HealthManagement
Promoting Management and Leadership

Volume 16 - Issue 3, 2016 - Cover Story

Future Leaders: What Healthcare Needs For Cybersecurity Risks

Mansur Hasib
******@***umuc.edu

Programme Chair of Cybersecurity Technology - The Graduate School of University of Maryland University College (UMUC) & Cybersecurity and Healthcare Speaker & Author

Twitter

What, in your view, are the greatest threats facing the healthcare sector in cybersecurity?

First, the wrong executives such as Chief Financial Officers are in charge of IT and cybersecurity strategy in half US healthcare organisations. One third have no cybersecurity executive on staff. In too many organisations qualified cybersecurity executives are not empowered to do the right thing. For example, even though strong, yet simple, authentication systems have been around for a while, too many healthcare organisations continue to rely on userid/password based systems – the weakest form of authentication. Authentication systems need to be easy and should not make life difficult for users. The second challenge is that governance and executive accountability is lacking. In the absence of due diligence, healthcare organisations are falling increasingly victim to ransomware and other similar attacks. Finally, new technology, including medical devices with weak security continue to be implemented without proper vetting – thus increasing the number of attack vectors and risks dramatically.

What can healthcare leaders do today to start addressing these threats?

Organisations must accept digital strategy as integral to organisational strategy. They need to hire qualified digital strategists, put them in charge at the highest levels of organisations to implement continuous innovation, data governance, and digital risk strategies. Importantly, leaders have to incentivise and engage the entire organisational workforce toward the solution. Cybersecurity is not a one-brain sport.

In your book Cybersecurity Leadership, you describe what you call 'ethical leadership'. Can you define this?

Ethical leadership is the principle of sharing the fruits of innovation and productivity with the very people producing this. This is also the very foundation of capitalism. Cybersecurity is essentially perpetual innovation. People innovate – machines do not. People will not innovate if they do not have an incentive to do so. Ethical leadership inspires a cybersecurity culture through higher levels of engagement, loyalty, and innovation. In this manner, a people-focused cybersecurity strategy becomes a powerful innovation, revenue, and profit driver for any organisation.

What is the biggest mistake healthcare CEOs are making when it comes to implementing effective cybersecurity?

CEO s have ignored people and focused on buying technology. They treat people as the "weakest link" and force them to go through meaningless cybersecurity awareness training based on an outdated information security model. Instead, people can be our greatest strength. Training should focus on proper usage of all the technology and data that each person uses. In terms of staffing, organisations have been penny-wise and pound-foolish. They are looking for purple squirrels at mouse pay. Instead of setting compensation at market, they are trying to hire based on artificial budget numbers. Hence they have created an artificial "skills gap". Companies have also been reluctant to develop internal

talent with known organisational loyalties. Organisations need to implement strong talent development and retention programmes tied to the concept of ethical leadership.

Can you describe what is unique about the graduate cybersecurity technology programme at the University of Maryland University College (UMUC), and why you think its principles could work for present healthcare executives?

The main problem in executive education is that business schools do not teach cybersecurity and digital strategy and most cybersecurity education focuses on technology and ignores business concepts. Executives are taught to think of people as expenses. Of course this kills innovation, productivity and loyalty. As a result, people become a major source of internal threats – both accidental and intentional. Many academic cybersecurity programmes are really computer science or engineering programmes or teach a small aspect of cybersecurity. At UMUC we are holistic and transparent in our approach and deal with all aspects of cybersecurity.

We understand that cybersecurity is a vast interdisciplinary field with people, policy, and technology aspects. To cover this range, we have four Masters Degree tracks providing clarity in career possibilities: Cybersecurity Management and Policy, Cybersecurity Technology, Digital Forensics and Cybersecurity Investigations, and Cybersecurity Operations and Information Assurance. However all students go through cybersecurity leadership, decision-making, and analytics. As an open university we believe education should be available to anyone. Therefore we leverage technology to offer our programmes to 93,000 students worldwide with 12,000 students in our graduate and undergraduate cybersecurity tracks. In most programmes we accept people from a wide range of disciplines because we believe in an interdisciplinary business approach to digital strategy. Our students are mostly working professionals and they apply what they learned by completing projects in their courses. Professors, with deep real world experiences, teach and mentor our students. We feel we are producing the next generation of business executives at UMUC.

