When Emerging Technologies Cross Academic Boundaries: Collaboration or Competition?

Dr. Barbara Christe, Indiana University-Purdue University of Indianapolis

Barbara Christe is a professor and director of the healthcare engineering technology management program in the Purdue School of Engineering and Technology at Indiana University Purdue University Indianapolis (IUPUI). She coordinates a unique academic program that prepares engineering technology graduates to support the safe and effective use of medical equipment in the clinical setting. Dr Christe has a bachelor's degree and master's degree in biomedical engineering from Marquette University and Rensselaer at Hartford respectively. Her doctorate is in higher education administration from the University of Phoenix. She conducts research in the clinical applications of radio frequency identification technologies (RFID) as well as STEM student retention.

Mr. Joe Tabas, Indiana University-Purdue University of Indianapolis

Joe Tabas is a lecturer of Engineering Technology at the IUPUI school of Engineering Technology. His areas of research include digital electronics and data communication for medical devices and industrial control systems.

When Emerging Technologies Cross Academic Boundaries: Collaboration or Competition?

Abstract

Institutional barriers associated with disciplinary boundaries created by departments can prove particularly challenging to the approval and implementation of new academic credentials. This paper will utilize a case study technique to analyze the proposal and approval pathway of a certificate focused on medical device cybersecurity in an engineering technology department at a mid-western urban university. From inception through implementation, the paper will examine existing academic boundaries that may be crossed by emerging technologies. The challenges of the process can illuminate the hurdles of collaboration and inform readers who seek to implement other academic courses or programs in emerging areas.

Background

Cybersecurity is an emerging concern for many disciplines because protecting a myriad of types of data is critical to a variety of successful enterprises. The WannaCry virus that infected healthcare institutions in the United Kingdom in May of 2017 moved cybersecurity risks into the public view. To clarify, the hostile take-over of the networks of healthcare systems and hospitals, such as occurred in the United Kingdom and in several of the United States, is *not* related to medical device attacks. The ransom paid by hospitals to regain access to their networks is related to patient records, billing, and file storage. No successful medical device hacks or ransom have been recorded. However, experts have warned that the first medical device attack will certainly occur in the future.

Medical equipment is defined as devices that have been cleared by the FDA that are intended to be used for diagnostic, therapeutic, or monitoring care provided to a patient by a health care organization [1]. Examples of medical devices include patient monitors, imaging equipment such as CT scanners, and anesthesia machines. Almost all medical devices are directly associated with the patient in some way.

Healthcare Technology Management (HTM) is the name for the profession that supports the safe and effective use of medical technology in the clinical setting. Only a few academic programs offer training for healthcare engineering technicians and technologists, with most offered at the associate degree level. In addition, most programs are housed in public institutions who have been under legislative pressure to reduce the number of credit hours included in their degree. As a result, the emerging need for technicians trained in medical device cybersecurity is difficult to include within existing academic frameworks.

Whose responsibility is the vulnerability assessment of medical devices? Hospitals have established the boundaries between medical device cybersecurity and network cybersecurity relatively well – if the device is inside the patient room, it is the job of Healthcare Engineering Technicians (HET) – if the computer server or other device is outside the patient room, information technology (IT) ensures safety. However, academicians are not nearly so neat with

disciplinary boundaries and may struggle when emerging technologies cross academic units. Thus, when an HTM program sought to create a medical device cybersecurity certificate, collaborative challenges arose.

Medical Device Interoperability

Computer networks have been utilized to maintain patient records and billing in hospitals for a very long time. However, the American Recovery and Reinvestment Act (ARRA) legislation passed in 2009 offered financial incentives to establish electronic medical records – computerized storage of physiologic data, test results, and patient information recorded by clinicians. Networked electronic medical records (EMR) offered the potential for the ability to archive and share large amounts of patient information that could profoundly impact patient care.

As the implementation of the EMR proceeded, clinicians soon realized that patient physiologic information, like a blood pressure reading obtained through the use of a medical device, could be directly reported to the EMR through the hospital IT network. The process of a clinician utilizing a blood pressure device to obtain a patient blood pressure, then recording the numbers displayed on a scrap of paper and then entering the values on a computer seemed inefficient and potentially inaccurate. Thus, medical device manufacturers, healthcare engineering technicians, and clinicians sought to connect medical devices directly to the IT network, transferring information directly. This process is called interoperability.

The connections between the medical device and the network can be filled with challenges, however. First, medical devices feature a wide variety of physical connectors (USB, RS232, Ethernet, wireless connections of various types, etc.) to communication information. In addition, the data protocols (formatting) are not uniform. In fact, nearly 100 protocols for medical devices are currently in use. Lastly, some devices provide an absolutely enormous amount of information that is likely meaningless in large quantities. For example, the electrical activity of the heart (ECG) generates data in real time – yet most of the continuous information is unimportant – unless there is a cardiac event. The identification of the "important" data to archive and the data that is not clinically relevant is critical in the use of IT network storage. In addition, the quantity of data passed over the network must be evaluated in terms of bandwidth, especially for large hospitals.

