



# Health Care Cybersecurity Symposium

## *Managing Risk Within the Health Care Supply Chain*

NOVEMBER 8, 2021



## Agenda



### Opening Remarks

**Ben Steffen**, *Executive Director*, Maryland Health Care Commission

**Bob Atlas**, *President and Chief Executive Officer*, Maryland Hospital Association

### Protecting Your Organization Against Supply Chain Cyber-Attacks

**John Riggi**, *Senior Advisor for Cybersecurity and Risk*, American Hospital Association

### The Increasing Cybersecurity Risks in the IT Supply Chain

**Clay House**, *Chief Information Security Officer and Vice President of IT Risk Management*, CareFirst BlueCross BlueShield

### Roundtable Discussion: Best Practices for Third-Party Risk Management

**Rick Moore**, *Moderator, Founder and Chief Executive Officer*, MTC Group, LLC

**Lee Barrett**, *Executive Director and Chief Executive Officer*, EHNAC

**Brandon Neiswender**, *Vice President and Chief Operating Officer*, CRISP

**Tressa Springmann**, *Senior Vice President and Chief Information and Digital Officer*, LifeBridge Health

**Mike Zbarsky**, *Senior Chief Information Security Officer Advisor*, Hartman Executive Advisors



Thank You!



## Protecting Your Organization Against Supply Chain Cyber-Attacks




**John Riggi**

*Senior Advisor for Cybersecurity and Risk, American Hospital Association*



MARYLAND  
Department of Health


## ***Cybersecurity Symposium: Managing Risk Within the Health Care Supply Chain***




American Hospital Association  
Advancing Health in America

### **Cybersecurity and Risk Advisory Services**

Presented by John Riggi, Senior Advisor, Cybersecurity and  
Risk Advisory Services 11/08/2021



American Hospital Association  
Advancing Health in America



AHA CENTER FOR HEALTH  
**INNOVATION**

### ***Hacking Incidents Reported to OCR***

***2020 Total:***

***425 Breaches Impacting 26.7 Million Individuals***

***1/1/2021 - 11/03/2021***

***379 Breaches Impacting 36.4 Million Individuals***

Source : HHS, OCR website data accessed 01/11/2021 and 11/08/2021 <https://ocrportal.hhs.gov>

## Attack Patterns and Priority Risks

**#1 Priority - High impact ransomware attacks** especially those that result in a regional or statewide disruption of care delivery and risk patient safety.

**2) Third party cyber risk exposure** and impact through business associates and supply chain:

- Theft of large quantities of covered entity data in possession of business associates – ACO?
- Business associate as digital pathway into covered entity + Supply Chain Attacks
- Mission critical business associate becomes victim of ransomware attack

**3) Direct theft of data** - PHI, PII, Payment Information and Medical Research including, genomics, precision medicine, clinical trials, population health studies and cancer research.

**Las Vegas hospital hit in cyberattack, data stolen**

**WANTED BY THE FBI**  
**APT 40 CYBER ESPIONAGE ACTIVITIES**  
Continuity to Manage Protected Computers and Control Economic Espionage; Continuity to Manage Protected Computers and Control Economic Espionage

**Private Industry Notification**  
AMCA data breach has now gone over the 20 million mark  
Maine health system sued over Blackbaud breach that exposed info of 657,000 people

**Third-Party Health Data Breach Hits Pennsylvania Health Network**  
A Pennsylvania health system which exposed PHI  
Health Sector Cybersecurity Coordination Center (HC3) Sector Alert  
December 14, 2020  
Active Exploitation of SolarWinds Software Potentially Affecting HPH Sector

**JOINT CYBERSECURITY ADVISORY**  
Exploitation Appliance  
February 24, 2021  
Compromise of Microsoft Exchange Server  
The Joint Cybersecurity Advisory uses the MITRE Adversary Tactics Framework (ATF) to provide a common language for describing cyber threats and attacks.

**CYBERSECURITY ADVISORY**  
Russian SVR Targets U.S. and Allied Networks  
Cancer software security breach hits 40 health systems: Yale New Haven Health, Lifespan & more  
Opinion: We at Scripps Health were victims of a ransomware attack. Here's what we've learned.



7

## Ransomware Impact 2020 -2021

- **Risk to patient safety.** ED's shutdown - Ambulances placed on full divert - delay of emergency treatment. Trauma Center availability - Regional impact
- Telemetry systems inoperable – additional staff required for patient monitoring
- Radiology / Imaging / PACS down
- EMR rendered inaccessible treatment and drug allergies / interactions unknown – delay in rendering care
- Lab results unavailable
- Surgeries cancelled - ADT impact
- Pixus systems down
- Home care telemetry disrupted and patients placed at risk
- Ransomware “blast radius” – other providers who are dependent for ED, EMR, labs, imaging, cancer treatment and other third parties also disrupted
- Loss of all medical technology and/or network connected medical technology
- **Staff unprepared for extended clinical downtime procedures and paper charting lasting up to three to four weeks**
- *Three to four week recovery time for mission critical systems, ransom paid or not, residual impacts lasting minimum 6 months*
- Legacy systems unrecoverable
- Revenue cycle interruption and revenue loss due to incomplete charts.
- Timekeeping, email and VoIP systems disrupted
- Operational and physical security technology impact
- Third parties requesting independent certification before reconnection
- Increased insurance premiums or loss of coverage
- Class action and individual lawsuits from patients
- HHS OCR investigation/audit + State investigations
- Credit monitoring costs
- Increase in credit risk rating, increased financing and bond issuance
- Lost business opportunities, future revenue
- *Reputational harm – possible loss of patient, community and investor confidence*



8



# San Diego EDs Deluged With Patients After Cyberattack

— "I've been with UCSD for 30 years, and it's not something I've seen before."

by Randy Dotinga, Contributing Writer, MedPage Today October 30, 2021



The average daily census grew to 281 over the cyberattack period versus 174-229 patients during the same week over the previous 5 years

The take-home message from the studies is that "We should be discussing cyberattack impacts on regions, and developing regional preparedness plans,"

*Dameff stressed, adding that tabletop simulations of cyberattacks should be routine, and hospitals need to talk to each other about plans to handle critical patients.*

Christian Dameff, MD, of UCSD, in presentations at the American College of Emergency Physicians annual meeting.