Is there anyone leading the way in healthcare cybersecurity?

Healthcare organisations, which embraced digital strategy as a business driver, have done well. These organisations have very strong CEO /CIO partnerships going back decades. Technology, data, and analytics have been powering the mission of Kaiser Permanente for a long time. They have used digital strategy to make better decisions, improve healthcare, reduce errors, and engage partners and patients.

You have a particularly strong stance against CEOs and CFOs who do not engage with IT or CIOs/ CISOs – and vice versa. Do think this may be harsh?

I have been more vocal lately since my earlier polite advice has been largely ignored. In the meantime, three organisations with the wrong executives in charge have breached my own personal information and offered very little protection or remediation. I have seen and heard of executives in profitable companies lay off thousands of people just to increase their annual bonus. They have even fired CIO s and CISO s for pointing out issues instead of doing the right thing. I am disturbed that executives are not learning from incidents. For example breaches like Community Health Systems and later Anthem should never have happened. These were all failures in leadership and governance. In the meantime, the digital identities of half the US population have already been compromised and the rampage continues unabated. Offering to monitor credit for a year or two is an irresponsible response. A large number of victims are children who will face problems several years from now. I am particularly disturbed that money drives healthcare organisational strategy instead of strategy driving money. Having a CFO drive IT and cybersecurity strategy makes no sense. They do not believe technology is core to their mission. CFOs also tend to view technology as an office automation function. Since they feel inadequate managing this function, many of them have completely outsourced IT – resulting in even higher costs and perpetual stagnation. When IT got outsourced, internal IT talent and innovation also vanished with it. Outsourced IT will only do what you tell them to do.

The industry appears to believe in the myth that CFOs “save” money by controlling IT and cybersecurity costs. Yet I see countless examples of CFOs wasting money on inappropriate technology at “discount” prices or leaving critical positions unfilled in their efforts to “save” money. Most often they do not invest in continuous improvement to avoid problems. They spend money after a problem occurs – often on inappropriate technology and solutions – just to show that they did something.

If you had to write a job description for the ideal healthcare leader, what would it look like?

The modern healthcare executive needs to understand the new world of electronic health records, health information exchanges, health insurance exchanges, digital patient identities, patient and partner engagement through technology, integration of medical instruments and the entire spectrum of patient care, data analytics and business intelligence and data driven decision making – all while maintaining confidentiality, integrity, and availability of data and systems using a balanced mix of people, policy, and technology, while perennially improving over time. In order words they have to be a true healthcare digital strategist. We also need ethical leaders who understand that ethical leadership is not only profitable for business, it is the only way to achieve perpetual innovation and long term success in any organisation.

Dr. Mansur Hasib is the author of Cybersecurity Leadership where he shares a unique cybersecurity governance and culture model based on his research and 12 years experience as a Chief Information Officer. This book was cited in a US Senate hearing and is used by universities and government and private cybersecurity leadership programs.

Dr. Hasib serves as Programme Chair, Cybersecurity Technology in the Graduate School at University of Maryland University College (UMUC) and has a Doctor of Science in Cybersecurity. He also holds the prestigious CISSP , PMP, and CPHI MS certifications. With 30 years experience in healthcare, biotechnology, education, and energy, Dr. Hasib is a frequent speaker at conferences. Dr. Hasib developed a holistic graduate academic programme, which blends business, information technology and cybersecurity. In 2013, Dr. Hasib conducted a national study in US healthcare cybersecurity and published the book Impact of Security Culture on Security Compliance in Healthcare in the U.S..

Key Points

- Digital strategy is the same as organisational strategy today. Yet education of executives is focused on finance, marketing, and accounting.
- Cybersecurity is perennial innovation.
- People innovate.
- Cybersecurity leadership is critical for long-term success of organisations.

Published on : Thu, 25 Aug 2016