Not all medical devices currently have the ability to connect to the network to transmit physiologic data to the EMR. Estimates suggest that currently about one-third of devices are capable. Some device types are not appropriate for inclusion into the EMR as the equipment has a single purpose and does not generate meaningful data. Technology not connected to the Internet or networked is not a concern for cybersecurity threats.

In addition, some medical device communications are best managed in the opposite direction: from the network to the device. For example, a pharmacist can enter an order for medication into the computer network. This information could be transferred to an infusion pump that would then be programmed with the correct drug and dosage for the nurse to administer.

To facilitate the transmission of information between the network and medical devices, third-party middleware tools and software, called Medical Device Data Systems (MDDS), have emerged. These systems are device specific – designed to capture the date from one particular brand and model of a device and then send the data to the network. Companies, such as Capsule, have created libraries of many medical devices in order to manage the information transmission. The initial Capsule installation for each device can be challenging. As a result, some facilities have limited their network-connected devices to high stakes equipment like anesthesia machines or specific environments like the operating room.

Medical Device Cybersecurity

Medical device cybersecurity specifically looks at the vulnerabilities of the connections between the device, any middleware, and the network. The ANSI/AAMI Standard IEC TIR80001-1, *Application of Risk for Management of IT-networks Incorporating Medical Devices* identifies the activities that are required to minimize medical device vulnerabilities. This standard is specifically designed to support engineering technicians who have detailed knowledge of medical technology.

Kevin Fu, PhD, cybersecurity expert and Associate Professor at the University of Michigan offered the keynote lecture at the annual conference of the Association for the Advancement of Medical Instrumentation in June of 2017. He described the four major weaknesses in hospitals, urging attendees to increase cybersecurity vigilance. His keynote address prompted extensive discussion among HTM professionals who had not considered the risks of interoperability prior to the June meeting, driving medical device cybersecurity to the forefront.

Wirth [2] wrote in an article in *Biomedical Instrumentation and Technology* that "we are facing a serious and global shortage of cybersecurity skills." His article included an outline for a cybersecurity training program, utilized by the faculty members involved in the development of the certificate to craft the course content. The topic outline provided by Wirth incorporated regulations, priority differences, attack vectors, procurement best practices, threat management, and life cycle planning.

The recommendations of the US Department of Health and Human Services' Cybersecurity Task Force June, 2017 report *Improving Cybersecurity in the Healthcare Industr*y [3] included:

- Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities, and
- Increase healthcare industry readiness through improved cybersecurity awareness and education.

The proposed certificate would meet both of these recommendations.

The Medical Device Innovation, Safety and Security Consortium (MIDSS) is a non-profit public health and patient safety organization focused on medical device cybersecurity. The organization approaches medical device security as a public, epidemiological threat. This approach is unique but has drawn attention by clinicians and engineers alike. MDISS supports the use of MDRAP, a medical device risk-assessment platform that guides technicians through vulnerability

identification and mitigation. This organization approached this institution as a partner in medical device cybersecurity education.

Certificate Development

Driven by this publicity and strong push from employers, a Midwestern public university sought to create and offer a medical device cybersecurity academic credential, leveraging a partnership with MIDSS. Grant funding was made available by this group as well as from the campus to develop course content and generate an academic credential. The credential was intended serve learners who support the delivery of healthcare through technology by promoting secure and compliant utilization of medical devices. The certificate provides in-depth content that will supplement the skills of technicians who currently work in clinical settings to align with a rapidly changing demands of medical technology. Course content was selected, vetted with the program advisory board, and shared with constituents.

The certificate was designed to include four courses for a total of 12 credits. Learners are able to ensure that medical technology is protected from cyber threats and that patient physiological data is secure. Course content will be adapted and responsive to the changing medical device cybersecurity landscape. The course material is extremely narrowly focused on medical devices like ventilators and defibrillators. While some background information technology material guides terminology, the specific content is more closely related to clinical engineering than computer networking. In addition, the course content is focused on the skills needed by technicians working in the clinical setting – hospitals, clinics and other patient care areas.

The campus features five hospitals and partnering with clinical engineers already engaged in medical device cybersecurity threat detection and mitigation offered a substantive foundation for the certificate. One hospital in particular was a leader in the use of MDRAP and had utilized students as part of the review process. As a result, the program connected with hospital-based engineers who could drive the learning objective development of the certificate with the most current software tools.

