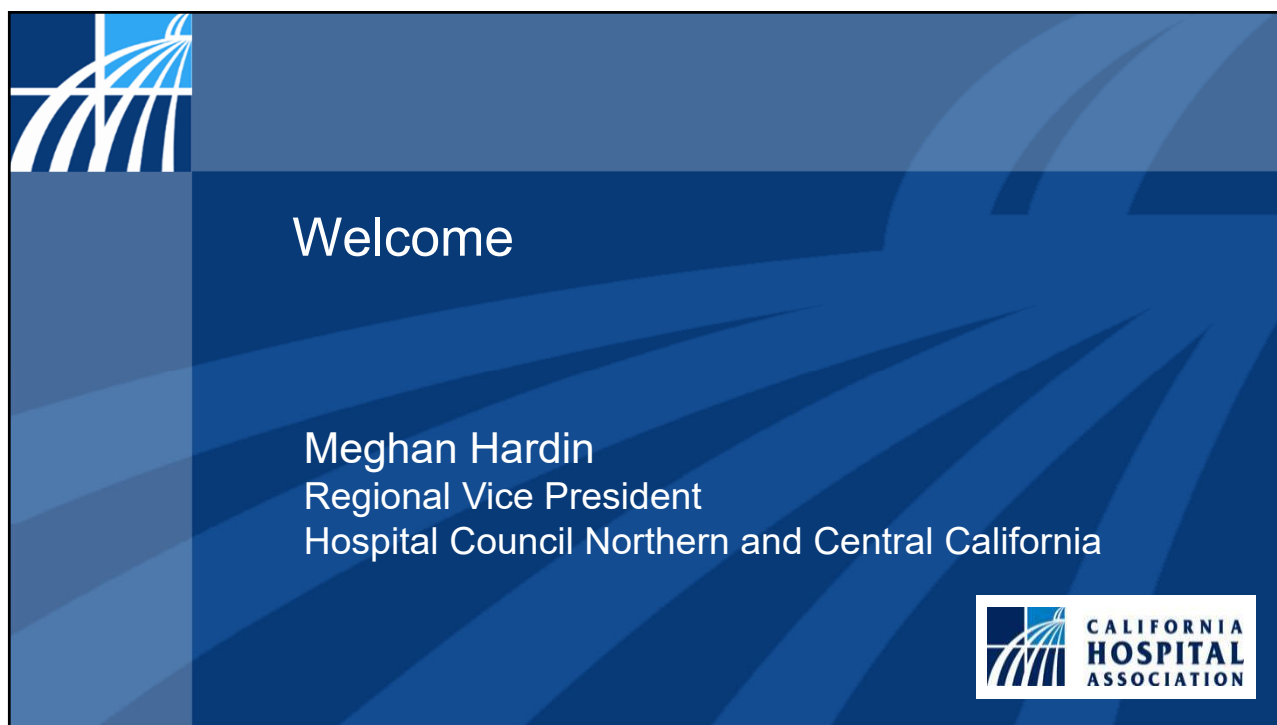
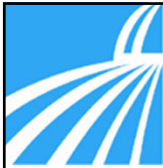




1



2



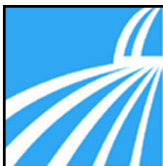
Continuing Education

Continuing education credits are offered for this program or application has been made for compliance, health care executives, legal, nursing and risk managers.

Full attendance and completion of the online evaluation and attestation of attendance are required to receive CEs for this webinar.

3

3



Questions

Online questions will be taken throughout the presentation.

Please type your question in the Q&A box at the bottom of your screen, press enter.

4

4



Polling Question #1

5

5



Polling Question #2

6

6



Faculty



John Riggi is the first Senior Advisor for Cybersecurity and Risk for the American Hospital Association and their 5000+ member hospitals. John leverages his nearly 30 years with the FBI and CIA in the investigation and disruption of cyber threats, international organized crime and terrorist organizations to assist on policy and advocacy issues. His trusted access to hospital leadership and government agencies enhances John's national perspective and ability to provide uniquely informed risk advisory services.

7

7




Faculty




Kelly Mather joined BayHealth Development in 2020. Previously, Kelly was the President/CEO of Sonoma Valley Hospital. Starting in 2010, Kelly led the revitalization of the hospital where she created a values based culture with excellent quality and satisfaction results, oversaw extensive upgrades in the facility, raised over \$35 million with the hospital foundation, affiliated with UCSF Health and improved the financial stability of the organization.

8

8




Faculty




Tamra Durfee is the Director of Technology at Enloe Medical Center in Chico, CA. Tamra is an innovative and experienced IT Professional whose background includes Information Security, IT Architecture, and Project Management. She developed and implemented an enterprise-wide information and medical device security program to preserve the availability, integrity and confidentiality of hospital information resources.

