BENS ENGAGEMENT

CYBERSECURITY EDUCATION IN MBA PROGRAMS

June 2017
BENS wishes to thank Dr. Emily Goldman of U.S. Cyber Command for her support of this engagement. For questions related to this effort, please contact Susan Maybaumwisniewski at smaybaum@bens.org.
CONTENTS

I SUMMARY ............................................................................................................................. 4
II BENS MEMBER CHAMPIONS AND GOVERNMENT PARTNERS ............... 5
III STRUCTURED INTERVIEWS ......................................................................................... 6
IV SUPPLEMENTAL RESEARCH ....................................................................................... 6
V FINDINGS .......................................................................................................................... 7
VI RECOMMENDATIONS ..................................................................................................... 8
APPENDIX: KEY DISCUSSIONS ......................................................................................... 9
Cyberspace, with its promise of innovation, prosperity, and connectivity, also presents a series of risks to our national security that must be managed cooperatively by our public and private sectors. As future business leaders, today’s MBA students will need to assume a more proactive role and work with their government counterparts to manage, deter, and respond to cyber threats. These efforts must begin in the classroom with instruction designed to help students effectively navigate and manage a complex cyber threat environment.

The ability of business leaders to understand and manage cyber risks, just as they would financial, operational, or compliance risks, is now an essential business skill. Effective cybersecurity risk management is a potential determinant of organizations’ competitiveness, prosperity, and even viability.

At the request of and in collaboration with U.S. Cyber Command, BENS undertook a review on the type and quality of instruction on cyber issues within Masters of Business Administration (MBA) programs. BENS Member Champions performed research and consulted with representatives of ten universities to understand current practices, requirements, and constraints in these programs. Their approaches can be grouped into roughly four categories:

A. MBAs focused on cybersecurity.
B. Cybersecurity course or module requirements.
C. Joint degree programs with technical schools.
D. Extracurricular emphasis on cybersecurity issues.

Each of these approaches has strengths and weakness, and no one model is uniformly appropriate for every school. Administrators should utilize an approach that’s consistent with their specific resources and course objectives. Schools should also share teaching materials and best practices where possible. Finally, where appropriate, schools should look to partner with public sector entities to, among other things, provide insights to students on national-security equities in cybersecurity decision making.
BENS Members:

Philip Bilden
Founder & CEO, SHIELD Capital Partners

Lars Buttler
President, Madison Sandhill Global

Jim Dean
President & CEO, TrueCourse Advisory Services, LLC

Mike Denny

Craig Jimenez
President, EcoCentri LLC

Scott Johnson
CEO, SJ Partners

Dave Lacquement
Principal Cyber Technical Account, Booz Allen Hamilton, Inc.

Gerry Mauer
Financial Representative, Northwestern Mutual Financial Network

Bill Obenshain
Chairman Center for Financial Services, DePaul University

Dan Roche
Vice President, Northern Trust

Todd Rosenblum
Senior Executive for WW Business Development, IBM

Jim Smith
Principal, Charles River Associates

Raj Surati

Roger Swinford
President & CEO, Calhoun International

Daniel Wallance
Lead Associate, Booz Allen Hamilton, Inc.

Jeffrey Wells
Partner, Cybersecurity & Capital, InnoVacien, LLC

Government Partners:

Dr. Emily Goldman
Director, Combined Action Group, United States Cyber Command and the National Security Agency

John DeLong
Director of Compliance, the National Security Agency

Michael Warner
Historian, United States Cyber Command
Findings from this effort relied heavily upon insights from conversations with a broad cross-section of business-focused academia. In particular, we wish to thank interlocutors from:

- Carnegie Mellon University
  - Tepper School of Business
- Dartmouth
  - Tuck School of Business
- DePaul University
  - College of Business
- George Washington University
  - School of Business
- Georgia Tech
  - Scheller College of Business
- Harvard University
  - Harvard Business School
- National Defense University
  - College and Eisenhower School
- University of Kansas
  - School of Business
- University of South Florida
  - Muma College of Business
- William & Mary
  - Mason School of Business

Beyond the educational institutions that BENS Member Champions interviewed directly for this effort, BENS surveyed other institutions with relevant programs or initiatives. Representative examples include:

- American University Kogod School of Business
- Coventry University Business School (UK)
- Excelsior College
- George Mason University
- Georgia Tech
- George Washington University School of Business
- Harvard University
- James Madison University
- Loyola University Sellinger School
- Mannheim Business School
- MIT Sloan School of Management
- Oxford University Said Business School
- Stanford University
- Temple University Fox School of Business
- Washington University Olin Business School