©2021 American Hospital Association

## JOINT CYBERSECURITY ADVISORY

Co-Authoring by:



Product ID: AA21-265A

September 22, 2021

TLP:WHITE

### Conti Ransomware

#### SUMMARY

**Note:** This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 9. See the [ATT&CK for Enterprise](#) for all referenced threat actor tactics and techniques.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have observed the increased use of Conti ransomware in more than 400 attacks on U.S. and international organizations. In typical Conti ransomware attacks, malicious cyber actors steal files, encrypt servers and workstations, and demand a ransom payment.

To secure systems against Conti ransomware, CISA, FBI, and the National Security Agency (NSA) recommend implementing the mitigation measures described in this Advisory, which include requiring multi-factor authentication (MFA), implementing network segmentation, and keeping operating systems and software up to date.

[Click here](#) for indicators of compromise (IOCs) in STIX format.

#### Immediate Actions You Can Take Now to Protect Against Conti Ransomware

- Use [multi-factor authentication](#).
- Segment and segregate networks and functions.
- Update your operating system and software.

# WHITE PAPER

## STRATEGIC THREAT INTELLIGENCE: PREPARING FOR THE NEXT "SOLARWINDS" EVENT



- The centralized system easily controls multiple subsystems, networks, or products, requiring little interaction or no activation from the controlled system.
- The system possesses an undisclosed, unpatched, or unknown opening that attackers can exploit for a degree of administrative control.
- The exploited opening of the centralized product can affect, in either a limited or total ability, the subsystem it controls.



### How Health-ISAC and AHA Work Together

The AHA and Health-ISAC have urged for more ways to improve cyber security in a global approach to defend against cyber threats. Hospitals and health systems, and the patients they care for every day, are heavily targeted by cyber adversaries, including sophisticated nation-states. Defenders have made great strides to protect their networks, secure patient data, preserve health care services' efficient delivery and, most importantly, ensure patient safety. However, it cannot be done alone. Hospitals and health systems need more active support from the public and private sector to defend patients from cyber threats.

Health-ISAC and AHA partner in a variety of ways. Highlighting just a few examples regarding information sharing, Health-ISAC shares many threat and vulnerability reports with AHA for the benefit of their 5,000 member hospitals. AHA and Health-ISAC will



MUST READ: Tech workers are preparing to quit. Persuading them to stay won't be easy

## Kaseya urges customers to immediately shut down VSA servers after ransomware attack

Victims are already seeing ransom demands ranging from \$45,000 to \$5 million.



Kaseya » Other » Informational

### Important Notice July 12th, 2021

July 12, 2021 3AM US EDT

As posted in the previous update we released the patch to VSA On-Premises customers and began deploying to our VSA SaaS Infrastructure prior to the 4:00 PM target. The restoration of services is progressing, with 95% of our SaaS customers live and the remaining servers coming online for the rest of our customers in the coming hours. Our support teams are working with VSA On-Premises customers who have requested assistance with the patch.

We will continue to post updates on the patch rollout progress and server status.

July 11, 2021 10PM US EDT

VSA Update:

As posted in the previous update we released the patch to VSA On-Premises customers and began deploying to our VSA SaaS Infrastructure prior to the 4:00 PM target. The restoration of services is progressing according to plan, with 60% of our SaaS customers live and servers coming online for the rest of our customers in the coming hours. Our support teams are working with VSA On-Premises customers who have requested assistance with the patch.



### CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack

Note: this guidance was published to [www.cisa.gov](https://www.cisa.gov) on July 4, 2021 at <https://www.cisa.gov/news/current-events/2021/07/04/cisa-fbi-guidance-msp-and-their-customers-affected-kaseya-vsa>

CISA and the Federal Bureau of Investigation (FBI) continue to respond to the recent supply-chain ransomware attack leveraging a vulnerability in Kaseya VSA software against multiple managed service providers (MSPs) and their customers. CISA and FBI strongly urge affected MSPs and their customers to follow the guidance below. CISA and FBI recommend affected MSPs:

- Download the [Kaseya VSA Detection Tool](#). This tool analyzes a system (either VSA server or managed endpoint) and determines whether any indicators of compromise (IoC) are present.
- Enable and enforce multi-factor authentication (MFA) on every single account that is under the control of the organization, and—to the maximum extent possible—enable and enforce MFA for customer-facing services.
- Implement allowlisting to limit communication with remote monitoring and management (RMM) capabilities to known IP address pairs, and/or
- Place administrative interfaces of RMM behind a virtual private network (VPN) or a firewall on a dedicated administrative network.

CISA and FBI recommend MSP customers affected by this attack take immediate action to implement the following cybersecurity best practices. Note: these actions are especially important for MSP customer who do not currently have their RMM service running due to the Kaseya attack.

CISA and FBI recommend affected MSP customers:

- Ensure backups are up to date and stored in an easily retrievable location that is air-gapped from the organizational network;
- Revert to a manual patch management process that follows vendor remediation guidance, including the installation of new patches as soon as they become available;
- Implement:
  - Multi-factor authentication; and
  - Principle of least privilege on key network resources admin accounts.

**Resources:** CISA and FBI provide these resources for the reader's awareness. CISA and FBI do not endorse any non-governmental entities nor guarantee the accuracy of the linked resources.

- For the latest guidance from Kaseya, see Kaseya's [Important Notice July 2nd, 2021](#).
- For indicators of compromise, see Peter Lowe's GitHub page [Bkyl Kaseya CnC Domains](#). Note: due to the urgency to share this information, CISA and FBI have not yet validated this content.
- For guidance specific to this incident from the cybersecurity community, see Cado Security's GitHub page, [Remediate the RMM Infrastructure: Responding to the RMM Ransomware: Kaseya Supply Chain Attack](#). Note: due to the urgency to share this information, CISA and FBI have not yet validated this content.
- For advice from the cybersecurity community on securing against MSP ransomware attacks, see Gavin Stone's article, [How secure is your RMM, and what can you do to better secure it?](#)
- For general incident response guidance, CISA encourages users and administrators to see [Joint Cybersecurity Advisory AASD-245A: Technical Approaches to Uncovering and Remediating Malicious Activity](#).