9

9





Ransomware and Emerging Cyber Threats: A National Perspective



John Riggi, Senior Advisor for Cybersecurity and Risk Advisory Services, AHA

2/11/2021

10

Hacking Incidents Reported to OCR in 2020

**368 Breaches Under Investigation Impacting
19.2 Million Individuals**

57 Resolved Breaches Impacting 7.5 Million Individuals

**Total 2020 = 425 Breaches Impacting 26.7 Million
Individuals**

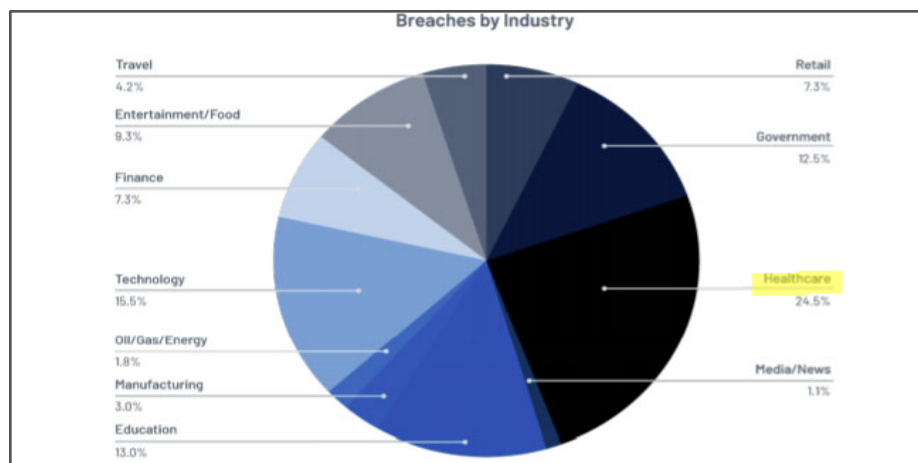
Source : HHS, OCR website data accessed 1/11/2021 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf Image:
Naked Security -Sophos



Riggi -
11

©2021 American Hospital Association -

11

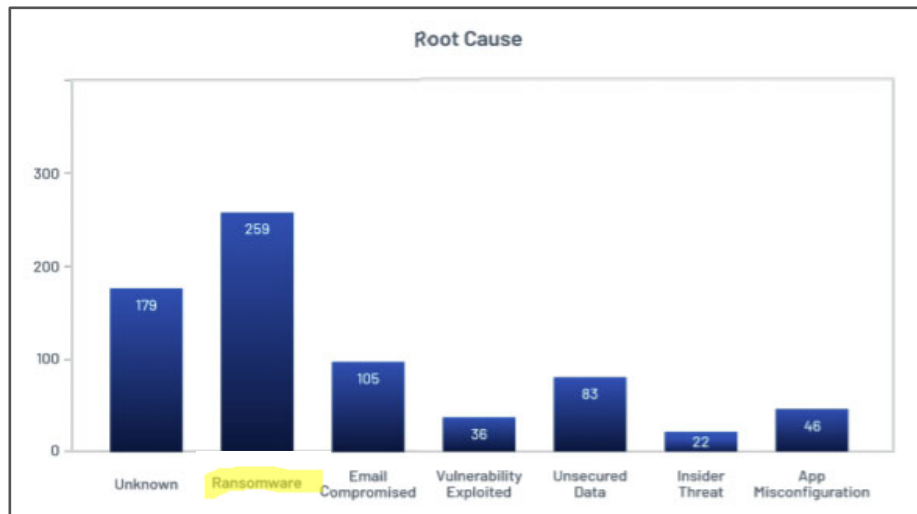


Research by Tenable 2020 Threat Landscape Feb. 2021

Riggi -
12

©2021 American Hospital Association -

12



Research by Tenable 2020 Threat Landscape Feb. 2021

Riggi -
13

©2021 American Hospital Association -

13

COVID-19 Induced Cyber Triple Threat - Cyber Criminals Exploiting a Crisis

Threat 1: Expanded Attack Surface


- Rapid Expansion and Deployment of network and internet connected technologies
- Connected Medical Devices and Ventilators, remote monitoring to save PPE
- Telehealth and Telemedicine
- Telework
- Cloud Services



Riggi -
14

©2021 American Hospital Association

14



GUIDANCE FOR SECURING VIDEO CONFERENCING

This product is for organizations and individual users leveraging videoconferencing tools, some of whom are remotely working for the first time.

