PERSPECTIVE

BY **Steven L. Kanter,** MD
AAHC President / CEO

There is an escalating number of cyberattacks targeting healthcare institutions. And there are growing concerns about the vulnerability of the 'Internet of Things,' including medical devices such as pacemakers and insulin pumps. These technologies, along with issues of patient trust, privacy, and transparency, require academic health center leaders to be on the vanguard of preparing for and managing cybersecurity risks. In this issue of Leadership Perspectives, three academic health center leaders share their experiences and insights on crisis management in a healthcare environment that is increasingly the venue-of-choice for cybercriminals.

Jeffrey R. Balser MD, PhD, president and CEO of Vanderbilt University Medical Center and dean of the Vanderbilt University School of Medicine, notes the importance of giving IT security directors a direct reporting relationship to top leadership and giving IT security concerns primary consideration at the highest level of governance, while also recognizing that "many challenges in cybersecurity are cultural."

Randolph Hall, PhD, vice president of research at the University of Southern California, highlights his institution's three-pronged approach to cybersecurity: studying internet traffic behavior, simulating incidents to test and improve responses, and looking closely at the aspects of human behavior that might lead to or defend against security breaches.

Martin Paul, MD, PhD, president of Maastricht University in the Netherlands, grounds his message in a specific example of an attempted, but unsuccessful, cyberattack. In describing his institution's work in managing cybersecurity risks, he cautions that traditional crisis management protocols are not sufficiently robust to deal effectively with modern cybersecurity issues.

Academic health centers must be proactive in cybersecurity, including educating their own leadership teams, engaging with leaders of other academic health centers, and being prepared to manage a cyberthreat. There will be valuable programming on cybersecurity and other aspects of crisis management at AAHC events throughout the year, including presentations, case studies, and simulation exercises.

www.aahcdc.org

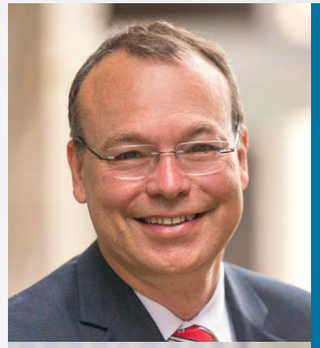
Association of Academic Health Centers
1400 Sixteenth Street, NW, Suite 720
Washington, DC 20036
202.265.9600

Association of Academic Health Centers®
Leading institutions that serve society

ASSOCIATION OF ACADEMIC HEALTH CENTERS

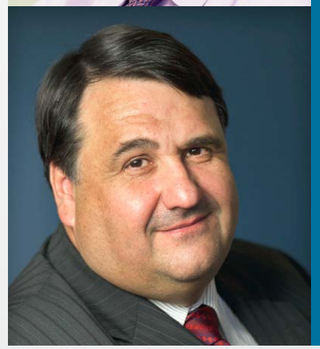
LEADERSHIP PERSPECTIVES

Crisis Management: Cybersecurity



Jeffrey R. Balser, MD, PhD
PRESIDENT AND CEO OF VANDERBILT UNIVERSITY MEDICAL CENTER AND DEAN
Vanderbilt University School of Medicine

Randolph Hall, PhD
VICE PRESIDENT OF RESEARCH
University of Southern California



Martin Paul, MD, PhD
PRESIDENT
Maastricht University

WINTER 2019
www.aahcdc.org

Association of Academic Health Centers®
Leading institutions that serve society

Jeffrey R. Balser, MD, PhD // *President and CEO of Vanderbilt University Medical Center and Dean*

Vanderbilt University School of Medicine

Through a multi-year reorganization effort with Vanderbilt University that concluded in May 2016, Vanderbilt University Medical Center (VUMC) became a legal and financially separate not-for-profit corporation. While we remain highly interactive with the University in academic programs, VUMC has established independent operating and management structures tailored to the needs of an academic health system. Among the most important has been information technology.

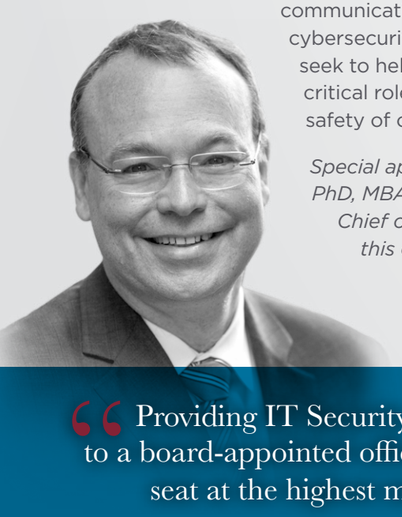
We created three separate, highly interactive branches of our IT organization. One, VUMC IT, focuses on infrastructure such as communications, storage, and administrative IT. Another, Health IT, focuses on clinical enterprise decision-support and our electronic medical record. The third, IT Security, is responsible for cybersecurity. The directors of all three units are highly interactive, and report directly to VUMC's Chief Operating Officer.

Providing IT Security a direct reporting relationship to a board-appointed officer elevates cybersecurity to a seat at the highest management tables. In myriad settings, we find cybersecurity requires consideration as a primary, rather than secondary, concern. Further, the reporting structure gives IT Security leverage to challenge assumptions, assuring concerns are considered in a broad array of strategic and operational decisions. Critical input at the earliest stages of a project enables us to say in some cases, "no, we can't consider that for the following security reasons," or, more often, "yes, we can do that, but first the following security concerns need to be mitigated."

Many of the challenges in cybersecurity are cultural. Expanding two-factor authentication as "a way of life" is an example. In healthcare, it is essential that we become accustomed to verifying the identity of individuals accessing our networks. Achieving "buy-in" for these efforts is a major undertaking, as we seek to effect cultural change that modifies routine practices for 23,000 VUMC employees.

