Background for Senate discussion on a proposed cybersecurity initiative
May 5, 2016

UMD sits at ground zero for leadership in the global war on cybercrime. Government agencies such as the Department of Homeland Security, the National Security Agency (and CYBERCOMMAND), the CIA, and the FBI as well as leading industry giants are located within a few miles of our campus. UMD has existing strategic partnerships with all of them. We are also the *only university in the nation* to be ranked in the top 25 in computer science, criminology, economics, engineering, information studies, information systems, mathematics, physics, public health, public policy, and the social sciences. UMD's global outreach is second-to-none and growing. We are one of the few universities in the world with the potential to truly integrate all of these fields and computing capacity into a single educational and research powerhouse in this important field.

Thus we are being urged to consider a major university-wide, multifaceted cybersecurity initiative that would leverage the university's significant expertise in research and entrepreneurship and strategic location to train industry executives at the highest level, provide briefings on the latest developments, and facilitate partnerships of faculty and students with industry and government to help commercialize ideas, research, and solutions that focus on cybersecurity solutions.

Meeting these challenges and opportunities will require new research, and – more fundamentally -- the development of new curricula and educational programs that draw on this diverse range of knowledge and expertise to train students and working professionals to contribute to the security of Maryland and the Nation. The University is working towards the creation of an externally facing, cybersecurity initiative to complement our academic and research programs in this area spearheaded by Dr. Michael Wertheimer, Professor of the Practice in the Maryland School of Public Policy.

Ultimately the expectation is that the Maryland Global Cybersecurity Initiative will grow the formidable strengths of the University along five main pillars of activity:

1) **Executive Programs** that will focus on CEO and C-suite education and certification
   C-Level courses and certifications might include:
   - Courses in cybersecurity as related to board level and senior executive decisions
   - The development of policy considerations and roundtables on topics affected by cybersecurity and convening thought leadership and experts to discuss those topics.
   - Formulation of an executive course in cybersecurity for executives outlining applied cybersecurity practices and principals

- Formation of government and industry partnerships and hosting inter industry forums and simulations with a cybersecurity focus on current challenges amongst different verticals in the industry such as the Internet of things.

Cybersecurity Journal:

- A monthly online journal that features plain-language case studies and scholarship covering cyber events and topics relevant to industry and government leaders. (A "Harvard Business Review" for cyber.)

Situational Awareness Website:

A daily website would be developed to provide the latest in (overnight) cyber threat updates, presented in prose accessible and impactful to a CEO such as:

- A list of industry leading web journal articles summarized in a "news clips format"
- Examination of the best cyber metrics that encapsulate macro level activity on a daily, weekly and monthly basis (a cyber stock ticker)

2) **Partner Programs and Applied Research** that will incorporate academic faculty, graduate and undergraduate students, together with a dedicated Institute research staff to deliver immediate industry and government solutions. These might include
   - Providing for joint collaborative opportunities in pre-competitive cybersecurity exercises, simulations and research and development.
   - Formulating positions on topics related to cybersecurity at the State and Federal level.
   - Establishing a newsletter for cyber threat data and potential implications with scholarly articles on position and response.
   - Publishing articles and host public roundtables with senior government officials and cyber thought leaders and the University.
   - Providing opportunities to help commercialize ideas, research and solutions that focus on cybersecurity solutions campus and consortium wide.
   - Establishing a cybersecurity research consortium and venture fund.

3) Work in collaboration with the new FFRDC, the **National Cybersecurity Center of Excellence** (NCCoE) (http://research.umd.edu/news/news_story.php?id=8577) (https://nccoe.nist.gov)

4) **Academic Programs** that will offer current, and future students opportunities across many, possibly all colleges to both learn and exercise cybersecurity through experiential learning, K-12 engagement, and "cyber-track" coursework. Some of these are already in place or under development.

5) **Broadening our basic advanced research** in cybersecurity to include the interests of all Colleges. This might include cryptography, programming

languages, network and systems security, architecture, policy, public health, education, and many others.