As the authority for securing telework, the Cybersecurity and Infrastructure Security Agency (CISA) established this product line with cybersecurity principles and practices that individuals and organizations can follow to video conference more securely. Although CISA is providing this general risk advisory guidance, individuals and organizations are responsible for their own risk assessments of specific systems and software. For optimum risk mitigation, organizations should implement measures at both the organizational and user levels.

BACKGROUND

- The Federal Government, state and local governments, the private sector, and general public have pushed to embrace remote work and online collaboration.
- Video conferencing has emerged as a pervasive tool for business continuity and sustained social connection. Although increased network and online collaboration tools provide necessary capabilities, video conferencing has increased the attack surface exploited by malicious actors.
- Once niche products, many of these tools were created for a subset of the business community and were not scaled for cross-domain usage. Entire industries, sectors, and stakeholder sets and how profoundly dependent on online tools—simultaneously.
- Avoid the unanticipated exponential growth and unprecipitated popularity of these platforms. Many video conferencing users have not implemented necessary security precautions—or might be unaware of the latent risks and vulnerabilities.

FOUR PRINCIPLES AND TIPS TO SECURE VIDEO CONFERENCING


1. CONNECT SECURELY

Risk: The initial settings for home Wi-Fi networks and many video conferencing tools are not secure by default, which—if not changed—can allow malicious actors to compromise sensitive data while you work from home.

Mitigation: Change default passwords for your router and Wi-Fi network. Check that you are using Wi-Fi encrypted with WPA2 or WPA3. Verify your video conferencing security settings and use encrypted video conferencing tools whenever possible.

Tips: Here are some simple actionable tips for connecting securely at home.

- Change default password to strong, complex passwords for your router and Wi-Fi network.
- Choose a generic name for your home Wi-Fi network to help mask who the network belongs to, or its equipment manufacturer.
- Ensure your home router is configured to use WPA2 or WPA3 wireless encryption standard at the minimum, and that legacy protocols such as WEP and WPA are disabled. See CISA's Tip on [Home Network Security](#) for additional information.



Health Information Privacy

U.S. Department of Health & Human Services

HIPAA for Individuals

Filing a Complaint

HIPAA for Professionals

Newsroom

Notification of Enforcement Discretion for telehealth remote communications during the COVID-19 nationwide public health emergency

We are empowering medical providers to serve patients wherever they are during this national public health emergency. We are especially concerned about reaching those most at risk, including older persons and persons with disabilities. – Roger Severino, OCR Director.



Attacks on Connected Medical Devices

What is an Attack on Connected Medical Devices?

The Food and Drug Administration (FDA) defines a medical device as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them, intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease."

Real-World Scenario:

A threat actor gains access to a care provider's computer network through an e-mail phishing attack. He proceeds to take command of a file server to which a heart monitor is attached. While scanning the network for devices, the attacker takes control (e.g., power off, continuously reboot) of all heart monitors in the ICU, putting multiple patients at risk.

IMPACT

Patients are at great risk because an attack has shut down heart monitors, potentially during surgery and other procedures.

How Can HICP Help?

The publication, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in managing the current most pertinent cybersecurity threats to the sector. The material on this flyer is a section of the publication that examines cybersecurity threats and vulnerabilities that affect the healthcare industry.

Riggi – 15

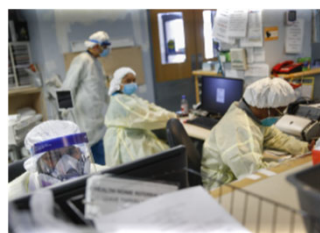
©2021 American Hospital Association

15

COVID-19 Induced Cyber Triple Threat - Cyber Criminals Exploiting a Crisis (cont.)

Threat 2: Increased Attacks

- Up to a 700% increase in phishing emails, including BEC
 - ✓ MFA, Email ATP, Verbal Authentication – Education!
- Attacks on devices and remote network vulnerabilities
 - ✓ Network/Device Mapping, Inventory, Security and Patching
- Business Associate and Cloud Attacks
 - ✓ Data Mapping, Vendor Risk Management Program, BAA, Cyber Insurance
- Ransomware Attacks – Patient Care and Safety Issue!**
 - ✓ Redundant Offline Backups, Patching, Incident Response Plan and Exercise
- Theft of COVID Related Research, Treatment Protocols and Vaccine Research
 - ✓ Risk Management Program to Identify Risk and Protect Research and Preserve Government Funding



Riggi – 16

©2021 American Hospital Association

16

Coronavirus Themed E-mail Phishing
Health Sector Cybersecurity Coordination Center (HC3)
HC3@HHS.GOV
Date: February 3, 2020



Recently, malicious cyber threat actors have been leveraging the current news cycle to launch Coronavirus themed cyberattacks at their targets. Prominent news reporting and the resulting elevated concern for the Coronavirus issue is being used as context for a malicious email phishing campaign. The phishing emails contain links to malware that is frequently used to target healthcare organizations and their IT systems.