U.S. WHITE

## Chinese APT Group Compromised Healthcare Organizations by Exploiting Zoho Password Management Platform Flaw

Posted November 8, 2021 by HIPAA Journal

An advanced persistent threat (APT) actor has been conducting an espionage campaign seen the systems of at least 9 organizations compromised. The campaign targeted c in a range of critical sectors, including healthcare, energy, defense, technology, and

The campaign was identified by security researchers at Palo Alto Networks and while of the hacking group has yet to be confirmed, the researchers believe the attacks were conducted by the Chinese state-sponsored hacking group APT27, aka Iron Tiger, Em TG-3390, and LuckyMouse based on the use of hacking tools and techniques that m APT27 activity.

## 42% of Healthcare Organizations Have Not Developed an Incident Response Plan

Posted November 2, 2021 by HIPAA Journal

Hacks, ransomware attacks, and other IT security incidents account for the majority of data breaches reported to the Department of Health and Human Services' Office for Civil Rights, but data breaches involving physical records are also commonplace. According to the Verizon Data Breach Investigations Report, disclosed physical records accounted for 43% of all breaches in 2021, which highlights the need for data security measures to be implemented covering all forms of data.

## Nationwide Laboratory Services Ransomware Attack Affects 33,000 Patients

Posted November 5, 2021 by HIPAA Journal

Boca Raton, FL-based Nationwide Laboratory Services, which was acquired by Quest Diagnostics in the summer, was the victim of a ransomware attack earlier this year.

Nationwide Laboratory Services detected a breach of its systems on May 19, 2021, when ransomware was used to encrypt files across its network and prevent files from being accessed. Steps were immediately taken to contain the attack and a third-party cybersecurity firm was engaged to assist with the investigation and remediation efforts.

## HVAC Vendor Allegedly Hacked: Access Gained to Hospital Systems

Posted August 23, 2021 by HIPAA Journal

In early August, a hacker made contact with Dissent of *DataBreaches.net* and claimed to have hacked into the systems of a HVAC vendor. Through that vendor the hacker claimed to have gained access to the networks of its clients, one of which was Boston Children's Hospital.

The company in question is Canton, MA-based ENE Systems. *DataBreaches.net* reported in a recent blog post that the hacker had attempted to extort money from the HVAC vendor but the ransom was not paid. The hacker still claimed to have access to the network of ENE Systems and those of its clients and told Dissent that he/she was not interested in causing harm to the hospital. *DataBreaches.net* was asked to reach out to the hospital and make it clear that its network had been breached through the HVAC vendor, in case the vendor had not communicated the breach to the hospital. *DataBreaches.net* was provided with screenshots as proof of the hack.





# FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government

APRIL 15, 2021 • STATEMENTS AND RELEASES

The Biden administration has been clear that the United States desires a relationship with Russia that is stable and predictable. We do not think that we need to continue on a negative trajectory. However, we have also been clear—publicly and privately—that we will defend our national interests and impose costs for Russian Government actions that seek to harm us.

Today the Biden administration is taking actions to impose costs on Russia for actions by its government and intelligence services against U.S. sovereignty and interests.

## The Industry's Highest Performing Cybersecurity Platform

Fortinet Security Fabric Delivers Broad, Integrated, and Automated Protection Everywhere You Need It.

[Learn More](#)

## Fortinet Security Fabric Delivers End-to-End Security for 5G Ecosystems

Fortinet provides consistent security across 5G private and public networks, leveraging the fastest NGFWs to enable industrial enterprises and MNOs. And with 5G wireless WAN, offers flexible, ultra-fast connectivity for SD-WAN.

[Read more](#)



27 May 2021

Alert Number  
**MI-000148-MW**

**WE NEED YOUR HELP!**

If you find any of these indicators on your networks, or have related information, please contact

**FBI CYWATCH immediately.**

Email:  
[cywatch@fbi.gov](mailto:cywatch@fbi.gov)

Phone:  
**1-855-292-3937**

\*Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA.

This FLASH has been released **TLP:WHITE** subject to standard copyright rules. **TLP:WHITE** information may be distributed without restriction.

## APT Actors Exploiting Fortinet Vulnerabilities to Gain Access for Malicious Activity

The FBI is continuing to warn about Advanced Persistent Threat (APT) actors exploiting Fortinet vulnerabilities. As of at least May 2021, an APT actor group almost certainly exploited a Fortigate appliance to access a webserver hosting the domain for a U.S. municipal government. The APT actors likely created an account with the username "elle" to further enable malicious activity on the network.

The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) previously warned in April 2021 that APT actors had gained access to devices on ports 4443, 8443, and 10443 for Fortinet FortiOS [CVE-2018-13279](#), and enumerated devices for FortiOS [CVE-2020-12812](#) and FortiOS [CVE-2019-5591](#).

Access gained by the APT actors can be leveraged to conduct data exfiltration, data encryption, or other malicious activity. The APT actors are actively targeting a broad range of victims across multiple sectors, indicating the activity is focused on exploiting vulnerabilities rather than targeted at specific sectors. Please see Joint Cybersecurity Advisory AA21-092A, published 2 April 2021, for more information on this activity.





CYBER SECURITY NEWS · 4 MIN READ

# DHS Secretary: "Killware," Malware Designed To Do Real-World Harm, Poised To Be World's Next Breakout Cybersecurity Threat

SCOTT IKEDA · OCTOBER 22, 2021

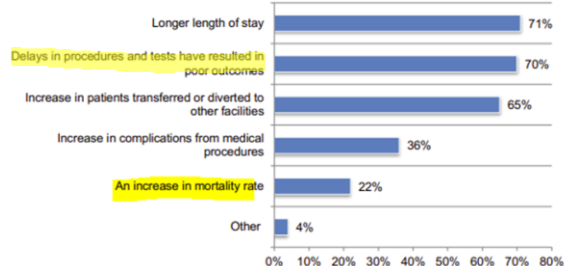
## New Ponemon Institute Research Shows Ransomware Attacks on Healthcare Delivery Organizations Can Lead to Increased Mortality Rate

by Rob Clampa | Sep 22, 2021

An Independent Analysis of Nearly 600 Providers Also Demonstrates How COVID-19 Has Reduced Their Ability to Defend Against Cyber Threats

**Figure 1. What impact does ransomware have on patient care?**

More than one response from the 43 percent of respondents in HDOs that had a ransomware attack.



