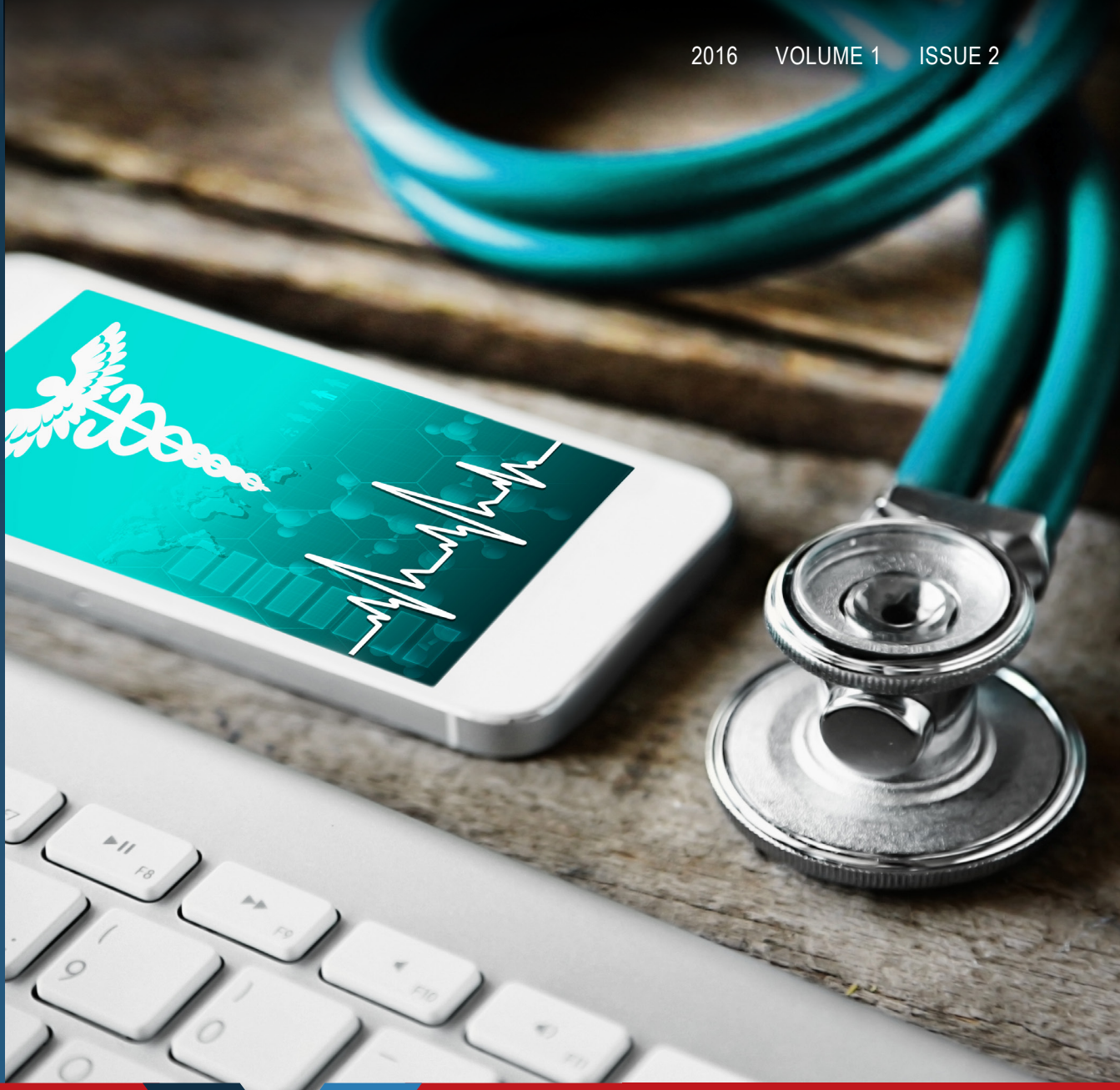
2016 VOLUME 1 ISSUE 2



the EXCHANGE

ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

TRACIE
HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

Welcome to Issue 2!

Welcome to the second issue of the ASPR TRACIE newsletter, *The Exchange*. Continuing with this year's theme "Critical Issues in Healthcare System Preparedness," this issue focuses on cybersecurity and cyber hygiene. ASPR TRACIE has been busy working closely with subject matter experts from all levels to bring readers the most current information on this incredibly pressing issue. But that's not all—we continue to release new Topic Collections and respond to a variety of requests for technical assistance. Our team relies on your feedback—please contact us with comments, questions, technical assistance needs, and to share resources. We look forward to our continued collaboration!

Shayne Brannman, Director,
ASPR TRACIE

John L. Hick, MD, Senior Editor

The ICF ASPR TRACIE Team:

Meghan Treber, Project Director
Audrey Mazurek, Deputy Project Director
Corina Solé Brito, Communications Manager and Technical Resources Lead
Bridget Kanawati, Assistance Center Lead
Jennifer Nieratko, Special Projects Manager

Foreword

"Another Hospital Victim of Cyberattack."

"Multiple Hospitals Hit in Ransomware Attack Wave."