Attempting to exploit human greed, fear, and curiosity are common tactics among phishing campaigns – malicious e-mails deliberately crafted to entice the recipient to click a link or open an attachment in the e-mail which, while appearing helpful, compelling, or interesting, actually contains malicious code. Victims who interact with malicious links or attachments may expose their systems, networks, and valuable information. These exposures allow an attacker to use infected systems as a platform to phishing campaign is attempting to exploit illness currently in the news and for these Coronavirus themed phishing malware. At least one campaign for Disease Control and target Am

WANTED BY THE FBI

CHINA MSS GUANGDONG STATE SECURITY DEPARTMENT HACKERS

Unauthorized Access; Conspiracy to Access Without Authorization and Damage Computers; Conspiracy to Commit Theft of Trade Secrets; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

Li Xiaomeng Deng Xuebin

CAUTION

On July 7, 2020, a grand jury in the United States District Court for the Eastern District of Washington indicted Li Xiaomeng and Deng Xuebin for their alleged participation in a long-running campaign of cyber network operations targeting the networks of critical infrastructures and large companies across a wide variety of industries, including high-tech manufacturing, civil, health, and medical device engineering, business, educational, and gaming software, state energy, pharmaceuticals, and defense. The indictment highlighted Li and Deng's alleged actions, including a recent focus on COVID-19 research, testing, and treatment; the targeting of political dissidents, religious minorities, and human rights advocates in mainland China, Hong Kong, the United States, and Canada; and the exfiltration into corporate networks of documents in Europe and Asia.

Some of Li and Deng's network operations were allegedly undertaken for their own economic benefits, while others were allegedly for the benefit of China's Ministry of State Security (MSS), including the Guangdong State Security Department.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Seattle www.fbi.gov

**NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY**

MITIGATING RECENT VPN VULNERABILITIES

ACTIVE EXPLOITATION

Multiple Nation State Advanced Persistent Threat (APT) actors have weaponized CVE-2019-11510, CVE-2019-11539, and CVE-2019-13379 to gain access to vulnerable VPN devices.

In August, 2019, the Canadian Centre for Cyber Security released guidance for mitigating vulnerabilities in 3 major VPN products (Pulse Secure®, Palo Alto GlobalProtect™, and Fortinet Fortigate®). That guidance lists indicators of compromise for detecting malicious activity [1]. This Cybersecurity Advisory is intended to convey additional actions for compromise recovery and longer-term actions for hardening.

MITIGATIONS FOR PULSE SECURE® VPN CLIENT

On April 24, 2019, security researchers released a series of vulnerabilities in the Pulse Secure® VPN from version 5.1R0X to 5.6R0X [2]. These vulnerabilities allow for remote arbitrary file downloads and remote code execution on Pulse Connect Secure and Pulse Policy Secure gateways. Other vulnerabilities in the series allow for interception or hijacking of encrypted traffic sessions. Exploit code is freely available online via the Metasploit® framework, as well as GitHub®. Malicious cyber actors are actively using this exploit code. System owners are strongly recommended to upgrade to the respective versions listed in the table below [3].

Riggi – 17

©2021 American Hospital Association

17

COVID-19 Induced Cyber Triple Threat - Cyber Criminals Exploiting a Crisis (cont.)

Threat 3: Resource Constraints

- Hospitals and health systems face human, financial and technical cybersecurity resource constraints **due to reduced hospital revenue**
- The AHA released a report in June 2020 which estimated the total losses for hospitals and health systems to be at least \$323 billion
- Leaving limited funds available to bolster cybersecurity defenses, recruit and retain **scarce** cybersecurity professionals



Riggi – 18

©2021 American Hospital Association

18

October 28 – 30, 2020

- On 10/28 late evening, an unprecedented cyber warning was issued by the government: “CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers.”
- AHA had been briefed directly prior to the public warning by FBI and DHS
- On 10/29 the AHA issued a special bulletin amplifying the warning and indicating phishing emails are the primary “attack vector” - methodology
- Potential for multiple hospitals being targeted in same region simultaneously

Riggi –
19

©2020 American Hospital Association -

19

JOINT CYBERSECURITY ADVISORY
Ransomware Activity Targeting the Healthcare and Public Health Sector
AA20-302A
October 28, 2020

Special Bulletin
October 29, 2020
New Information on Imminent Ransomware Threat against U.S. Hospitals

Ransomware Wave Hits Healthcare, as 3 Providers Report EHR Downtime
A joint alert from HHS, DHS, CISA, and the FBI warn of an imminent wave of ransomware attacks, including Ryuk, as three providers deal with IT disruptions under EHR downtime.

Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack
A wave of damaging attacks on hospitals upended the lives of patients with cancer and other ailments. "I have no idea what to do," one said.

Riggi –
20

©2020 American Hospital Association -

20

Ransomware Trends 2020 - 2021



- Attacks are highly targeted against specific hospitals and health systems
- Phishing emails is still the primary “attack vector” – because it’s simple and it works
- Increasing in sophistication and severity. Ryuk, Conti and DoppelPaymer
- Network and data backups may be targeted first
- Ransomware may now execute within hours or minutes upon initial compromise leaving very little reaction time to identify and contain
- Ransom demands are increasing and scaled based upon size of organization targeted, multi-million dollar requests common, reports of ransom demands exceeding \$60,000,000 in 2020
- High volume/disruptive telephone calls to executives and staff demanding ransom payment
- Ransomware attack combined with other cyber crimes - data extortion. Criminals threaten to sell /publish stolen patient data

Riggi –
21

©2020 American Hospital Association

21

Ransomware Impact 2020 -2021

- ... Disruption to patient care and business operations – Patient Safety issue
- ... Telemetry systems inoperable – nurse must be present for critical patients
- ... EMR rendered inaccessible – treatment and drug allergies/interactions unknown resulting in a delay in rendering care
- ... Lab results and imagery unavailable
- ... Surgeries cancelled
- ... EDs shutdown – Ambulances places on full divert – delaying emergency treatment



Riggi –
22

©2020 American Hospital Association

22

Ransomware Impact 2020 -2021 (cont.)

- ... Ransomware “blast Radius” – dependent providers and third parties also disrupted
- ... Recovery time form ransomware attacks, even if able to restore from unaffected backups, is a minimum 3 to 4 weeks- residual impacts lasting up to 6 months
- ... Increased insurance premiums
- ... Increase in credit risk leading to increase in cost of financing
- ... Lost revenue implications burn rate, and of course;
- ... Reputational harm – loss of patient, community and investor confidence

Riggi –
23

©2020 American Hospital Association

23

Contributing Factors 2020 -2021

- ... Email – Phishing Attack. *Need for increased employee awareness and training*
- ... Email – Insufficient email technical security controls. *Need for increased email advanced threat protection, behavior and signature based, quarantine of attachments, safe links*
- ... Lack of multifactor authorization (MFA) for remote access of networks, VPN, and email. *Institute MFA for all categories of remote access – Then internally for all system administrative privileges*
- ... "Flat" networks. *Need for network segmentation*
- ... Lack of real time 24/7 log, event, incident and alerts monitoring. *Need full time internal or external Managed Detection and Response (MDR) service.*
- ... *capabilities, bitcoin.*

Riggi –
24

©2020 American Hospital Association

24

Contributing Factors 2020 -2021 (cont.)

- ... Insufficient or delayed leadership notification, response and/or emergency containment actions. *Need updated, organization wide, routinely tested cyber incident response plan, with clear lines of designated and delegated emergency action authorities*
- ... Inability to restore from backups. *Need to ensure backups are offline, network segmented, multiple copies on prem and in cloud, highly secure, no remote access, MFA, 3-2-1 rule*
- ... Unprepared for a multi-week or multi-month IT disruption. *Need contingency plans for continuity of patient services, imaging, lab results, documentation on paper, revenue cycle disruption, 3rd party dependencies*
- ... Insufficient cyber insurance coverage hindering response and recovery efforts. *Conduct review of cyber insurance coverage for limitations, exclusions, ransomware coverage, forensics firms capabilities, bitcoin*

Riggi –
25

©2020 American Hospital Association

25



Coronavirus News: Bipartisan Bill Seeks to End Medicare Sequester; CDC Adjusts Quarantine Options

AHA testifies at Senate hearing on cyber threats amid pandemic. The Senate Homeland Security and Governmental Affairs Committee today held a [hearing](#) on defending communities from cyber threats during the COVID-19 pandemic.

Testifying at the hearing, John Riggi, AHA senior advisor for cybersecurity and risk, [said](#) the pandemic has led to a cyber "triple threat" for hospitals and health systems: an expanded attack surface due to rapidly expanded network- and internet-connected technologies and services; increased cyberattacks of all types; and fewer available resources to bolster cybersecurity defenses.

"A ransomware attack on a hospital crosses the line from an economic crime to a threat-to-life crime; such attacks should therefore be aggressively pursued and prosecuted as such by the federal government," Riggi said. "...We recommend that, given the increased cyber threat environment and attacks specifically targeting hospitals and health systems, along with resource constraints imposed upon hospitals and health systems in response to COVID-19, additional safe harbor protections from civil and regulatory liability be provided to hospital and health system victims of cyberattacks."

