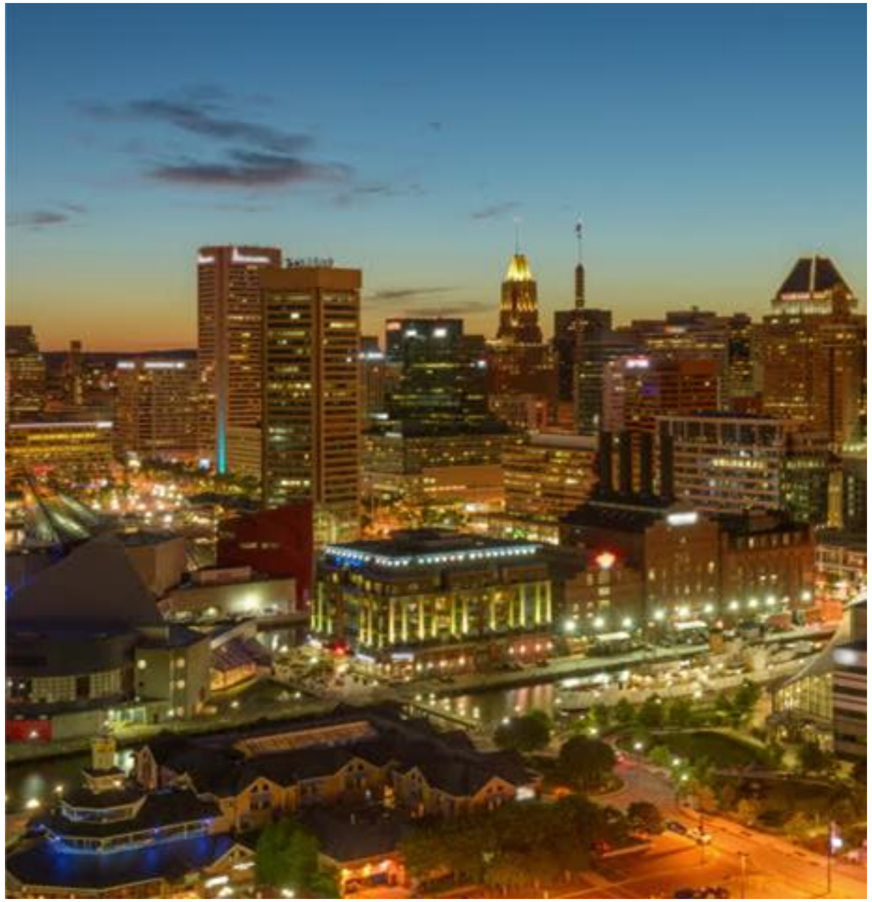
From Chris Hart (2024). Review of National and State-Level Data Relating to Cyber Incidents and Cybersecurity at Healthcare Organizations. Research supported by the Center for Health and Homeland Security at the University of Maryland, Baltimore.



Maryland Threat Landscape

- Since 2010, Maryland healthcare organizations have suffered 84 breaches categorized as “hacking/IT incidents” affecting more than 500 people. (OCR)
- In 2023, over 3.5 million people were impacted by hacking/IT incidents of Maryland organizations, a significant increase from previous years.
- According to a 2021 Maryland Healthcare Commission report, from 2018-2020 Maryland had the highest number of breaches per-capita among 7 states with similar per-capita hospital inpatient rates.

From Chris Hart (2024). Review of National and State-Level Data Relating to Cyber Incidents and Cybersecurity at Healthcare Organizations. Research supported by the Center for Health and Homeland Security at the University of Maryland, Baltimore.



Kinetic Impacts

- According to a 2024 Ponemon study:
  - **92%** of all hospitals experienced a cyber incident in 2023
  - Average cost of single most expensive attack was **$4.7 million**
  - Hospitals suffering a cyber incident lost an average of **$1.47 million** due to disruptions to normal healthcare operations

Financial Impacts

- According to a 2023 study, of the 68% of hospitals surveyed that experienced a ransomware attack:
  - 28% reported an increase in the mortality rate
  - 59% reported delays in procedures and tests have resulted in poor outcomes
  - 44% reported an increase in complications from medical procedures
  - 48% reported longer length of stay
  - 46% reported an increase in patients transferred or diverted to other facilities

Change Healthcare

Widespread Impact- Change Healthcare was attacked, impacting the entire U.S. healthcare system.

Critical Role- Processes billing and insurance for hospitals, pharmacies, and medical practices.

Massive Data Breach- 190 million patient records were compromised.

