STOPPING DIGITAL THIEVES: THE GROWING THREAT OF RANSOMWARE

HYBRID HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

JULY 20, 2021

Serial No. 117–44

Published for the use of the Committee on Energy and Commerce
govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
52–136 PDF WASHINGTON : 2023

COMMITTEE ON ENERGY AND COMMERCE

FRANK PALLONE, JR., New Jersey
Chairman

BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
DIANA DEGETTE, Colorado
MIKE DOYLE, Pennsylvania
JAN SCHAKOWSKY, Illinois
G. K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
PAUL TONKO, New York
YVETTE D. CLARKE, New York
KURT SCHRADER, Oregon
TONY CÁRDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan
MARC A. VEASEY, Texas
ANN M. KUSTER, New Hampshire
ROBIN L. KELLY, Illinois, *Vice Chair*
NANETTE DIAZ BARRAGÁN, California
A. DONALD MCEACHIN, Virginia
LISA BLUNT ROCHESTER, Delaware
DARREN SOTO, Florida
TOM O'HALLERAN, Arizona
KATHLEEN M. RICE, New York
ANGIE CRAIG, Minnesota
KIM SCHRIER, Washington
LORI TRAHAN, Massachusetts
LIZZIE FLETCHER, Texas

CATHY MCMORRIS RODGERS, Washington
Ranking Member
FRED UPTON, Michigan
MICHAEL C. BURGESS, Texas
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
BRETT GUTHRIE, Kentucky
DAVID B. MCKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
TIM WALBERG, Michigan
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina
GARY J. PALMER, Alabama
NEAL P. DUNN, Florida
JOHN R. CURTIS, Utah
DEBBBIE LESKO, Arizona
GREG PENCE, Indiana
DAN CRENSHAW, Texas
JOHN JOYCE, Pennsylvania
KELLY ARMSTRONG, North Dakota

PROFESSIONAL STAFF

JEFFREY C. CARROLL, *Staff Director*
TIFFANY GUARASCIO, *Deputy Staff Director*
NATE HODSON, *Minority Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

DIANA DEGETTE, Colorado
Chair

ANN M. KUSTER, New Hampshire
KATHLEEN M. RICE, New York
JAN SCHAKOWSKY, Illinois
PAUL TONKO, New York
RAUL RUIZ, California
SCOTT H. PETERS, California, *Vice Chair*
KIM SCHRIER, Washington
LORI TRAHAN, Massachusetts
TOM O'HALLERAN, Arizona
FRANK PALLONE, JR., New Jersey *(ex officio)*

H. MORGAN GRIFFITH, Virginia
Ranking Member
MICHAEL C. BURGESS, Texas
DAVID B. MCKINLEY, West Virginia
BILLY LONG, Missouri
NEAL P. DUNN, Florida
JOHN JOYCE, Pennsylvania
GARY J. PALMER, Alabama
CATHY MCMORRIS RODGERS, Washington
(ex officio)

C O N T E N T S

STOPPING DIGITAL THIEVES: THE GROWING THREAT OF RANSOMWARE

TUESDAY, JULY 20, 2021

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:34 a.m.., in the John D. Dingell Room 2123, Rayburn House Office Building, and remotely via Cisco Webex online video conferencing, Hon. Diana DeGette (Chair of the subcommittee) presiding.

Members present: Representatives DeGette, Kuster, Rice, Schakowsky, Tonko, Ruiz, Peters, Schrier, Trahan, O'Halleran, Pallone (ex officio), Griffith (subcommittee ranking member), Burgess, McKinley, Dunn, Joyce, Palmer, and Rodgers (ex officio).

Also present: Representative McNerney.

Staff present: Jeffrey C. Carroll, Staff Director; Austin Flack, Policy Analyst; Waverly Gordon, General Counsel; Tiffany Guarascio, Deputy Staff Director; Perry Hamilton, Clerk; Rebekah Jones, Counsel; Zach Kahan, Deputy Director, Outreach and Member Service; Chris Knauer, Oversight Staff Director; Kevin McAloon, Professional Staff Member; Will McAuliffe, Counsel; Jon Monger, Counsel; Kaitlyn Peel, Digital Director; Kylea Rogers, Staff Assistant; Andrew Souvall, Director of Communications, Outreach, and Member Services; Benjamin Tabor, Junior Professional Staff Member; Sarah Burke, Minority Deputy Staff Director; Marissa Gervasi, Minority Counsel, Oversight and Investigations; Nate Hodson, Minority Staff Director; Peter Kielty, Minority General Counsel; Emily King, Minority Member Services Director; Bijan Koohmaraie, Minority Chief Counsel; Clare Paoletta, Minority Policy Analyst, Health; Alan Slobodin, Minority Chief Investigative Counsel, Oversight and Investigations; Michael Taggart, Minority Policy Director.