"A ransomware attack on a hospital crosses the line from an economic crime to a threat-to-life crime; these attacks should therefore be aggressively pursued and prosecuted as such"

"...With resource constraints imposed upon hospitals and health systems in response to COVID-19, **additional safe harbor protections from civil and regulatory liability be provided to hospital and health system victims of cyberattacks.**"



Riggi –
26

©2021 American Hospital Association -

26

Cybersecurity bill with AHA-supported provisions signed into law Jan. 05 2021

President Trump yesterday signed into law a bill ([H.R. 7898](#)) containing provisions that require the Secretary of Health and Human Services to **consider certain recognized cybersecurity best practices when making determinations against HIPAA-covered entities and business associates victimized by a cyberattack**.

For example, the bill recognizes cybersecurity practices established under the National Institute of Standards and Technology Act and approaches established under Section 405(d) of the Cybersecurity Act of 2015 by the Healthcare and Public Health Sector Coordinating Council (HSCC) Working Group, whose members include the AHA. The [HSCC expressed strong support](#) for the provisions. The legislation cleared the Senate by unanimous consent on Dec. 19.

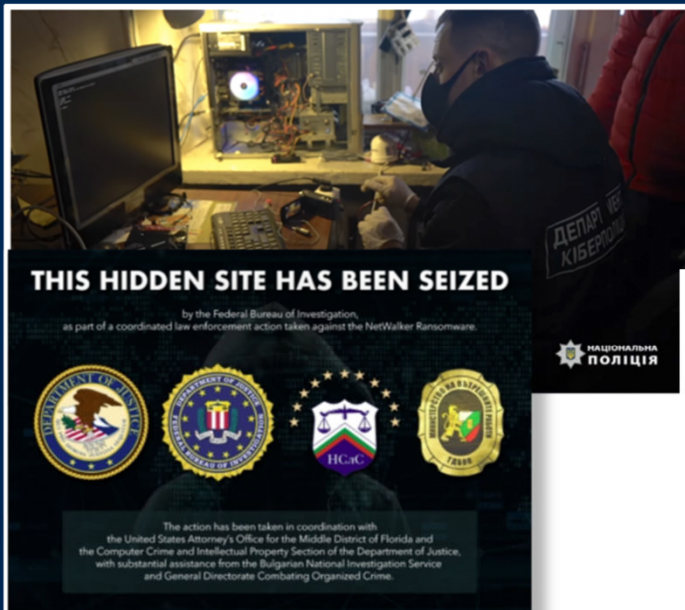
- Recognized Cybersecurity Practices in Place Previous 12 months
- Reduced Fines
- Early, Favorable Termination of Audits

"This law will have long lasting positive impact for the entire health care sector in securing patient data and protecting patients from cyber risks," said John Riggi, AHA senior advisor for cybersecurity and risk. "The law provides the right balance of incentivizing voluntary, enhanced cybersecurity protocols in exchange for regulatory relief and recognition that breached organizations are victims, not the perpetrators."

Riggi –
27

©2021 American Hospital Association

27



Seizure page of dark web hidden resource used to communicate with NetWalker ransomware victims.

Emotet Takedown Disrupts Vast Criminal Infrastructure; NetWalker Site Offline



Riggi –
28

©2021 American Hospital Association

28

Cyber Incident Response Plan

- *Backup status and security, 3-2-1, restoration point and time, offline?*
- Do we have a **unified** cyber-incident response plan & is it up-to-date?
- Multi-day impact and multi-incident plan?
- Does it include specific individuals from all clinical, business, administrative and facilities functions - with defined roles, responsibilities and ***off hours contact information and plan access?***
- Activation and decision escalation protocol and matrices?
- Leadership role – ***designation and delegation of critical authorities?***
- Is the plan regularly tested, gaps and best practices identified and updated to include current threat scenarios such as ransomware?



©2021 American Hospital Association

29

Cyber Incident Response Plan (cont.)