To effect the advantages of having IT Security at the management table, the support of the entire senior leadership team is essential to helping move culturally challenging practice changes into the organization. From expanding employee training to become continuous and routine, to regular communication to make visible the high volume of cybersecurity threats we face on a daily basis, we seek to help everyone at VUMC understand the critical role cybersecurity plays in assuring the safety of our patients.

*Special appreciation goes to **John F. Manning, Jr.**, PhD, MBA, Chief Operating Officer and Corporate Chief of Staff at VUMC, for his assistance with this commentary.*



> "Providing IT Security a direct reporting relationship to a board-appointed officer elevates cybersecurity to a seat at the highest management tables."

Randolph Hall, PhD // *Vice President of Research*

University of Southern California

In a recent survey*, 76 percent of healthcare security professionals reported that their organization had experienced a significant security incident in the past 12 months. To protect against such incidents, which range from the negligent insider who enables a data breach to national state actors, academic health centers should utilize technologies and strategies based on proven research.

At the University of Southern California (USC), our Information Sciences Institute has a 47-year history of research on the technologies underlying the internet (and its predecessor, the ARPANET), including creation of the Domain Name System, the Network Voice Protocol, and Grid Computing. Today, we study how to protect the internet and all of its components from threats.

Our approach has been three pronged: 1) studying behavior we observe and monitor in internet traffic; 2) simulating incidents within a controlled environment, through our DETER testbed; and 3) understanding human behavior that may cause or protect against security breaches. We have, for instance, pioneered techniques for detecting internet outages, as well as detection of denial-of-service attacks (in which a machine is maliciously overloaded by a flood of input); and we have developed standards for creating passwords that are both strong and memorable to users.

Our DETER testbed, supported by the Department of Homeland Security and the National Science Foundation, provides a unique national and international resource that emulates real-world complexity within a controlled environment so that sophisticated attacks might be simulated without harming the actual network. Within DETER, we provide modules for modeling human behavior, orchestrating network experiments, and coordinating experiments among multiple parties.

Cybersecurity is particularly challenging in academic health centers. We support a highly diverse user group, both internal and external, with demands for access and transparency that compete against privacy and security. Our information systems are critical to our operation (failures endanger health and safety), and we are both strictly regulated and subject to penalties when we fail to protect. We are also experiencing an explosion of new technologies that will interface with our systems, including patient wearables, point-of-care devices, and new imaging and "omic" equipment.

One thing for sure: cybersecurity cannot be ignored and requires staffing, education, proactive testing of vulnerabilities, and standards that are applied across the entire institution.

**2018 Health Information and Management Systems Society Survey.*

> "Academic health centers support a highly diverse user group with demands for access and transparency that compete against privacy and security."

Martin Paul, MD, PhD // *President*

Maastricht University

"Hello Nick, I have to make an international transfer as soon as possible, pay an invoice. Can you do that for me? Let me know, then I can send you the details immediately. Sincere, Martin Paul.
Reply to: Martin Paul <fred627ceo@mail.com>".

This email was recently sent to a colleague on my executive board, the Vice-President of Maastricht University. It was obviously crafted in Dutch and then translated in Google Translate—a typical case of CEO impersonation fraud.

Maastricht University faced the first CEO fraud attempt about two years ago, and it almost succeeded. Nowadays, my direct colleagues and our finance executives know exactly how to spot the red flags of CEO fraud. But the question is: how do we deal with all the other cybersecurity threats?

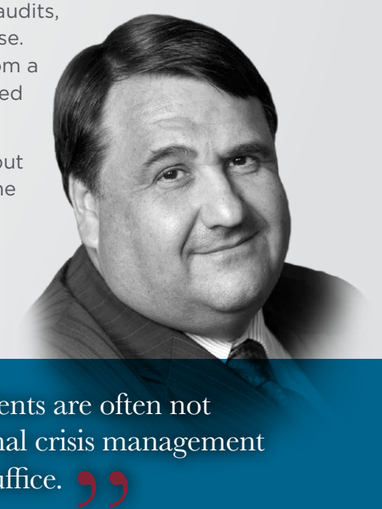
Besides CEO fraud, we face spam, phishing emails, DDos attacks, hack attempts, ransomware and even espionage. Unlike traditional safety and security threats, cyber-related incidents are often not manifest right away. When they are, it is usually unclear when or where they originated and which data, systems or networks are affected. Information about cyber-incidents is often sketchy or speculative. One reason is that victims face the additional risk of reputational damage. Therefore, traditional crisis management protocols will not suffice.

We follow three lines of defense against cybercrime. First: **Be prepared**—establish strategic policies (for example: "Never pay ransom") and an Enterprise Security Architecture. Second: **Be informed**—implement a Security Operations Center (SOC) to audit IT-systems, monitor traffic wand system use, detect anomalies, and perform threat intelligence. Third: **Be responsive**—implement a Computer Security Incident Response Team (CSIRT).

Most importantly: work closely together with your peers.

UM researchers work together with their hospital colleagues within Maastricht University Medical Centre (MUMC+), so we align our privacy and security measures and regulations. Dutch institutes on Higher Education and Research have joined forces with University Medical Centers in a national collaboration called SURF. SURF not only supplies our National Research Network, but also provides a coordinating role in flourishing communities supporting common security frameworks, audits, yearly threat analyses, and incident response. UM's Crisis Management highly benefits from a large bi-annual cyber-incident exercise called Ozon, co-ordinated by SURF.

CEO fraud has become business as usual, but cyber crisis management needs to be on the agenda for years to come.



> "Cyber-related incidents are often not manifest right away...traditional crisis management protocols will not suffice."