Ransomware: Third-party risk

f t i in

**Report: Ransomware is a patient mortality risk, driven by COVID, third-party vendors**

Healthcare, September 22, 2021



Health workers wait with a patient outside of Mount Sinai Hospital on April 4, 2020, in New York City. Nearly a quarter of respondents say cyberattacks have contributed the mortality rate in their organizations, according to a new report. (Photo by Spencer Platt/Getty Images)



## CISA INSIGHTS

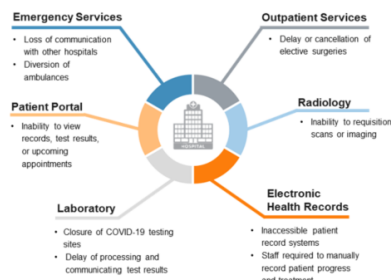
### **Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm**

September 2021

#### **Executive Additional External Stress: Ransomware Attacks**

In addition to the pandemic's stress on hospitals across the nation, external pressures, such as ransomware or the attacks on supporting infrastructure, can degrade operations in a time of crisis or urgency. Insights into the *Provide Medical Care* NCF gained by correlating bed utilization rates and excess deaths led to subsequent analysis on the threat that ransomware poses to the U.S. hospital systems. Although there are no deaths directly attributed to hospital cyber-attacks, statistical analysis of an affected hospitals' relative performance indicates reduced capacity and worsened health outcomes, which can be measured in the time of the COVID-19 pandemic in excess deaths.

The ransomware attack on a hospital system's network resulted in inaccessible patient schedules and records, disrupted communication, and delays in processing and communicating test results (Figure 6). Downstream effects included cancelled or delayed surgeries and cancer treatments, closure of several COVID-19 test collection sites, inability to submit radiology imaging, and loss of communication between hospitals in the network (Figure 7). This forced critical patient diversion, paper-based record-keeping, and suspension of care to high-risk patients. Although there are no deaths directly attributed to the cyber-attack, statistical analysis of its relative performance indicates reduced capacity.



BRIEFING ROOM

Administration Priorities

## Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

**Section 1. Policy.** The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.



THE WHITE HOUSE  
WASHINGTON

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

SUBJECT: What We Urge You To Do To Protect Against The Threat of Ransomware

DATE: June 2, 2021

The number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyberattacks – both private and public sector – is a top priority of the President's.

Under President Biden's leadership, the Federal Government is stepping up to do its part, working with like-minded partners around the world to disrupt and deter ransomware actors. These efforts include disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.

The private sector also has a critical responsibility to protect against these threats. All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location. But there are immediate steps you can take to protect yourself, as well as your customers and the broader economy. Much as our homes have locks and alarm systems and our office buildings have guards and security to meet the threat of theft, we urge you to take ransomware crime seriously and ensure your corporate cyber defenses match the threat.

The most important takeaway from the recent spate of ransomware attacks on U.S., Irish, German and other organizations around the world is that companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively. To understand your risk, business executives should immediately convene their leadership teams to discuss the ransomware threat and review corporate security posture and business continuity plans to ensure you have the ability to continue or quickly restore operations.

selected a small number of highly impactful steps to help you focus and make rapid progress on driving down risk.

#### What We Urge You To Do Now

**Implement the five best practices from the President's Executive Order:** President Biden's *Improving the Nation's Cybersecurity* Executive Order is being implemented with speed and urgency across the Federal Government. We're leading by example because these five best practices are high impact: multifactor authentication (because passwords alone are routinely compromised), endpoint detection & response (to hunt for malicious activity on a network and block it), encryption (so if data is stolen, it is unusable) and a skilled, empowered security team (to patch rapidly, and share and incorporate threat information in your defenses). These practices will significantly reduce the risk of a successful cyber-attack.

**Backup your data, system images, and configurations, regularly test them, and keep the backups offline:** Ensure that backups are regularly tested and that they are not connected to the business network, as many ransomware variants try to find and encrypt or delete accessible backups. Maintaining current backups offline is critical because if your network data is encrypted with ransomware, your organization can restore systems.

**Update and patch systems promptly:** This includes maintaining the security of operating systems, applications, and firmware, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to drive your patch management program.

**Test your incident response plan:** There's nothing that shows the gaps in plans more than testing them. Run through some core questions and use those to build an incident response plan: Are you able to sustain business operations without access to certain systems? For how long? Would you turn off your manufacturing operations if business systems such as billing were offline?

**Check Your Security Team's Work:** Use a 3<sup>rd</sup> party pen tester to test the security of your systems and your ability to defend against a sophisticated attack. Many ransomware criminals are aggressive and sophisticated and will find the equivalent of unlocked doors.

**Segment your networks:** There's been a recent shift in ransomware attacks – from stealing data to disrupting operations. It's critically important that your corporate business functions and manufacturing/production operations are separated and that you carefully filter and limit internet access to operational networks, identify links between these networks and develop workarounds or manual controls to ensure ICS networks can be isolated and continue operating if

21

©2021 American Hospital Association

◆ WSJ NEWS EXCLUSIVE | U.S.

## Ransomware Targeted by New Justice Department Task Force

After 'worst year ever' for the cyberattacks, department seeks to disrupt digital ecosystem that supports them



The Justice Department's criminal, national security and civil divisions will take part in the ransomware task force.

PHOTO: ARIEL ZAMBELICH/THE WALL STREET JOURNAL

22

©2021 American Hospital Association

June 11, 2021

**President urged to include health care cybersecurity in infrastructure plans: DOJ prioritizes ransomware attacks.** The Healthcare and Public Health Sector Coordinating Council (HSPHSCC) has urged President Biden to include support for health care cybersecurity in a full-scale infrastructure bill.

Technology

"The healthcare sector, despite making progress on cyber threats without enhanced federal programs a lesser resourced organizations, such as small and fall further behind. We are only as strong as the weakest link in the chain."