- Legal, regulatory, financial and reputational risks
- Internal and external communications strategy
- Out of band communications
- Paper copies and downtime procedures
- Continuity of operations – emergency management
- Cyber insurance requirements – forensics firm
- FBI, government and forensics firm integration



©2021 American Hospital Association

30

Risk Tolerance and Cyber Insurance

- **How much cyber risk are we willing to accept**
- **How much risk are we willing to transfer**
- Do we have cyber insurance
- What are the limitations and requirements
- Vendor and subcontractor requirements
- **Scales with VRM risk prioritization**
- Is our cyber insurance coverage adequate and current to cover all costs associated with a:
 - ✓ Multi-day network outage
 - ✓ Breach mitigation and recovery
 - ✓ Lost revenue
 - ✓ Reputational harm
 - ✓ Legal and regulatory exposure
 - ✓ Victim and patient services – credit monitoring
- Forensics firms panel – integration with IRP
- Interaction and integration with other insurance policies
- Ransomware coverage – bitcoin
- “Act of war” exemption for cyber



©2021 American Hospital Association

31

Strategic Vendor Risk Management Program Considerations

- Does your organization have a vendor risk management program (VRM)? What is the governance structure and does that structure still make sense?
- Is there a formal process to incorporate cybersecurity in the VRM program?
- Is there process to conduct periodic in-depth technical, legal, policy and procedural review of the VRM program and the BAA?
- Does the BAA include cybersecurity and cyber insurance requirements for the vendor and any subs of the vendor? Are the coverages and limits sufficient?
- Annual cyber risk assessments for vendors?
- Compliance requirements with applicable regulatory standards – HIPAA, PCI, PII, taxpayer funded medical research and IP?

©2021 American Hospital Association

32

Strategic Vendor Risk Management Program Considerations (cont.)

- **Identify, risk classify and risk prioritize** vendors and their subcontractors based upon:
 - ✓ **Aggregation** of data – Regulated data and unregulated data such as pop health genetic studies, clinical trials, COVID-19 research
 - ✓ **Access** to sensitive data, networks, systems and physical locations
 - ✓ **Criticality/Impact** to continuity of operations – Clinical, facilities, utilities, business (e.g. telecom, medical transcription, billing and coding, PPE supplies, etc)
 - ✓ **Foreign** operations and foreign subcontractors
- **Implement risk based controls and cyber insurance requirements**
- Need to balance financial opportunities and greater supply-chain flexibility with potentially higher cyber risks associated with certain vendors

<https://healthsectorcouncil.org/wp-content/uploads/2020/09/Health-Industry-Cybersecurity-Supply-Chain-Risk-Management-Guide-v2.pdf>



©2021 American Hospital Association

33

A Layered, Risk Based Approach to Cybersecurity = Defense in Depth

Polices and Dynamic Processes for:

- Network Mapping and Access
- Data Classification and Mapping
- Baseline Network Activity
- Network Segmentation
- Application Inventory
- Device and IoT Inventory



Riggi -
34

©2021 American Hospital Association

34



John Riggi
Senior Advisor for Cybersecurity and Risk

John Riggi, having spent nearly 30 years as a highly decorated veteran of the FBI, serves as the first senior advisor for cybersecurity and risk for the American Hospital Association and their 5000+ member hospitals. John leverages his distinctive experience at the FBI and CIA in the investigation and disruption of cyber threats, international organized crime and terrorist organizations to assist on policy and advocacy issues and provide trusted advisory services for the nations' hospitals and health systems. His trusted access to hospital leadership and government agencies enhances John's national perspective and ability to provide uniquely informed risk advisory services.

John represented the nation's hospitals in testimony provided to the Senate Homeland Security Committee hearing on cyber threats to hospitals in Dec. 2020. John also served as the nation's hospital representative to the FCC hospital robocall protection group which made final recommendations on reducing unlawful robocalls to hospitals in Dec. 2020. John initiated and co-led a national HHS/healthcare sector task group to develop resources to assist the field in managing cyber risk as an enterprise risk issue. John launched a national campaign with the AHA and government agencies to help members protect medical research against foreign threats.

In various leadership roles at the FBI, John served as a representative to the White House Cyber Response Group and a senior representative to the CIA and was the national operations manager for terrorist financing investigations. John also led counterintelligence field surveillance programs in Washington DC and financial crimes and terrorist financing squads in New York City. John ultimately rose to the ranks of the Senior Executive Service and in that capacity led the FBI Cyber Division national program to develop mission critical partnerships with the healthcare and other critical infrastructure sectors. John held a national strategic role in the investigation of the largest cyber-attacks targeting healthcare and other sectors.