The Approval Process

The university has a defined certificate creation/approval process that begins in the department and is somewhat complicated due to the complex connections between two campus administrations. The program initiating the credential is responsible for connecting with any other programs who could be viewed as potential overlap. This process is illustrated in Table 1. In past campus-level review situations for new courses or course change requests, the School of Informatics and Computing program in Health Information Management (HIM) has been contacted to offer evidence of a lack of overlap. The Health Information Management program is focused on the electronic medical record as well as the education and policy of such records. In contrast, the healthcare engineering technology management program is focused on the medical devices as well as the device/patient interface. Documentation was secured from the HIM program director indicating support for the proposed certificate.

Table 1 Approval process for certificate

Stage	Outcome
1. Industry representatives encourage certificate development, review content for appropriateness	Certificate framework reviewed by constituents
2. Program director creates certificate proposal and submits to undergraduate education committee in School	Certificate created
2.a Program sought support from the School of Informatics	Support was documented
3. School-level undergraduate education committee review	Committee representative from the computer information technology department objected to the proposal. Chair of the undergraduate education committee sought unanimous agreement to approve the proposal
3. a. Chair of undergraduate education committee requested discussion among two department chairs (chair of the department who authored the proposal and chair of the department whose representative on the undergraduate education committee objected to the proposal)	Chair of computer information technology (CIT) department strongly objected to the proposal
3. b. The department chairs met with the dean to seek a resolution	No resolution was achieved
3. c A program representative (not the program director) met with the two chairs to negotiate a compromise	The CIT department agreed to support the proposal when one CIT course was added to the certificate curriculum.
4. Undergraduate education committee review	Proposal was reviewed and passed on to the next stage
5. Faculty Senate review	Faculty senate approved the proposal
6. Campus-level undergraduate education committee review	Committee was confused, thinking the certificate overlapped nursing programs. Clarification was made, certificate was approved to move forward to the next stage
7. Proposal moved on to the main campuses for approval	At the time of publication, the certificate had been approved on February 22, 2018. Student admissions is delayed until a degree code has been assigned.

Within the School of Engineering and Technology, the Computer Information Technology (CIT) program has a robust cybersecurity curricular component. In addition, the program faculty are leaders in research into network cybersecurity threats and mitigation. When the first HETM course in interoperability was proposed in 2015, the program directors and faculty members from both CIT and HETM met. The group discussed the course content at length and agreed that the

HETM course focused on medical devices, the interface between the patient and the medical device, and the passage of physiologic data from the medical device to the network. In addition, it was agreed that this was in the HETM domain as it focused on devices like intravenous pumps, ECG monitors, and anesthesia machines. Hospital IT networks are absolutely a CIT domain but the connection from the medical device to the network is the realm of technicians who graduate from the HETM program. The courses were approved shortly after.

Prior to the initial school-level review of the certificate approval, the program director of the CIT program was contacted several times without reply. The HETM program director assumed that the previous division of responsibilities were still appropriate and, as a result, the program had no concerns about the certificate. Unfortunately, this assumption was incorrect.

When the school committee met to consider the proposal, the CIT representative was against the credential and the committee chair sought to obtain unanimous consensus. As a result, the proposal was tabled to allow for additional discussion. The main objection stemmed from the use of the term "cybersecurity" – a term that was perceived to belong to the world of information technology alone.

The department chair associated with the CIT program and the department chair associated with the HETM program met to discuss the deep concerns about the use of the term "cybersecurity." In addition, the department chair associated with the CIT program had substantial issues with the content of the coursework as the material did not appear as exploring what was considered IT cybersecurity. In this way, the department chair associated with CIT was prepared to block the proposal. After unprofessional behavior was displayed, a request was made to include the Dean in a future discussion.

A meeting between the Dean and the two department chairs was held. Deep concerns were expressed that the CIT program must teach all material related to the concept of cybersecurity lest other academic programs on campus could also encroach on the territory. The HETM program director was not part of the conversation. As a result, the requisite medical device knowledge needed for course delivery was not raised. The result of the conversation was that the CIT program should teach all of the courses in the certificate in order for the CIT program to approve it. Collaboration across disciplines was not discussed. The certificate was viewed only as competition for a specific academic group. Interestingly, the competition was not viewed from student enrollment concerns but, instead, the focus was on "territory" – that approval of this certificate would erode the ability to deliver cybersecurity content by the CIT program.

To clarify the "territory", the constituents of the HETM program, namely the practicing engineers and technicians who support the use of medical devices in the clinical setting are a different group than the IT network specialists who may also work in healthcare settings but are not involved in the device/patient interface. Roundtable participants in a recent article [4] describe medical devices as a "special snowflakes" in the IT world because devices function and operate uniquely. This dramatic difference compared with traditional IT devices like routers and switches calls for specialized education and training.