Recently, we have all read headlines such as these, and some of you have no doubt been personally affected by recent cyber threats or actual attacks. No healthcare facility is immune to these threats and the significant impact an attack can have, particularly when all the information technology (IT) programs used to run daily operations are frozen. Healthcare and public health emergency managers play vital roles in coordinating consequence management once a cyberattack takes place. Before that, they should be helping reinforce to their facility staff basic cyber hygiene tactics. Although IT professionals are critical, the collaborative efforts between private and public agencies, local, state, and federal authorities are what make cybersecurity planning and consequence management successful. Simply put, cyberattacks are a crime. ASPR, through ASPR TRACIE, is pleased to highlight best and promising healthcare cybersecurity practices. This issue of *The Exchange* highlights lessons learned from a recent attack and features articles that demonstrate how collaboration at all levels is helping healthcare facilities implement practical, tangible steps to prevent, respond to, and recover from cyberattacks. The video "Cybersecurity and Healthcare Facilities" features subject matter experts describing the recent attack on MedStar, steps we can take to prevent and mitigate attacks, and what the federal government is doing to address cybersecurity. The Cybersecurity Topic Collection includes annotated resources reviewed and approved by a variety of subject matter experts. We hope this information makes your work easier and helps you secure your facility and data. Please don't hesitate to reach out to the ASPR TRACIE Assistance Center with additional best practices or ways you have addressed this issue, so others may benefit from your advances. Or if you require technical assistance or have questions about this topic, please send your inquiry to askasprtracie@hhs.gov. As always, we welcome your feedback.

Jessica Fantinato,
Deputy Director,
HHS/ASPR/Office of Emergency Management

At a Glance

Photo courtesy of HHS ASPR.

What's New With ASPR?

Much has happened since ASPR TRACIE published Issue 1 of *The Exchange*, which focused on Crisis Standards of Care (CSC). Dr. Lewis Rubinson shared his personal experiences treating Ebola patients in Sierra Leone in a newly-released video "Lessons Learned on Crisis Standards of Care in Kenema." Since our first newsletter, ASPR TRACIE has received and responded to numerous requests for CSC technical assistance, most recently strategies and guidelines for developing pre-hospital/emergency medical services plans. Dr. Nicole Lurie continues to head the federal response to the water crisis in Flint, MI. ASPR's Biomedical Advanced Research and Development Authority (BARDA) is supporting the collection of blood samples from people in the continental United States and Puerto Rico who have been infected with Zika virus (see also ASPR TRACIE's Zika: Resources at Your Fingertips). And as this newsletter was being finalized, ASPR was working closely with local, state, and federal partners to support the medical response effort to the mass shooting in Orlando, FL. On a lighter note, ASPR recognized six videos (out of nearly 100 applicants) on health preparedness submitted by young producers from across the country. The video judged "best overall entry" focused on how emergency preparations differ in Alaska, our nation's least densely populated state. For more information on how ASPR is working to strengthen the nation's ability to prepare for, respond to, and recover from emergencies, visit the ASPR webpage and blog!

ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

Lessons Learned from the MedStar Health System Outage: An Interview with Craig DeAtley, PA-C

(Commentary Provided by Dr. John L. Hick)

Abstract: *In the related ASPR TRACIE video "Cybersecurity and Healthcare Facilities," Craig DeAtley described the March 2016 cyberattack on the MedStar Health system, which comprises 10 hospitals, more than 250 outpatient centers, and more than 30,000 employees in Washington, DC, Maryland, and Virginia. In this interview with Dr. John Hick (ASPR TRACIE's Senior Editor), Craig expands upon certain points raised in the video, providing a more comprehensive overview of the incident, lessons learned, and the recovery process. He noted several challenges, including program integration and interconnectedness and newer staff needing to learn how to keep records using more traditional (i.e., not electronic) methods. Despite these challenges, Craig felt that the response worked well overall, as the hospital system had planned ahead, exercised regularly, and established solid working relationships with their information technology vendors.*

JH: Craig, you mentioned that over 370 programs were impacted by the ransomware. What were some of the most critical programs, and how did you overcome loss of access to the data?

CD: Overall, we grouped programs into one of four key categories:

1. Clinical (e.g., lab, radiological, medication orders);
2. Administrative (e.g., schedules for the operating rooms, for clinics, and staff; various forms, and phone directories);
3. Logistics (ordering and acknowledging receipt of routine items, including food and other materials [and related vendors]); and
4. Fiscal (to include paying staff, and accurately invoicing and paying vendors in a timely manner).

So many of these programs are integrated, and as they came

continued on page 3

ASPR TRACIE recently hosted a cybersecurity roundtable featuring: **Craig DeAtley** *(Director of the Institute for Public Health Emergency Readiness at the MedStar Washington Hospital Center) speaking about consequence management following the MedStar Ransomware Attack;* **Steve Curren**, *Director of ASPR's Resilience Division speaking about the cyber task force and the federal healthcare perspective on cybersecurity and cyber hygiene; and ICF International's Senior Vice President of Commercial Cybersecurity,* **Beth Musumeci** *discussing the critical steps healthcare entities can take to prevent cyberattacks. The panel was moderated by* **Dr. John Hick**.

continued from page 2

back up, we realized we needed a very clear understanding of each program and how they are linked with others. We also had to prioritize the programs, as it is not a good idea to try to restore them all simultaneously. In some cases, one program with a higher restoration priority was integrated with another program with lower priority; we recognized the need to be very flexible and set aside extra staff time for back-up/lag-time record keeping.