1. http://www.american.edu/kogod/cybergov/
**V | FINDINGS**

Research performed for this review highlighted the importance of covering cybersecurity issues within MBA programs. Interviewees generally agreed on several broad principles:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>As a matter of overall importance to private sector entities, cybersecurity issues will not decrease or recede in the foreseeable future, and the most likely scenario is a significant increase in the frequency and severity of cyberattacks.</td>
</tr>
<tr>
<td>2</td>
<td>Cyberattacks are likely to have increasingly severe and adverse effects on core business performance metrics. (Views differed somewhat on whether softer factors like adverse reputational effects of cyberattacks were likely to increase or level off.)</td>
</tr>
<tr>
<td>3</td>
<td>There have been, and will continue to be, cyber threats to and attacks on businesses that affect U.S. national security or U.S. national interests. To the extent that both public sector and private sector actors understand each other's equities and processes, greater collaboration between the two can enhance both sides' security posture.</td>
</tr>
<tr>
<td>4</td>
<td>At present, the vast majority of MBA programs do not adequately prepare students to address enterprise cyber risk. This should be addressed at every level—prior to higher education and within higher education. There is also a role for conveying skills within the context of executive education programs.</td>
</tr>
<tr>
<td>5</td>
<td>Broader availability of business cases related to previous cyber events would make a significant difference in the instruction students receive. The dearth of such materials relative to those available for more conventional business issues has constrained educators.</td>
</tr>
<tr>
<td>6</td>
<td>There is not currently, and ought not to be, one uniform standard for how to cover cyber issues within MBA programs (see below).</td>
</tr>
</tbody>
</table>

The absence of a uniform educational standard in this space has led to uneven outcomes. Some curriculums are completely devoid of cybersecurity related content, others are focused squarely on the subject. Yet, schools are currently experimenting and finding success with a variety of different models. Of the schools that participated in this review and appear to be taking the issue of cybersecurity seriously, four primary approaches emerged:

**MBAs focused on cybersecurity.** Recently, programs have emerged that purport to offer MBAs in cybersecurity issues, or where cybersecurity is a central focus.

**Cybersecurity course or module requirements.** Some programs are either implementing (or considering implementing) optional or required coursework related to cybersecurity.

**Joint degree programs with technical schools.** Several institutions have arrangements between their Business Schools and Computer Science, Engineering, or other technical schools that offer...
Cybersecurity Education in MBA Programs

joint or dual degrees (or at a minimum make specialized courses available to students from other schools).

**Extracurricular emphasis on cybersecurity issues.** Many schools have no formal instruction on cyber issues, but are increasingly making cyber education a focus of extracurricular programming. In practice, this might mean anything from recruiting guest lecturers to address cyber issues, to opening up research fellowship appointments in technical centers to qualified MBA candidates.

### VI | RECOMMENDATIONS

This review yielded five key recommendations for academia:

1. **Recognize the emergence of cybersecurity as a key issue for business leaders.** Provide instruction on the matter that is commensurate to its level of importance.

2. **Devise a strategy to cover the matter sufficiently.** This may take the form of one of the options outlined above (Sec. V, options A-D), some hybrid of those options, or choose an approach that leverages the institution's particular assets and resources.

3. **Consider going “broad”** (providing some minimum level of cybersecurity instruction to every MBA student) and “deep” (providing considerable instruction on the subject to a subset of students).

4. **Share best practices and teaching materials with other educational institutions where appropriate.**

5. **Where possible, partner with government institutions to provide students with increased situational awareness and real-world insights on possible public-private approaches to combatting cyber threats.** This may also better inform each partner on the strengths and weaknesses associated with each side.
APPENDIX | KEY DISCUSSIONS

Most of the findings in this paper are the result for several dozen meetings, interviews, and discussions throughout 2016 and 2017. The most significant include:

- **1/8/2016**: BENS staff met with Dr. Emily Goldman, Director of Commander’s Action Group at U.S. Cyber Command. The meeting was held to gain understanding of how BENS could partner with Cyber Command and create an action plan to move forward with a Private-Public Partnership of integrating cyber security into MBA programs.

- **2/17/2016**: BENS staff held an initial call with Steve Leonard from University of Kansas School of Business regarding the universities involvement in the Cyber MBA project.

- **4/7/2016**: BENS convened a teleconference between Members and representatives from the National Security Agency/U.S. Cyber Command. The objective of the call was to identify and discuss the specific subjects, themes, and/or case studies that could be incorporated in MBA programs.

- **4/20/2016**: BENS facilitated a call between our members and representatives from the MBA programs. Discussed during the call was the current state of cyber themes in the MBA program and whether/how they perceive the potential for greater inclusion.

- **4/29/2016**: On April 29th, 2016, BENS hosted a teleconference between representatives from Dartmouth’s Tuck School of Business, National Security Agency/U.S. Cyber Command, BENS Members and Staff to discuss opportunities regarding BENS Cybersecurity MBA project.

- **5/9/2016**: BENS hosted a teleconference between Members, representatives from the National Defense University’s (NDU) iCollege, and National Security Agency/U.S. Cyber Command officials to discuss possible opportunities regarding BENS Cybersecurity MBA project.

- **5/18/2016**: On May 18, BENS staff held a call with DePaul University regarding their participation in the cyber MBA program project.

- **5/19/2016**: On May 19th, 2016, BENS hosted a teleconference between William and Mary’s Raymond A. Manson School of Business to discuss opportunities regarding BENS cybersecurity MBA project.

- **8/4/2016**: BENS hosted a phone call between BENS staff, BENS Member Todd Rosenblum, National Security Agency/U.S. Cyber Command’s Dr. Emily Goldman, and Frank Cilluffo of George Washington University to discuss GWU’s possible involvement in the planned Cybersecurity MBA project.
Cybersecurity Education in MBA Programs