AHA also has urged Congress and the Biden Administration to ensure all patients have secure, sustained, equitable access to care.

## Exclusive: U.S. to give ransomware hacks similar priority as terrorism

Christopher Bing

Reuters last week reported that the U.S. Justice Department is elevating the priority of ransomware investigations similar to those of terrorism attacks following a May 7 attack on the Colonial Pipeline and damage to other sectors. The department this week announced it had seized \$2.3 million in bitcoin proceeds allegedly from the attack.

"The AHA has been leading a call to the government to pursue a coordinated campaign to disrupt these criminal organizations and seize their illegal proceeds, as was done so effectively during the global fight against terrorism," said John Riggi, AHA senior advisor for cybersecurity and risk. *"We have good reason to believe that our persistent advocacy and expert point of view on this issue helped influence this policy change."*

23

©2021 American Hospital Association

October 21, 2021  
6:45 PM EDT  
Last Updated: 4 days ago

Technology

## EXCLUSIVE Governments turn tables on ransomware gang REvil by pushing it offline

4 minute read

By Joseph Menn and Christopher Bing



1/3

Acting U.S. Attorney for the Northern District of California Stephanie Hays speaks about the Colonial Pipeline ransomware attack during a news conference with Deputy U.S. Attorney General Lisa Monaco and FBI Deputy Director Paul Abbate at the Justice Department in Washington, U.S.

©2021 American Hospital Association



WORLD

## Hackers Linked to Ransomware Attacks on JBS, Kaseya Arrested

U.S. and European officials disclosed arrests in Poland and Romania of people linked to REvil ransomware attacks



### Why Ransomware Attacks Are on the Rise and How the U.S. Can Fight Them

Ransomware attacks are increasing in frequency, victim losses are skyrocketing, and hackers are shifting their targets. WSJ's Dustin Volz explains why these attacks are on the rise and what the U.S. can do to fight them. Photo illustration: Laura Kammermann

By Robert McMillan

Updated Nov. 8, 2021 1:29 pm ET



## THE UNITED STATES DEPARTMENT OF JUSTICE

ABOUT

OUR AGENCY

TOPICS

NEWS

RESOURCES

CAREERS

Home » Office of Public Affairs » News

### JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, October 28, 2021

### Russian National Extradited to United States to Face Charges for Alleged Role in Cybercriminal Organization

A Russian national, residing in the Yakutsk region of Russia and in Southeast Asia, had his initial appearance in federal court today after his extradition from the Republic of Korea to the Northern District of Ohio to face charges for his alleged role in a transnational, cybercriminal organization.

According to court documents, Vladimir Dunaev, 38, was a member of a transnational, cybercriminal organization that deployed a computer banking trojan and ransomware suite of malware known as "Trickbot."



Martin Matischak  
November 6, 2021

Government News

## House approves massive infrastructure plan that includes \$1.9 billion for cybersecurity

Shown Here:  
Introduced in Senate (S.1316)

117th CONGRESS  
1st Session

## S. 1316

To amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to make a declaration of a significant incident, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 22, 2021

Mr. PERINE (for himself and Mr. PETERS) introduced the following bill, which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

## A BILL

To amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to make a declaration of a significant incident, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

### SECTION 1. SHORT TITLE.

This Act may be cited as the "Cyber Response and Recovery Act of 2021".

### SEC. 2. DECLARATION OF A SIGNIFICANT INCIDENT.

(a) IN GENERAL.—Title XXII of the Homeland Security Act of 2002 (5 U.S.C. 651 et seq.) is amended by adding at the end the following:

**"Subtitle C—Declaration Of A Significant Incident**

AMENDMENT NO. \_\_\_\_\_ Calendar No. \_\_\_\_\_

Purpose: To modernize Federal information security management, to amend the Homeland Security Act of 2002 to establish the Cyber Incident Review Office in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and to make technical corrections to the Homeland Security Act of 2002.

IN THE SENATE OF THE UNITED STATES—117th Cong., 1st Sess.

## H.R. 4350

To authorize appropriations for fiscal year 2022 for military

## 1 DIVISION E—FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2021

### 4 SEC. 5101. SHORT TITLE.

5 This division may be cited as the "Federal Information Security Modernization Act of 2021".

### 7 SEC. 5102. DEFINITIONS.

8 In this division, unless otherwise specified:

9 (1) ADDITIONAL CYBERSECURITY PROCEDURE.—The term "additional cybersecurity procedure" has the meaning given the term in section 10 3552(b) of title 44, United States Code, as amended 11 by this division. 12 13

## 13 DIVISION F—CYBER INCIDENT REPORTING ACT OF 2021 AND CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

## 14 TITLE LXI—CYBER INCIDENT REPORTING ACT OF 2021

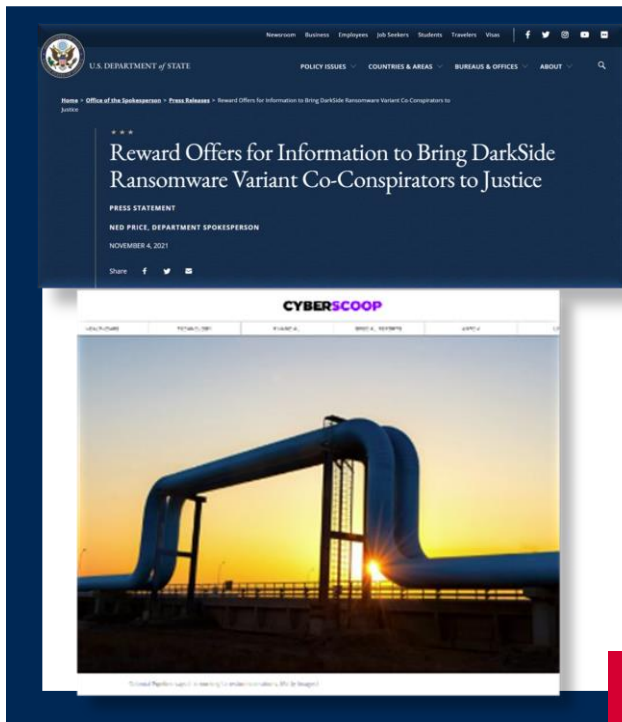
### 20 SEC. 6101. SHORT TITLE.