While healthcare facility staff know which programs they use daily (and would prioritize), this varies by specialty and category. In the case of MedStar, we all learned to be patient together. At a systems and facility perspective, we all now have much clearer and keener insight as to the interoperability and integration of our programs then we had at the outset of the attack.

"The integration and mutual respect are both important; so is trust from senior leadership."

JH: How robust was the cybersecurity annex of MedStar's emergency operations plan?

CD: There are two components of MedStar: standalone facilities, and the entire system they belong to. In addition to being part of the corporate emergency operations plan, cybersecurity was also part of each facility's hazard vulnerability assessment, and both had both been recently updated. Each facility had their own downtime procedure to fall back on, but this event reinforced the need to take a broader, more comprehensive look at cybersecurity and not just rely on 370 appendices (i.e., one for each program).

Lessons learned were two-fold. We are still in the process of after-action reporting and gleaning information from a number of approaches at the corporate and facility levels. For those facilities with a plan in place, we learned it could always be broader. Those who depended solely on down-time procedures realized the need for a broader approach.

Planners need to consider two primary audiences, as the layperson's understanding of the plan (and their related roles) will differ significantly from those with more technical expertise. A comprehensive plan would meet both of these needs and allow each person to pull out the section they need. MedStar will be reevaluating training to develop more creative ways to ensure that staff at all levels and specialties/assignments are as prepared as possible, and rely less on short, planned outages to ensure readiness.

JH: In our field, we know that IT professionals are not necessarily part of incident command, but they are critical to the response. Do you think healthcare systems know who to pull in when an attack occurs?

"We all learned to be patient together. At a systems and facility perspective, we all now have much clearer and keener insight as to the interoperability and integration of our programs than we had at the outset of the attack."

CD: This was a classic incident in which the IT professionals providing the technical expertise were critical in helping corporate and facility staff understand the scope of the problem, but were not necessarily in charge. Getting incident command to bring those disciplines together isn't always easy, but we did that—we have traditionally done that. Out of happenstance, foresight, or good luck, this experience reinforced that while IT/Information Systems personnel were not in charge, they had to be at the table. Another key takeaway from the event was the need for those at the table to be able to take a highly technical field with its own jargon and make it understandable to everyone else who has a response role. The integration and mutual respect are both important; so is trust from senior leadership.

continued on page 4

continued from page 3

"When you prepare with regularity, you come up with creative and time-proven solutions."

JH: Were any cybersecurity professionals on site? What was your relationship like before the event?

CD: There are staff you depend upon every day to keep the electronic system operational and react when problems are encountered. MedStar has staff at both the facility and corporate/system level. In events like this attack, the system's IT senior leadership worked closely with the vendors whose software was affected. Especially when we got into recovery mode, key vendors had a physical presence at corporate headquarters and local facilities to help the process along.

JH: How did you communicate about the event—both internally with staff and externally with patients and the public?

CD: Part of any incident revolves around initial notifications and alerts and we've become dependent on electronic systems to accomplish this. To address the challenge associated with these systems being inoperable, MedStar implemented several strategies. Corporate leadership held teleconferences two or three times a day with all command staff and leadership from individual facilities. Facility public information officers (PIOs) were part of a workgroup that met on a daily basis and drove the messaging, but all messages were ultimately approved by senior corporate leadership (not leadership from local facilities). Facility staff had in-person meetings with leadership once or twice a day to ensure information was being pushed out early and often. This was supplemented by patient rounding and hand-carried printed information.

To keep patients apprised of the computer repair process, healthcare providers increased daily rounding. Facility staff also printed simple update messages and placed them on patient's food trays. Staff also posted signs at facility entrances, acknowledging the problem without detailing it. These messages were meant to be reassuring without being overwhelming.

When communicating with the public (including the media), PIOs and others must take data security and privacy concerns (such as HIPAA), and public safety concerns into consideration. What you say to the public has to be tailored very carefully. Corporate MedStar staff carefully and selectively responded to information that was being released to the public through the media.

continued on page 5

continued from page 4

JH: In the video, you mentioned that some of the newer staff had a hard time using more traditional means of record keeping. How did you overcome that?

CD: A lot of credit goes to the mentorship of senior staff (those that had been there, seen this, done that) with helping newer staff adjust to using different tools to keep records. Their assistance was invaluable…they were willing to take care of their own responsibilities and help others. Pharmacists, nurses, respiratory therapists—staff from many departments stepped in to assist others. MedStar also used printed messages and instructions to supplement face-to-face meetings and messaging. Multiple strategies helped staff understand how MedStar was trying to help them work around the problems. In many cases, staff reported having a positive experience, noting that there was an avenue for them to quickly provide (often in-person) feedback through leadership to incident command.

"If there was one surprise, it was the rapidity with which we lost everything. The near immediacy and completeness of the loss was surprising. We were practiced at individual workarounds, but we had never prepared to lose everything."

"This wasn't a new experience for us. We've been working with the vendors for several years, so the relationship was solid. We also do system takedowns once if not twice a year for two to three days at a time. These do not impact daily operations, as we have backup systems that prevent the loss of any data. You need to have that tiered approach to team integration and solving the problem but you also need a tiered rehearsal of response to be successful."

JH: What surprised you most about the attack?