All of the externally focused elements of Dr. Wertheimer's vision are meant to generate revenue, and he is confident that they would. We would have to make some initial investment to establish the executive education programs, but the vision is that the revenue generated from these and the applied research work would be substantial and would be cycled back into existing and additional campus academic/research programs. While these are envisioned as high-level executive programs initially, they could be expanded or modified to accommodate our own students and other groups.

Dr. Wertheimer's overall vision for this initiative includes formation of an over-arching Institute, but a decision on whether or not to create such an entity should await the development of some of its components. There are a set of questions we need to address as a campus before we can proceed with the envisioned outwardly facing programs — questions centering on doing/managing work for others, doing applied and restricted (not secret) research, and what connection such activities might have with our existing or future academic and research programs. We have existing mechanisms in place to bring new academic proposals before the senate or other campus approval bodies, but some potentially important partnership opportunities in this area require additional consideration. I intend to ask the Senate Research Council for advice on these possibilities and questions, ideally by the end of the fall semester.

The reporting structure for the applied research components is still an open question, and I'd ask the research council for advice on that point as well.

I look forward to a good discussion with the Senate later this work.

SVP&P/VPR

UMD Corporate Relations

Executive Programs

C-Level Courses/ Certifications

Journal

Situational Awareness Website

Executive Director

Partnership Programs & Applied Research

Applied Research Staff

Incubators & Start-ups

Government & Industry Engagement (Technology, Policy, Journalism, etc.)

FFRDC

ADVISORY BOARD

Maryland Global Institute for Cybersecurity (MGIC)

Executive Programs

From "internal escalation" to "patch implementation," cybersecurity is a field abounding in technical jargon. MGIC executive programs will help leaders and decision-makers "cut through the gibberish," offering superior CEO and C-suite education and certification.

- C-LEVEL COURSES AND PROGRAMS
  - Courses in cybersecurity as it relates to the boardroom, including applied practices and principles
  - Executive master's degree in cybersecurity
  - Access to national thought leadership in the field, including access to policy positions and participation in roundtables on topics affected by cybersecurity
  - Discussions with government and industry partners through forums and simulations focused on cybersecurity challenges in different industry verticals
- MARYLAND CYBER JOURNAL
  - A national "business review" for cyber, this online journal will feature plain language case studies and coverage of events and topics that industry and government leaders can apply on a daily basis.
- MARYLAND CYBER WATCH
  - This daily briefing will provide the latest in overnight cyber-threat updates, translated into actionable suggestions and presented in prose accessible and impactful to a CEO.
  - Industry-leading Web journals digested into a moderated "news clips" format
  - Macro-level cyber activity summarized on a daily, weekly and monthly basis, Established with an Information Sharing and Analysis Center (ISAC) model for the university and its partners

Partner Programs and Applied Research

The Maryland Global Institute for Cybersecurity (MGIC) will leverage the university's strengths in research and entrepreneurship to deliver timely, affordable and effective cybersecurity solutions for industry and government partners.

- INNOVATION DISTRICT INITIATIVE
  - MGIC will make space available for partners to work side by side with University of Maryland students and faculty—even enabling companies to do R&D on campus with their own employees.
- RESEARCH
  - Dedicated institute research staff
  - Partner access to campus research facilities and talent
  - Corporate and government partnerships for applied cyber research opportunities with near-term commercial capabilities
- INNOVATION/COMMERCIALIZATION
  - Regular industry roundtables to focus on areas of innovation for university resources
  - A core set of grand challenges to be met through commercialization of R&D, such as developing the first securitizations of .umd.edu and .md.us
  - Opportunities for students and researchers to creatively problem-solve grand challenges as part of their curriculum

Partner Programs and Applied Research

- GOVERNMENT & INDUSTRY PARTNERSHIPS
  - Joint opportunities in exercises, simulations and R&D Positions on topics related to cybersecurity at the state and federal level
  - Newsletter focused on cyber-threat data and potential implications, with scholarly articles on position and response
- INCUBATORS/STARTUPS
  - Campus- and consortium-wide opportunities to help commercialize ideas, research and solutions that focus on cybersecurity solutions
  - An MGIC startup venture fund
  - A licensing waiver for institute start-ups to encourage students and faculty to create new companies with intellectual property developed on campus