21 This title may be cited as the "Cyber Incident Reporting Act of 2021".

### 23 SEC. 6102. DEFINITIONS.

24 In this title 6 SEC. 6105. RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.

7 (a) PROGRAM.—Not later than 1 year after the date 8 of enactment of this Act, the Director shall establish a 9 ransomware vulnerability warning program to leverage ex- 0 isting authorities and technology to specifically develop 1 processes and procedures for, and to dedicate resources 2 to, identifying information systems that contain security 3 vulnerabilities associated with common ransomware at- 4 tacks, and to notify the owners of those vulnerable systems 5 of their security vulnerability. 6



- **\$10,000,000 for information leading to the identification or location of any individual(s) who hold(s) a key leadership position in the DarkSide ransomware variant transnational organized crime group.**
- **\$5,000,000 for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in a DarkSide variant ransomware incident.**

29

©2021 American Hospital Association



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

President Trump yesterday signed into law a bill ([H.R. 7898](#)) PL 116-321 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**
- **Mitigation of other penalties**
- **No Increased Penalties for Not Having Recognized Cybersecurity Practices in Place**

"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."***

### Third Party Risk Management Program Considerations



- Does your organization have a third party risk management program (TPRM)? What is the governance structure and does that structure still make sense?
- Is there a formal process to incorporate cybersecurity in the TPRM program?
- Is there process to conduct periodic in-depth technical, legal, policy and procedural review of the TPRM 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?
- **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** to continuity of operations - Clinical, facilities, utilities, business (e.g. medical transcription, billing and coding, PPE supplies)
  - **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

©2021 American Hospital Association

*“Whenever there is a discussion about:*

- Data
- Technology
- Digital transformation
- Artificial intelligence
- Electronic medical records
- Sensitive data
- Medical devices
- Interoperability
- Clinically integrated care
- Business associates
- Mergers and Acquisitions



*...the conversation is not complete unless the discussion has also addressed the cybersecurity and risk issues which are embedded, often hidden, within these issues”*





**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 distinct cyber, criminal investigation and national security experience at the FBI and CIA to provide trusted strategic cyber and risk advisory services to the nations' hospitals and health systems.

[jriggi@aha.org](mailto:jriggi@aha.org)

(O) +1 202-626-2272  
(M) +1 202-640-9159

His trusted access to healthcare leaders and government agencies enhances John's unique national perspective on cyber and risk issues and greatly contributes to the AHA's policy and advocacy efforts. John represented the nation's hospitals in testimony before the Senate Homeland Security Committee hearing on cyber threats to hospitals in Dec. 2020.

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.

3



**Clay House**

*Chief Information Security Officer and  
Vice President of IT Risk Management,  
CareFirst BlueCross BlueShield*



## The Increasing Cybersecurity Risks in the IT Supply Chain





# SUPPLY CHAIN DISRUPTION



# SUPPLY CHAIN DISRUPTION



39

40

## DIGITAL SUPPLY CHAIN IS EVEN MORE SUSCEPTIBLE TO DISRUPTION

**50%** of attacks in 2019 used "island hopping"  
(CrowdStrike)

Chinese POS vendor raided by FBI for acting as **dropper**, **malware distribution**, and **C2**  
(Krebs On Security)

**55%** of organizations see DDoS attacks against APIs monthly – **49%** see injection  
(Radware)

**75%** of codebases contained malware; **67%** had license conflicts; **33%** contained unlicensed code  
(Synopsys 2020 Open Source Security & Risk Analysis)