CD: There was no "aha" moment. We knew it could happen. It was part of our hazard vulnerability assessment, and we had discussed cybersecurity at meetings. If there was one surprise, it was the rapidity with which we lost everything. The near immediacy and completeness of the loss was surprising. We were practiced at individual workarounds, but we had never really rehearsed losing everything, much less all at once. Another compelling new experience was the amount of patience everyone needed and displayed while restoring the programs to ensure they did not miss any details or programming.

JH: What are the top three takeaways you think are imperative for healthcare facilities to incorporate into their cyber preparedness efforts?

CD:

1. Facilities need to know that it's going to happen and more than once. Make sure that you have a comprehensive plan that looks at all of the response issues associated with being locked out or someone getting into your system. The plan needs to address the messaging, logistics, and security implications of a total system outage. Furthermore, plans and roles will vary when facilities operate on their own versus as part of a corporate structure.
2. Rehearse this plan like you would any other. Note that exercising cyber plans may be more challenging than those for other hazards, as it has to be done at various levels within the facility, as well as within the system, if applicable. Rehearsing for one program at a time will not adequately prepare you. You need to exceed your comfort level to prepare for a problem this vast.

continued on page 6

continued from page 5

"Rehearsing for one program at a time will not adequately prepare you. You need to exceed your comfort level to prepare for a problem this vast."

Recognize that the response to a cyberattack is going to be an intense, stressful, extended operation that requires a skillful incident management team capable of running 24/7 for a period of time. Leadership has to be multidisciplinary and multi-level, and will need to flex the plan to adjust to the nuances of each situation. Record keeping and clear, concise internal and external communication is critical to a solid response.

Recovery is a marathon. While MedStar is 99% back in service, some of the individual files that were locked may never be reopened. As is the case in cyberattacks, the system went down a whole lot faster than it's going to come back up.

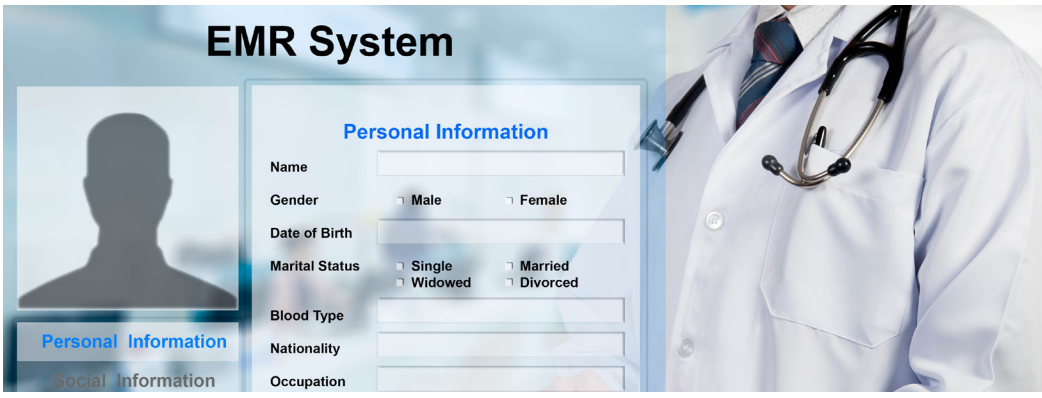
Dr. Hick comments: We're grateful to Craig for sharing his experiences. EVERY healthcare facility and system is at risk of cyber events that may vary from a denial of service attack on a switchboard to a ransom-driven attack on an electronic health record. These attacks will cause systems failures without any warning, so line personnel must be able to move to downtime procedures right away. Furthermore, IT personnel will have to do a very rapid situation analysis to determine the specifics of the threat. This may require shutting down additional systems – and these decisions may have to be made very rapidly, so the authority needs to be determined before an event.

Also, while IT staff have the technical expertise, the overall incident decisions have to be part of an incident command process – implementing and modifying downtime procedures, communicating (when many modes of usual communication may be down), and prioritizing system restoration (as well as making decisions about any ransom!) has to be performed in addition to the technical aspects of getting the system running. As with any incident, an all-hazards approach is key to success.

Despite careful attention on the user end (not opening suspect files/links) and the system end, these type of attacks are nearly certain to continue and increase in sophistication. Having a plan to recognize and respond to these events is just as important to maintaining facility operations as any utility failure plan or disaster plan. As always, there is no substitute for having a back-up system that staff are familiar with and that works. ■

Craig DeAtley, PA-C, currently serves as the Director of the Institute for Public Health Emergency Readiness at the MedStar Washington Hospital Center and co-shares the responsibility for facilitating MedStar Health emergency management activity.

John Hick, MD, serves as ASPR TRACIE's Lead Editor on detail from HHS/ASPR. He is an Emergency Physician and Deputy Chief EMS Medical Director at Hennepin County Medical Center in Minneapolis, MN, and a Professor of Emergency Medicine at the University of Minnesota.



A Culture of Health Information Security

Contributed by Chantal Worzala, Ph.D., MPA

The healthcare field is increasingly realizing the promise of networked information technologies to improve patient quality and safety and bring efficiencies to our business systems. But with those opportunities come vulnerabilities to theft and threats to the security of personal data for patients and employees, billing records—even the function of medical devices. Increasingly, bad actors are using phishing emails, malicious malware, and other tactics to attack hospital computers, networks, and connected devices.