The HETM program director, upon hearing the decision regarding the requirement that CIT faculty be involved in course instruction, explained that CIT faculty would have to enter an operating room and successfully identify an anesthesia machine before the person could teach a class. This knowledge of the operating room environment as well as the devices inside it was outside of the skill-set (or comfort level) with the CIT faculty and so additional negotiations were held. The proposal could not move forward for a vote until all of the school undergraduate education committee members would support the certificate.

A compromise was desperately needed. After much discussion, a decision was made to include one CIT course in the certificate that explored the general concepts of security. This course focuses on IT security concepts such as cryptology, authentication, security kernels, rogue programs, and steganography. Learners will be able to identify ways to ensure secure email usage and Internet access. These general skills have little application to medical devices but do offer a foundation in cybersecurity awareness. Following the certificate content change, the credential was approved by the school and moved to the campus.

Discussion at Campus Level

Campus approval was required and the meeting was held in November, 2017. Again, overlap with other programs was a concern raised by the subcommittee review, but this time with a focus on medical programs like nursing, dentistry, and occupational therapy. Essentially, the subcommittee expressed concern related to any program that utilized medical devices as potential overlap. In this case, explaining that healthcare engineering technicians support medical devices but do not utilize the devices for patient care was clarification enough for support. Interestingly, during the committee meeting, the nursing program was an enthusiastic endorser of the certificate, stating to the larger group that nurses needed to focus on delivering patient care and had no interest in how the medical devices were supported – as long as they were safe and available when needed.

Unfortunately, the campus level committee chair failed to click “submit” on the paperwork in the electronic approval software once the committee voted. As a result, subsequent review levels for the certificate have been delayed. An update on the approval process will be provided during the ASEE Conference.

Challenges and Lessons Learned

The little known profession of Healthcare Technology Management straddles several disciplinary areas and suffers confusion. Educating faculty, department chairpersons and deans as to the specific responsibilities of technicians who work in healthcare seems critical to the successful deployment of educational content. *Money Magazine* named this profession as one of the top five professions no one has heard of [5]. Interestingly, every hospital engages engineering technicians who maintain medical devices, with many actively involved in the life cycle management of this equipment. The threat of medical device vulnerability to hackers is especially concerning since the patient/equipment interface, if compromised, can cause harm or withhold vital therapies.

The ability for the HETM program director to adequately convey the need for this specialized academic credential was greatly lacking as evidenced by the confusion and concern at various levels and areas. In reflection, several lessons can be noted:

- A lack of discipline-specific understanding can cause significant pushback – in this case, the concept that offering discipline-specific applications of cybersecurity concerns about medical devices does not diminish the need for course content in cybersecurity of networks, software, or the Internet,
- Seeking unanimous consensus can be difficult when supporting information is incomplete or misunderstood,
- In theory, collaboration should be a shared goal of a united group of academicians – rather than a vision of competition for territory,
- Educators may need to understand that consensus around a shared goal may not exist and may limit explorations into emerging technologies,
- Examination of the constituents surrounding academic credential can help identify areas of overlap.

The fundamental lesson learned surrounds the ability to convey constituent needs to transcend academic boundaries. This salesmanship may be challenging for educators and difficult to implement. However, academic institutions and programs are urged to maintain technical currency and explore emerging technologies, despite the implementation challenges.

Conclusion

Medical device cybersecurity knowledge is a vital skill in the healthcare environment. Healthcare engineering technicians and technologists who support medical device use in patient care need cutting-edge skills to identify, evaluate, and mitigate risks, preventing hostile control from unauthorized sources. Academic programs can deliver coursework focused on this knowledge through a certificate. Seeking certificate approval can require clear communication and collaboration among academic colleagues who may confuse the boundaries between medical devices and hospital networks.

References

[1] American National Standard ANSI/AAMI EQ89:2015

[2] A Wirth, “The Importance of Cybersecurity Training for HTM Professionals,” *Biomedical Instrumentation and Technology*, vol. 50(5), pp. 382, September/October, 2016.

[3] United States Department of Labor Healthcare Industry Cybersecurity Task Force *Report on Improving Cybersecurity in the Healthcare Industry*, June, 2017. Available from https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf [Accessed February 1, 2018].

[4] R Jensen, S Copeland, S Domas, R Hampton, K Hoyme, M Jump, I Rekik, S Schwartz, and E Vasserman, “A Roundtable Discussion: Thawing Out Healthcare Technology's ‘Special Snowflake’ Cybersecurity Challenges.,” *Biomedical Instrumentation & Technology: Cyber*

Vigilance: Keeping Healthcare Technology Safe and Secure in a Connected World, Vol. 51, No. s6, pp. 10-16, 2017.

[5] D Bortz, “The 5 best jobs you've never heard of,” *Money Magazine*, 2015. Available from http://time.com/money/3661833/new-job-titles-2015/ [Accessed February 1, 2018].