**Bloomberg Businessweek**

### The Big Hack

How China used a tiny chip to infiltrate America's top companies





## SUPPLY CHAIN RISKS



Counterfeits

Integrity

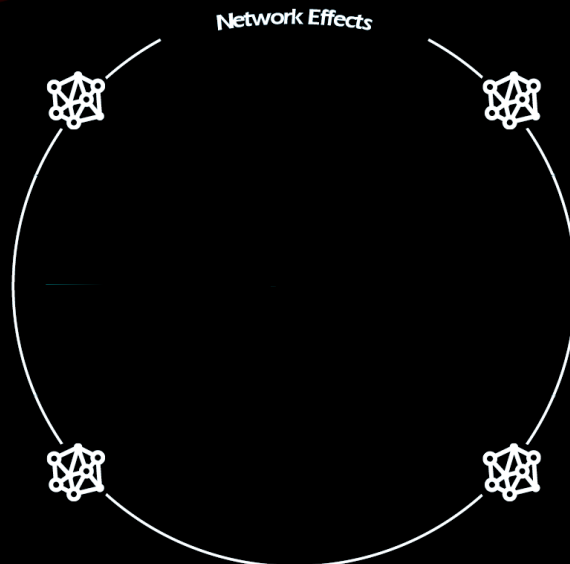
Availability

Tampering

Theft

Lifecycle

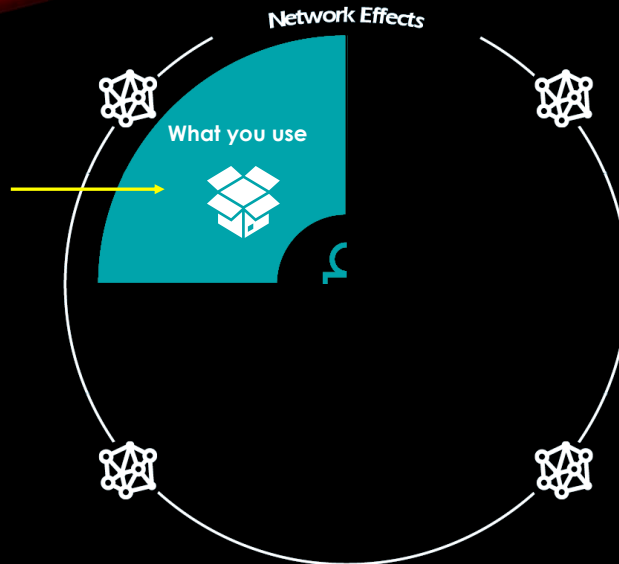
## IT SUPPLY CHAIN



## IT SUPPLY CHAIN

43

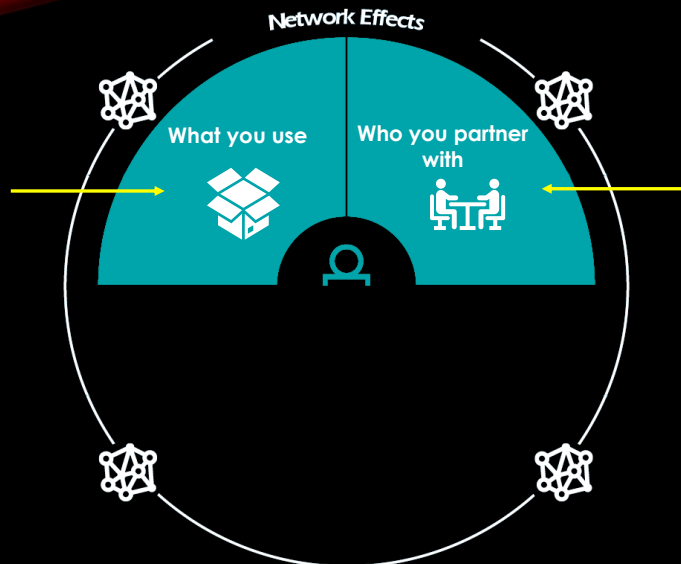
- Hardware/Software
- Components
- Libraries/Open Source
- APIs
- Cloud/Hosting Providers
- Utilities



## IT SUPPLY CHAIN

44

- Hardware/Software
- Components
- Libraries/Open Source
- APIs
- Cloud/Hosting Providers
- Utilities

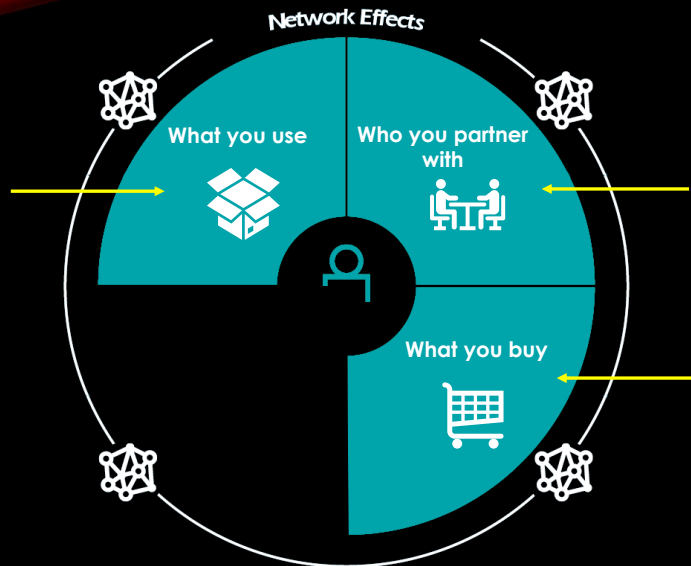


- Business Partners
- Services they provide
- Data you share/integrations
- Strategic vs Operational vs Commodity
- Financials

## IT SUPPLY CHAIN

45

- Hardware/Software
- Components
- Libraries/Open Source
- APIs
- Cloud/Hosting Providers
- Utilities

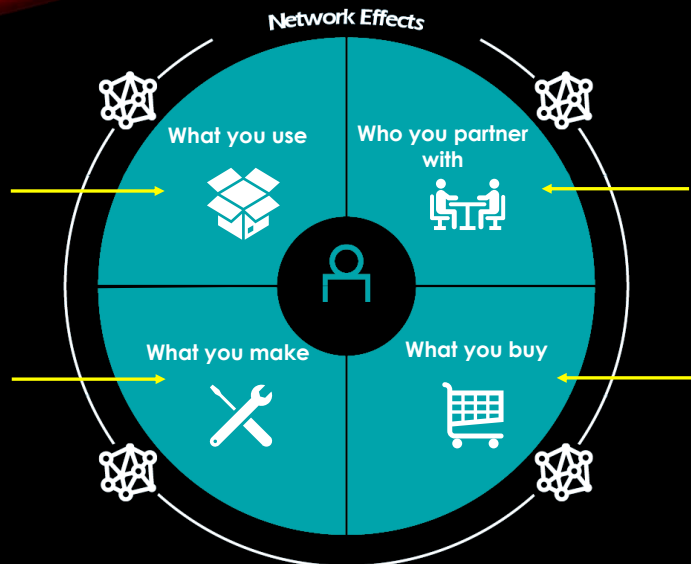


- Business Partners
- Services they provide
- Data you share/integrations
- Strategic vs Operational vs Commodity
- Financials
- Supplies
- Hardware/Software
- Services
- Disposal
- Quality Control
- Service Level & Operational Level Agreements

## IT SUPPLY CHAIN

46

- Hardware/Software
- Components
- Libraries/Open Source
- APIs
- Cloud/Hosting Providers
- Utilities



- Business Partners
- Services they provide
- Data you share/integrations
- Strategic vs Operational vs Commodity
- Financials
- Supplies
- Hardware/Software
- Services
- Disposal
- Quality Control
- Service Level & Operational Level Agreements

INTEGRATE CYBER  
SUPPLY CHAIN RISK  
MANAGEMENT  
WITH EXISTING RISK  
AND VENDOR  
MANAGEMENT  
INITIATIVES

Cyber Supply  
Chain  
Management



INTEGRATE CYBER  
SUPPLY CHAIN RISK  
MANAGEMENT  
WITH EXISTING RISK  
AND VENDOR  
MANAGEMENT  
INITIATIVES

Cyber Supply  
Chain  
Management



Understand Supply Chain  
(Internal & External)



INTEGRATE CYBER  
SUPPLY CHAIN RISK  
MANAGEMENT  
WITH EXISTING RISK  
AND VENDOR  
MANAGEMENT  
INITIATIVES

Cyber Supply  
Chain  
Management



Understand Supply Chain  
(Internal & External)



Categorize Suppliers  
(Strategic, Core, Commodity)

INTEGRATE CYBER  
SUPPLY CHAIN RISK  
MANAGEMENT  
WITH EXISTING RISK  
AND VENDOR  
MANAGEMENT  
INITIATIVES

Cyber Supply  
Chain  
Management



Understand Supply Chain  
(Internal & External)