While no economic sector is immune from attacks, criminals increasingly seek to infiltrate critical hospital infrastructure and information systems. These attackers have many different motives. Most recently, we have heard of ransomware attacks, where the motive is primarily financial. A criminal infiltrates a system, unleashing decryption software that locks down a single computer, or even an entire network, and then demands a ransom payment to provide the encryption key to restore the data. Other attacks may be motivated by a desire to steal data from a system, such as individual medical, financial, or identity data that can monetized. In some cases, healthcare organizations may have intellectual property that is of interest to others, such as clinical trial data, or high-profile patients that are of interest to one group or another.

Regardless of the motivations of the bad actors, hospital and health system leaders must take these cybersecurity challenges seriously because protecting patients and their personal data is a 24-7, year-round responsibility. However, cybersecurity is more than just an information technology (IT) issue—it requires an organization-level risk reduction and response plan, leadership support and board oversight, and vigilance from everyone with access to the network. These efforts depend on hospital executives and technology staff, and involve the entire hospital team. In short, it is important that healthcare leaders instill and support a culture of security for health information within their organizations, parallel to the culture of safety for clinical care.

Entities within the healthcare field are working to continuously defend and improve the security of their networks by implementing safety measures, testing, maintaining back-ups, and deploying the latest upgrades. They are also encrypting networks and workstations. Many hospitals conduct an annual threat assessment and work to identify vulnerabilities through extensive penetration testing. Increasingly, hospitals and health systems are conducting table top exercises or other simulations to assess their readiness to respond in the event of an actual attack.

continued on page 8

continued from page 7

Figure 1 illustrates some of the specific cybersecurity measures being implemented by hospitals. It is important to remember, however, that an organization can be doing everything right and still fall victim to a cyber-attack because the tactics are constantly changing and new threats emerging.

Figure 1. Cybersecurity Measures Implemented by Hospitals[1]

Most Wired Survey Tracks Hospital Use of Important Cybersecurity Measures (Sponsored by Hospitals & Health Networks)			
Measure	Share of hospitals implementing measure:		
	More than 90%	More than 80%	More than 70%
Unique identification of system users	✓		
Automatic logoff of system users	✓		
Require use of strong passwords	✓		
Passcodes for mobile devices	✓		
Use of intrusion detection systems		✓	
Encryption of wireless networks		✓	
Encryption of laptops and/or workstations	✓		
Encryption of removable storage media			✓
Encryption of mobile devices			✓
Mobile device data wiping	✓		
At least annual risk analysis to identify compliance gaps and security vulnerabilities	✓		
At least annual infrastructure security assessment	✓		
Security incident event management			✓

[1]Recreated with permission from the American Hospital Association.

continued on page 9

continued from page 8

Addressing these growing cybersecurity challenges therefore requires active information sharing, so that organizations can stay ahead of emerging cybersecurity risks and contribute to collective knowledge of threats to guard against. Several private sector entities, such the Nation's Healthcare and Public Health Information Sharing and Analysis Center, (NH-ISAC) and Health Information Trust Alliance (HITRUST), provide information-sharing opportunities. In addition, the federal government has provided information-sharing resources through its cybersecurity initiatives, which include healthcare facilities and law enforcement agencies. The federal government also is working to provide more educational and other resources to the healthcare field. The recently formed Healthcare Industry Cybersecurity Task Force is charged with better understanding the cyber needs of the healthcare field and identifying helpful resources. These steps are critically important, as are measures to identify, disrupt and apprehend the bad actors. As a nation, we must bolster the security of our ecosystem, not just place the burden on individual institutions.

For its part, the American Hospital Association has a dedicated cybersecurity webpage that includes many resources that can help hospital leaders better understand cybersecurity threats and incorporate cyber risk reduction and response into their strategic priorities. The webpage also includes links to recent cybersecurity alerts. We have also developed resources on specific topics, such as what to do when an attack happens, the importance of staff training, and ransomware.

We also work in close partnership with HHS/ASPR, the FBI, the FDA, and other federal partners. Cyber threats will continue, but ongoing vigilance by the healthcare field and active pursuit of bad actors by law enforcement can mitigate the problem. ■

Chantal Worzala Ph.D., MPA, currently serves as the American Hospital Association's Vice President for Health Information and Policy Operations.

Related AHA Resources

Webinar Replay: What Health Care Leaders Need to Know to Adopt and Use NIST's Cybersecurity Framework in Health Care

Audiocast: Ransomware - Emerging Cybersecurity Risk for Health Care Organizations

A message from the AHA on cybersecurity: What hospitals need to know about ransomware

Protecting Medical Devices from Cyber Threats: An Update from the FDA

Contributed by Suzanne B. Schwartz, MD, MBA

Most of us have benefited from the improvements and efficiencies in healthcare that have evolved over the past decade. Information flows more freely and monitors are digitally calibrated to alert healthcare providers and hospital staff of some of the smallest changes in patient status.

But with this increase in efficiency comes new kinds of threats. As medical devices have become more interconnected and interoperable, they pose new cybersecurity risks.

Some medical devices, like computer systems, can be vulnerable to security breaches, potentially affecting the safety and effectiveness of the device. And, as medical devices are increasingly interconnected via the Internet, hospital networks, other medical devices, and smartphones, the risk and effect of cybersecurity breaches reverberates throughout this system.