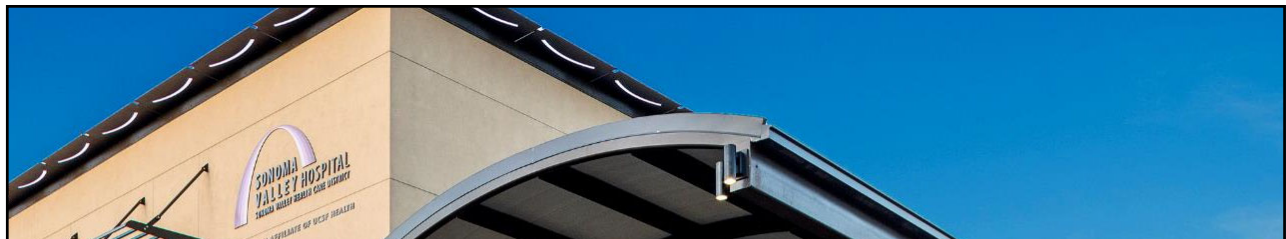
He also served on the NY FBI SWAT Team for eight years. John is the recipient of the FBI Director's Award for Special Achievement in Counterterrorism and the CIA's George H.W. Bush Award for Excellence in Counterterrorism, the CIA's highest award in this category. John presents extensively on cybersecurity and risk topics and is frequently interviewed by the media.

jriggi@aha.org

(O) +1 202-626-2272

(M) +1 202-640-9159


35




Sonoma Valley Hospital

Since October 11, 2020


36




Our Story




Sonoma Valley Hospital is a small district hospital in Sonoma, California serving the 42,000 residents of the valley




We affiliated with UCSF Health in 2018



We run a tight ship and invest all that we can in I.T. but are not able to follow all the best practices

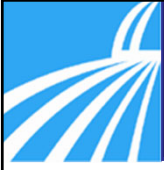


2020 was a memorable year for all, but the cyber-attack on October 11th was a very unfortunate and costly event



Our extremely small team is strong, resourceful, committed and resilient

37

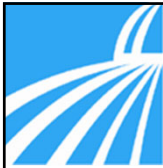


Actions

- CEO made aware of the Ransomware attack notice by I.T. staff
- Followed the response plan and immediately shut down all systems
- Law enforcement was notified
- Hospital went on downtime procedures in every department
- Cyber security experts were engaged

Mather - 38

38



Actions (cont.)

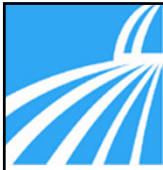
- Began containment with internal staff and remote experts
- UCSF leadership helped us navigate throughout the 100 days
- Recovery “experts” came within a week
- Breach management & notification with cyber attorney
- Except mammography, patient care continues with down time procedures

Mather - 39

39



40



Lessons Learned

Administrative

- Cyber insurance
- Cyber security training and awareness (attack started with a phishing email)
- IT Security role in house
- Engage legal that specializes in cybersecurity
- Engage a third party that specializes in threat actor communication and negotiation
- Engage an external company (if internal resource is constrained) for incident response and tracing
- Strong passwords and regular password change policy should be in place

Mather - 41

41



Lessons Learned (cont.)

Information Technology

- Backup is critical, periodic validation of backup is also necessary
- Keep up with security patches
- Build a sustainable plan to avoid end of support/end of life software and hardware
- IT assets inventory (physical and virtual)
- Multi-factor authentication
- Secured email
- Logging (crucial for incident response and ongoing monitoring)
- Disaster recovery (failover and annual testing will be ideal)

Mather - 42

42




ENLOE
MEDICAL CENTER

Tamra Durfee
Director, Technology



43



Top Ten Recommendations

1. ASSUME you will be hit with ransomware
 - It hasn't happened, because it hasn't happened
 - Have a plan and practice it, CSIRP
2. Backups
 - Follow 3-2-1 industry standard
 - TEST your backup restore process

Durfee - 44

44

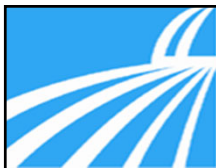


Top Ten Recommendations (cont.)

3. Two-Factor Authentication
 - NO remote access without 2FA
4. Firewalls
5. Privileged Access Management
6. Medical devices
7. Patching

Durfee - 45

45




Top Ten Recommendations (cont.)

8. PRINT vendor and staff contact info, passwords
9. Vendor help
 - Have reliable partners
 - Staff cannot work 24x7
10. Incident Response Vendor
 - On retainer if possible

Durfee - 46


46



Questions?

Please type your questions in the Q/A section at the bottom of your Zoom screen.

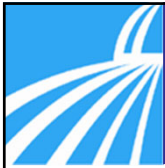
47



Contact Information

Meghan Hardin Regional Vice President Hospital Council Northern and Southern California mhardin@hospitalcouncil.org	Kelly Mather Chief Executive Officer BayHealth Development Kelly.Mather@BayHealthDevelopment.com
John Riggi Senior Advisor for Cybersecurity and Risk American Hospital Association jriggi@aha.org	Tamra Durfee Director, Technology Enloe Medical Center Tamra.Durfee@enloe.org

48



Thank You and Evaluation

Thank you for participating in today's webinar.
An online evaluation will be sent to you shortly.

For education questions, contact:
CHA Education at (916) 552-7637 or
education@calhospital.org