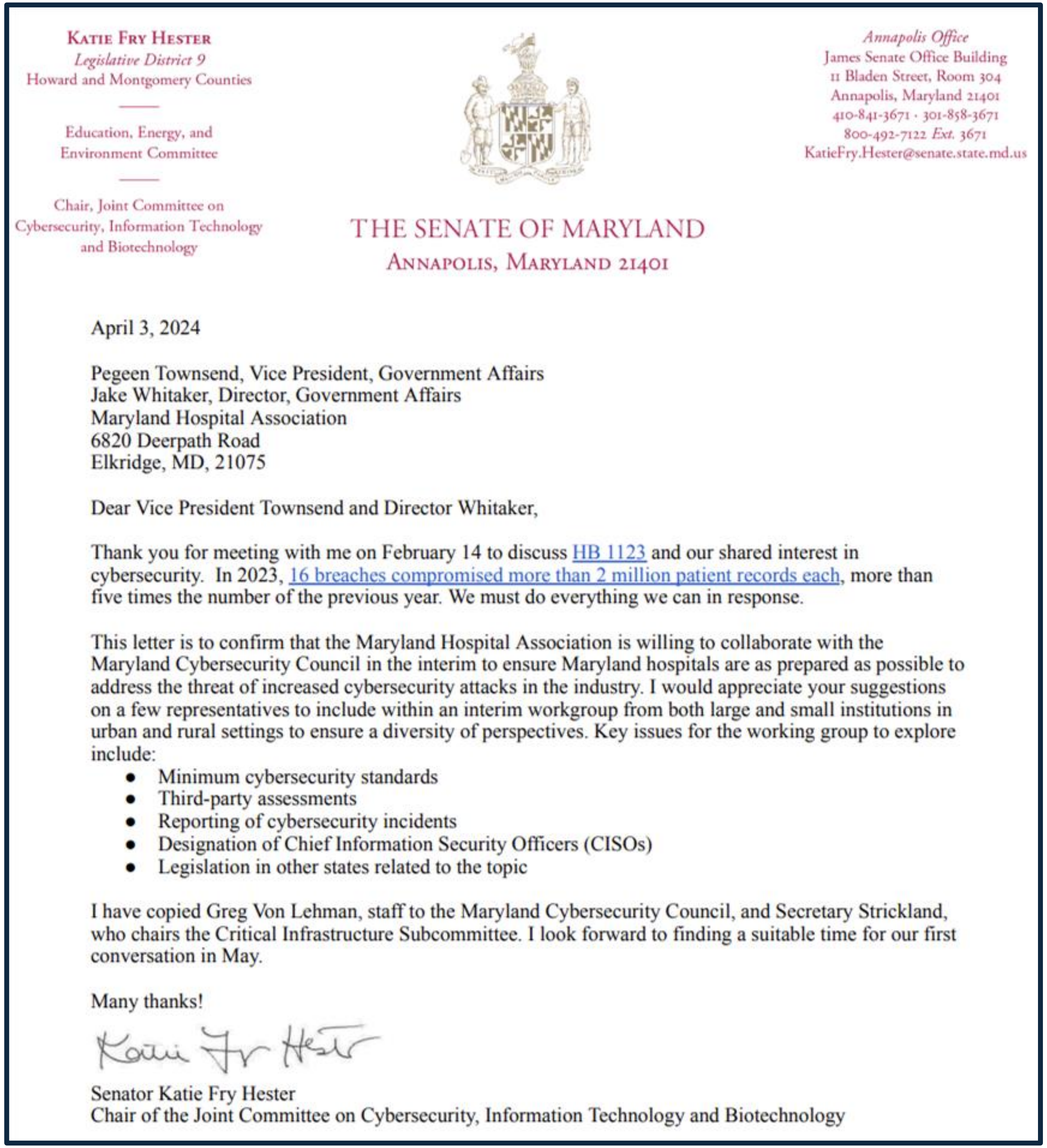
Key Functions Impacted:

- ❑ **Eligibility Checks** – Verifies patient coverage and costs.
- ❑ **Claims Submissions** – Sends claims to insurers.
- ❑ **Claims Status** – Tracks claim progress and rejections.
- ❑ **Prior Authorizations** – Approves high-cost services before treatment.

HB333/SB 691
No Need to Reinvent the Wheel

- SB 691 adopts the same approach to healthcare cybersecurity and protections that the General Assembly codified in HB 969 (2023), sponsored by Delegate Qi. This provided protections for utilities, with common provisions including:
  - Expanded regulator responsibility for the agencies commensurate with the threat
  - Incorporation of NIST frameworks and guidance

On April 3, 2024 Senator Hester sent a letter to MHA:



KATIE FRY HESTER
Legislative District 9
Howard and Montgomery Counties

Education, Energy, and
Environment Committee

Chair, Joint Committee on
Cybersecurity, Information Technology
and Biotechnology

Annapolis Office
James Senate Office Building
11 Bladen Street, Room 304
Annapolis, Maryland 21401
410-841-3671 · 301-858-3671
800-492-7122 *Ext.* 3671
KatieFry.Hester@senate.state.md.us

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

April 3, 2024

Pegeen Townsend, Vice President, Government Affairs
Jake Whitaker, Director, Government Affairs
Maryland Hospital Association
6820 Deerpath Road
Elkridge, MD, 21075

Dear Vice President Townsend and Director Whitaker,

Thank you for meeting with me on February 14 to discuss HB 1123 and our shared interest in cybersecurity. In 2023, 16 breaches compromised more than 2 million patient records each, more than five times the number of the previous year. We must do everything we can in response.

This letter is to confirm that the Maryland Hospital Association is willing to collaborate with the Maryland Cybersecurity Council in the interim to ensure Maryland hospitals are as prepared as possible to address the threat of increased cybersecurity attacks in the industry. I would appreciate your suggestions on a few representatives to include within an interim workgroup from both large and small institutions in urban and rural settings to ensure a diversity of perspectives. Key issues for the working group to explore include:

- Minimum cybersecurity standards
- Third-party assessments
- Reporting of cybersecurity incidents
- Designation of Chief Information Security Officers (CISOs)
- Legislation in other states related to the topic

I have copied Greg Von Lehman, staff to the Maryland Cybersecurity Council, and Secretary Strickland, who chairs the Critical Infrastructure Subcommittee. I look forward to finding a suitable time for our first conversation in May.

Many thanks!

Katie Fry Hester

Senator Katie Fry Hester
Chair of the Joint Committee on Cybersecurity, Information Technology and Biotechnology

Conclusion

“The increasing incidence of ransomware attacks and proliferating cyberthreats require a coordinated approach led by government, in partnership with private sector efforts to innovate on cyber protections and distributed data systems that limit damage after an intrusion”[1]

HB 333/SB 691 answers the call

[1] Genevieve P Kantor, et al (2024), Lessons From the Change Healthcare Ransomware Attack. Journal of the American Medical Association.