Recent cybersecurity vulnerabilities could have directly affected medical devices or hospital network operations, including:

- Network-connected/configured medical devices infected or disabled by malware;

- The presence of malware on hospital computers, smartphones and tablets, targeting mobile devices using wireless technology to access patient data, monitoring systems, and implanted patient devices;
- Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel);
- Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices); and
- Security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access, such as plain-text or no authentication, hard-coded passwords, documented service accounts in service manuals, and poor coding/SQL injection.

continued on page 11

continued from page 10

The U.S. Food and Drug Administration (FDA) encourages medical device manufacturers to carefully consider possible cybersecurity risks while designing medical devices and to have a plan to manage system or software updates. By focusing on cybersecurity during the design phase, manufacturers can reduce the vulnerability in their medical devices.

The FDA released a final guidance in October 2014, titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," which identifies cybersecurity issues that manufacturers should consider while preparing premarket submissions for medical devices in order to maintain information confidentiality, integrity, and availability. It also recommends that manufacturers submit documentation to the FDA about the risks identified and controls in place to mitigate those risks, as well as submit their plans for providing patches and updates to operating systems and medical software.

But premarket considerations are only one aspect of medical device cybersecurity. While manufacturers can incorporate controls in the design of a product to help prevent these risks, it is essential that manufacturers also consider improvements during maintenance of devices, as the evolving nature of cyber threats and emergence of newly identified vulnerabilities means risks may arise throughout a device's entire lifecycle.

In January 2016, the FDA issued draft guidance for medical device manufacturers that outlines postmarket recommendations for medical device manufacturers, including the need to proactively plan for and to assess cybersecurity vulnerabilities—consistent with the FDA's Quality System Regulation. A big part of effective cybersecurity is creating a proactive approach and fostering multi-stakeholder collaboration, which will help stay ahead of cybersecurity threats and protect patients. In this respect, the FDA stresses in the draft guidance the importance of information sharing via participation in an Information Sharing Analysis Organization (ISAO), a collaborative group in which public and private-sector members share cybersecurity information, including threats and vulnerabilities.

continued on page 12

"It is essential that manufacturers also consider improvements during maintenance of devices, as the evolving nature of cyber threats and emergence of newly identified vulnerabilities means risks may arise throughout a device's entire lifecycle."

continued from page 11

The draft guidance recommends that manufacturers should implement a structured, systematic, and comprehensive cybersecurity risk management program and respond in a timely fashion to identified vulnerabilities. Critical components of such a program should include:

- Applying the 2014 National Institute for Standards and Technology voluntary Framework for Improving Critical Infrastructure Cybersecurity, which includes the core principles of "Identify, Protect, Detect, Respond and Recover;"
- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Understanding, assessing, and detecting presence and effect of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Clearly defining essential clinical performance to develop mitigations that protect, respond, and recover from the cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and
- Deploying mitigations that address cybersecurity risk early and prior to exploitation.

In order to spur the creation of proactive programs, the FDA considers most actions taken by manufacturers to address cybersecurity vulnerabilities and exploits as "cybersecurity routine updates or patches." This means that the FDA does not require advance notification, additional premarket review, or reporting under its regulations. For a small subset of cybersecurity vulnerabilities and exploits that may compromise the essential clinical performance of a device and present a reasonable probability of serious adverse health consequences or death, the FDA would require medical device manufacturers to notify the agency.

In addition, the FDA indicates in this draft guidance that in cases where this type of "uncontrolled" vulnerability is quickly addressed in a way that sufficiently reduces the risk of harm to patients, the FDA does not intend to enforce urgent reporting of the vulnerability to the agency if certain conditions are met:

- There are no serious adverse events or deaths associated with the vulnerability;
- Within 30 days of learning of the vulnerability, the manufacturer notifies users and implements changes that reduce the risk to an acceptable level; and,
- The manufacturer is a participating member of an ISAO and reports the vulnerability, its assessment, and remediation to the ISAO.

The FDA issued the draft guidance in January 2016, and the 90-day public comment period has closed. FDA staff is reviewing all public comments and will finalize the guidance as quickly as possible.

The FDA's mission is to protect and promote public health. We believe that our proactive measures to inform device manufacturers of our expectations can help prevent, limit, and mitigate the potential of exploitation of cybersecurity vulnerabilities in medical devices. These steps will not only encourage innovation in medical device security but protect patients over the long term. ■

Suzanne B. Schwartz, MD, MBA, currently serves as the Associate Director for Science and Strategic Partnerships and the Acting Director for Emergency Preparedness/Operations & Medical Countermeasures, in the Office of the Center Director, Center for Devices & Radiological Health, U.S. Food and Drug Administration, U.S. Department of Health and Human Services.

About the HHS Health Care Industry Cybersecurity Task Force

Contributed by Emery Csulak, PMP, CISSP

On March 17, 2016, the U.S. Department of Health and Human Services (HHS) Health Care Industry Cybersecurity Task Force officially launched, with 21 members who represent healthcare industry stakeholders, cybersecurity experts, and federal agencies. The Task Force was established in support of Section 405 of the Cybersecurity Act of 2015 and to help identify opportunities for improving cybersecurity in the healthcare industry. Also at this time, national news was buzzing with stories regarding ransomware attacks at notable organizations such as Hollywood Presbyterian Medical Center in California and MedStar in Washington, DC. The Task Force is looking forward to the opportunity to help the healthcare industry understand, prepare for, and respond to cybersecurity challenges.