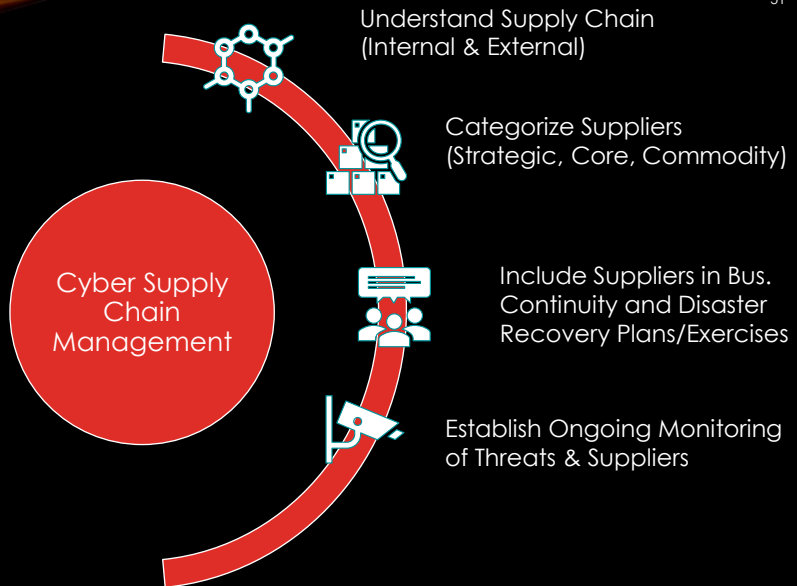


Categorize Suppliers  
(Strategic, Core, Commodity)

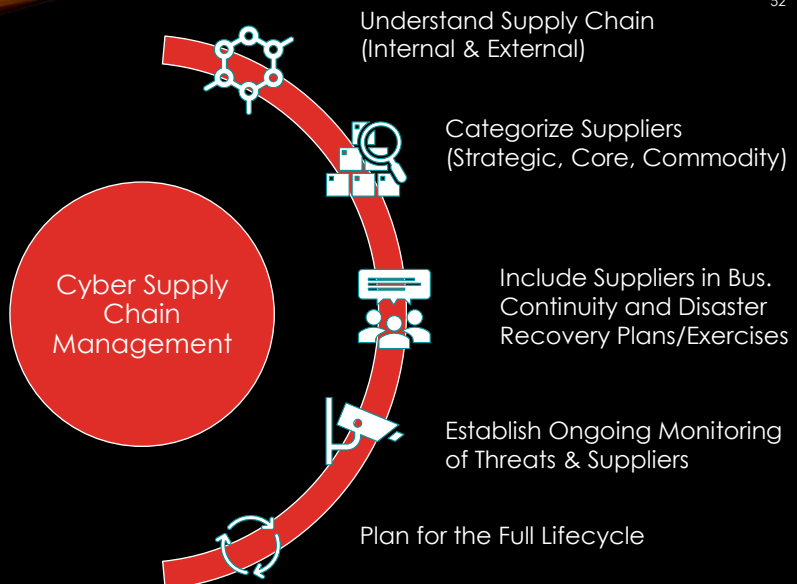


Include Suppliers in Bus.  
Continuity and Disaster  
Recovery Plans/Exercises

INTEGRATE CYBER  
SUPPLY CHAIN RISK  
MANAGEMENT  
WITH EXISTING RISK  
AND VENDOR  
MANAGEMENT  
INITIATIVES



INTEGRATE CYBER  
SUPPLY CHAIN RISK  
MANAGEMENT  
WITH EXISTING RISK  
AND VENDOR  
MANAGEMENT  
INITIATIVES



# PROTECT THE IT SUPPLY CHAIN

53

## Goods We Buy

- Software
  - Open-Source management and practices like SAFECODE
  - Must have defined processes to secure their build process and distribution
  - Restrict build & support to countries not on US Restrictions List
  - ISO 27034 Application Security Standards or similar
- Hardware
  - NIST 800-147B for BIOS security
  - Defense Federal Acquisition Regulation Supplement (DFARS) Contractor Counterfeit Electronic Part Detection and Avoidance (252.246-7007)
  - Transported Asset Protection Association guidelines (TAPA FSR)
  - Customer-Trade Partnership Against Terrorism (C-TPAT)
  - No Development or Manufacturing in US Restricted countries

## Services We Buy

- Restrict Services to those provided in countries not on US Restrictions List
- Use of Jump Servers for privileged access
- Restrict access to VDI or other controlled mechanism – no VPN
- End-point standards
- Restrict Data access, persistence, and transit to appropriate geographies
- Access to Sensitive data only in approved Offshore Development Centers or others as approved via Risk Acceptance Process
- Require background checks
- Assess Availability (e.g. DR, DDoS, etc.)
- Assess Integrity (e.g. ACID Transactions, business resumption, etc.)
- Assess Confidentiality (e.g. traditional SIG questions)

## What We Build & Deploy

- Software
  - Manage Open Source
  - Secure SDLC practices
  - Automated build & deploy
  - Include only approved libraries
  - Maintain currency
  - Patch regularly
  - Maintain Build Bill-of-Materials
  - Contextual authentication/authorization
  - Asset Management
- Infrastructure
  - CIS/PCI/FedRAMP Configuration Benchmarks
  - Standard configurations automatically built from approved mount points
  - Only approved software
  - Patch regularly
  - Maintain currency
  - Asset Management

# QUESTIONS

Clay House

[clay.house@carefirst.com](mailto:clay.house@carefirst.com)

54



## Roundtable Discussion

### *Best Practices for Third-Party Risk Management*



**Rick Moore, Moderator, Founder and Chief Executive Officer, MTC Group, LLC**

**Lee Barrett, Executive Director and Chief Executive Officer, EHNAC**

**Brandon Neiswender, Vice President and Chief Operating Officer, CRISP**

**Tressa Springmann, Senior Vice President and Chief Information and Digital Officer, LifeBridge Health**

**Mike Zbarsky, Senior Chief Information Security Officer Advisor, Hartman Executive Advisors**



## Thank You

For more information, view the recording [\*here\*](#).