Key Activities of the Task Force

With over 1 million health care providers serving the United States, the industry reflects a wide range of organizations from large multi-billion dollar enterprises to small offices, such as a local dentist. The challenges this creates in educating and resourcing cybersecurity are enormous. The overall goal of the Task Force is to ensure continuous delivery of healthcare services by ensuring secure and reliable services. One aspect of ransomware, as an example of a security challenge, is the potential loss of access to medical records by staff. For some in the industry, this may be a mere inconvenience during routine services. However, for some medical professionals, the inability to access to Electronic Health Records (EHR) may directly affect the timely identification and resolution of a serious medical condition.

In the News: Recent Articles on Cybersecurity and Healthcare Facilities

Hackers Offering Bulk Discount to Unlock Encrypted MedStar Data

Infographic: Top 10 Cybersecurity Threats of the Future

Why Hospitals are the Perfect Targets for Ransomware

Ponemon: 89 Percent of Healthcare Entities Experienced Data Breaches. Healthcare IT News.

continued on page 14

continued from page 13

The following key Task Force activities stem from the legislation:

- Analyze how other industries have implemented strategies and safeguards for addressing cybersecurity threats;
- Analyze challenges and barriers private entities face securing themselves against cyber-attacks;
- Review challenges in securing networked medical devices and other software connected to EHR;
- Provide and disseminate information to healthcare industry stakeholders of all sizes for the purpose of improving preparedness for, and response to, cyber threats and attacks;
- Establish a plan to implement real-time, actionable threat indicators and defensive measures with healthcare industry stakeholders; and
- Report to congressional committees on the findings and recommendations of the Task Force.

Why was the Task Force Formed?

Regardless of the increased visibility of cybersecurity threats, many organizations are not prepared, either due to lack of knowledge, limited resources, or other reasons. The Task Force was formed to learn from other industries and adapt best practices to the healthcare sector. For example, one effective strategy used by other industries includes engaging chief executive officers (CEO) in understanding the cyber threats facing their business.

By providing information to industry stakeholders, the Task Force seeks to emphasize that cyber hygiene is everyone's responsibility. Regardless of the hacker's intent, the disruption of any component of the healthcare delivery model can lead to unintended (possibly catastrophic) consequences. From preventing the access to healthcare records to disrupting the timely arrival of an ambulance—cyberattacks can directly affect a patient and a facility—simultaneously.

Discussing the Challenges

The Task Force routinely discusses the evolving cybersecurity challenges facing the healthcare sector to help inform the communication strategy moving forward. Some of the challenges discussed to date have included:

- The need for leadership to start the conversation regarding cybersecurity. Without CEO engagement, cybersecurity is unlikely to succeed.
- Legal issues associated with the supply chain (e.g., unmanaged supply chain risk).
- Prioritizing resources for cybersecurity in light of decreasing healthcare profit margins.
- The perception that sharing data in healthcare is equivalent to "losing patients."
- Overcoming the assumption that security is someone else's responsibility and IT can simply "come in and clean up."

Through the next several months the Task Force will be working with their respective communities to examine these and other challenges.

"…cyber hygiene is everyone's responsibility. Regardless of the hacker's intent, the disruption of any component of the healthcare delivery model can lead to unintended (possibly catastrophic) consequences."

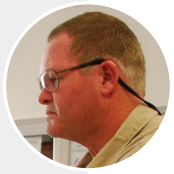
Summary

Healthcare and healthcare delivery are evolving. So, too, is the threat of a cyberattack. The risk of hackers and the potential their activities have to disrupt care delivery will only increase. The Task Force will continue to meet monthly to discuss with partners and other experts how to best message about cybersecurity to ensure they share the best, most timely ideas with the healthcare sector. ■

Emery Csulak, PMP, CISSP, currently serves as the Chief Information Security Officer/Senior Official for Privacy at the Centers for Medicare & Medicaid Services.

RECOMMENDED RESOURCES

TR TECHNICAL RESOURCES



Cybersecurity

The resources in this Topic Collection can help stakeholders better protect against, mitigate, respond to, and recover from cyber threats, ensuring patient safety and operational continuity. https://asprtracie.hhs.gov/technical-resources/86/Cybersecurity/86

Virtual Medical Care

This Topic Collection highlights lessons learned from recent events and strategies for implementing virtual medical care during a disaster. https://asprtracie.hhs.gov/technical-resources/55/Virtual-Medical-Care-telemedicine-nurse-triage-lines/55

AC ASSISTANCE CENTER

ASPR TRACIE recently hosted a roundtable with subject matter experts titled "Cybersecurity and Healthcare Facilities." Speakers shared lessons learned from the recent attack on MedStar Health, general information about cyberattacks and cyber hygiene, and the collaborative effort being taken by the federal government to address this threat.

You can access a summary sample of TA requests, which range from providing individuals with topic-specific resources (e.g., hazard vulnerability assessments) to researching and providing individuals with topic-specific resources (e.g., coalition supply cache lessons learned, hospital stockpiling resources, crisis standards of care).

IE INFORMATION EXCHANGE

Check out the Information Exchange!

Register for the ASPR TRACIE Information Exchange, where you can click on the Cybersecurity thread and share your opinions and resources with your colleagues. Already have an account? Simply log in and share your feedback! Need help registering for the Information Exchange? Access our quick tutorial here.

New: Access redacted requests for CSC technical assistance, most recently specific to state-level strategies for developing and implementing CSC and CSC guidelines for pre-hospital/emergency medical services.

OTHER RESOURCES

Dr. Lewis Rubinson shared his personal experiences treating Ebola patients in Sierra Leone in a newly-released video "Lessons Learned on Crisis Standards of Care in Kenema."

New: We invite you to access and comment on the Draft ASPR TRACIE report "Current and Future Healthcare Trends and their Impact on Disaster Preparedness."

UPCOMING 2016 EVENTS

July

July 14, 2-3 pm EST; Virtual Webinar
Healthcare Coalition Engagement in Mass Gathering Events

Join the ASPR TRACIE webinar on the role of healthcare coalitions in planning for and executing health and medical services during mass gatherings.

July 17-19; San Diego, CA
Health Forum and the American Hospital Association Leadership Summit

This event offers leaders in healthcare the opportunity to discuss the issues facing their organizations and network to learn more about promising practices.

July 19-21; Phoenix, AZ
NACCHO Annual 2016

This conference offers local health department staff, partners, funders, and individuals interested in local public health the chance to share information around the theme "Cultivating a Culture of Health Equity."

August

August 29-September 1; Miami, FL
18th International Society for Burn Injuries (ISBI) Congress

This year's event focuses on "Guiding Burn Care in Lower and Middle Income Countries." Be sure to visit the ASPR BARDA booth and look for the BARDA/OEM/MSCR poster featuring ASPR TRACIE!

September

September 8; Rockville, MD
Disaster Health Education Symposium

Look for ASPR TRACIE at this symposium, sponsored by The National Center for Disaster Medicine and Public Health. Learn more about our resources and the various types of technical assistance we can provide.

September 20-22; Minneapolis, MN
2016 ASTHO Annual Meeting and Policy Summit

This event offers the opportunity for healthcare and public health leaders to network and share best practices.

December

December 13-14; Washington, DC
National Healthcare Coalition Preparedness Conference

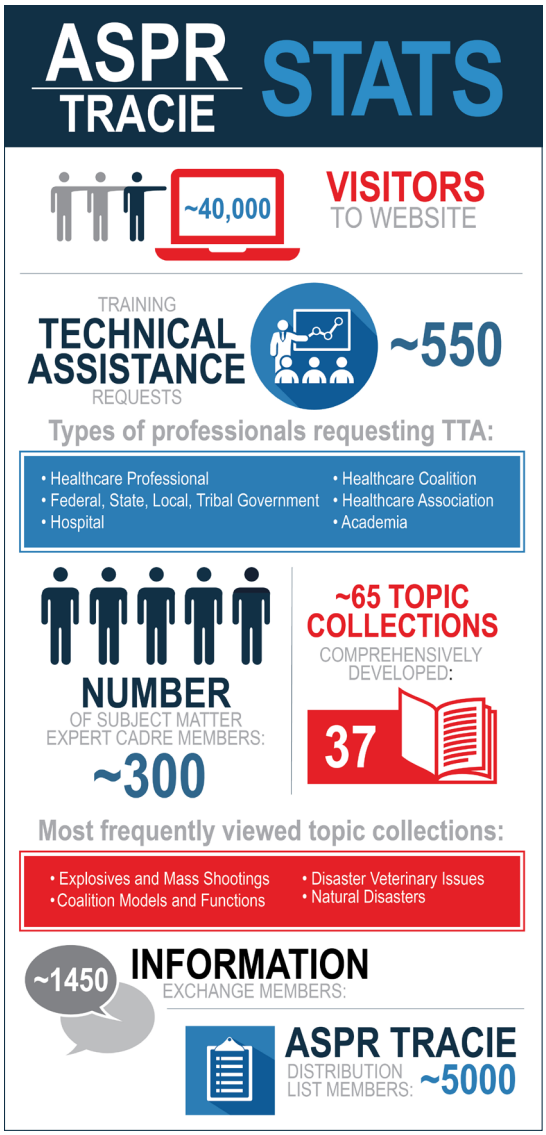
This independent conferences "exists for coalitions, by coalitions," and presents opportunities for members to learn about the implementation of healthcare coalitions and coalition activities.

ASPR TRACIE:

Your Healthcare Emergency Preparedness Information Gateway

The Exchange is produced by the Office of the Assistant Secretary for Preparedness and Response (ASPR) Technical Resources, Assistance Center, and Information Exchange (TRACIE). Through the pages of *The Exchange*, emergency health professionals share firsthand experiences, information, and resources while examining the disaster medicine, healthcare system preparedness, and public health emergency preparedness issues that are important to the field. To receive *The Exchange*, please go to ASPR TRACIE's homepage (**https://asprtracie.hhs.gov/**), and enter your email address in the "Subscribe to the ASPR TRACIE Listserv" box on the bottom right.

ASPR TRACIE was created to meet the information and technical assistance needs of ASPR staff, healthcare coalitions, healthcare entities, healthcare providers, emergency managers, public health practitioners, and others working in disaster medicine, healthcare system preparedness, and public health emergency preparedness. The infographic illustrates ASPR TRACIE's reach since launching in September 2015.



ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

TRACIE
HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

CONTACT US

ASPR TRACIE

Toll-Free: 1-844-587-2243

askASPRtracie@.hhs.gov

https://asprtracie.hhs.gov