Ms. DEGETTE. The Subcommittee on Oversight and Investigations hearing will now come to order.

And I must say we are all extremely glad to be back in person. Welcome back to our in-person Members, and welcome to our Members who are here remotely.

Today our subcommittee is having a hearing called "Stopping Digital Thieves: The Growing Threat of Ransomware," and the hearing will examine the growing threats posed by ransomware to U.S. businesses and critical infrastructure, and we will discuss recommendations for combating those threats.

Due to the COVID–19 public health emergency, as I said, members can participate either in person or remotely. And if members are not vaccinated—I think everybody here is, but if they are not, they must wear a mask and be socially distanced. They can remove their mask when they are recognized. And again, anyone else present in this committee room, including press, must wear a mask and be socially distanced or be vaccinated.

For Members who are participating remotely, your microphones will be set on mute for the purposes of eliminating any background noise. Members participating remotely will need to unmute our microphone each time you wish to speak. Please note once you unmute your microphone, anything that is said in Webex will be heard over the loudspeakers in the committee room, and may—and will be on C–SPAN. So just—we have experienced that some in the last few weeks, so just be aware.

Because Members are participating from different locations, all recognition of Members, such as for questions, will be in the order of subcommittee seniority.

And as always, if at any time during the hearing I am unable to chair the hearing, the vice chair of the subcommittee, Mr. Peters, will serve as Chair until I am able to return.

Documents for the record can be sent to Austin Flack at the email address we have provided to staff. All documents will be entered into the record at the conclusion of the hearing.

And the Chair will now recognize herself for the purposes of making an opening statement.

OPENING STATEMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Today's hearing tackles a growing threat to our national security, economic security, and public safety, and that is ransomware. In short, a ransomware attack occurs when criminals break into a network, lock it down, steal data, and then extort everyday Americans into, often, massive ransom payments. These digital thieves are infiltrating our schools, hospitals, food suppliers, and critical infrastructure companies.

The seriousness of the issue is hard to overstate. All you need to do is to look at the front page of the newspaper to see the problem is getting worse. Earlier this year, the whole country watched as a single attack on Colonial Pipeline's information technology system shut down the gas and fuel supply to the entire eastern seaboard. This attack alone caused massive gas lines, hoarding—and many stations ran out of fuel.

Last year, more than 560 healthcare organizations, many of which were already reeling from COVID–19, found themselves victims of ransomware. Hospital systems had to cancel appointments and surgeries, reroute ambulances, and delay critical treatment for cancer patients.

Our food supply was also recently in the crosshairs when, a few weeks ago, cyber criminals attacked the company JBS, the largest meat producer in the world, threatening a vital link in our Nation's food supply.

And these are just the attacks that we know about. Companies and organizations wanting to save face and maintain the confidence of the public often meet the ransom demands in secret—always pay in hard-to-trace cryptocurrency.

Like many—or almost always doing that.

Like many of the issues we have examined in the last year and a half, like vaccine confidence and the state of our public health infrastructure, the ransomware challenge is not new, but it has been exacerbated by the COVID–19 crisis. Cyber criminals thrive on exploiting vulnerabilities in our networks. The explosion of remote work and remote school during the pandemic greatly expanded these vulnerabilities.

For example, experts are projecting our K through 12 schools will face a nearly 90 percent increase in the number of ransomware attacks just this year. And it is not just the breadth of targets that is growing. The average size of ransom payments has also increased, reaching an estimated $312,000 per organization in 2020.

Simply put, the time to address this crisis is now. To win the fight, we need not just a whole-of-government approach but, really, a whole-of-society approach. Both the public and private sectors have a role to play.

First, the public sector must continue to develop and to lead a well-coordinated response. This includes coordination across U.S. Government agencies and private industry, and working closely with our international partners. With President Biden's recent actions, we are seeing the outlines of such a response take place, and the administration is rightfully treating the issue as a national security threat.

For example, our Nation's first Cyber Director was sworn in just last week, and our Federal agencies are conducting a series of collaborations with the private sector to address ransomware and other critical cyber issues. I applaud the efforts that the Cybersecurity and Infrastructure Security Agency announced last week. That agency is working to ensure that small to medium-sized businesses across our country are—that are victimized by ransomware attacks have the resources needed to minimize harm and restart operations.

Internationally, it is imperative that countries no longer provide safe haven for these criminal organizations. And President Biden has vowed that America will take any necessary action to defend its people and its critical infrastructure. The President already addressed the international part of this issue head on, both at the G7 summit and in multiple one-on-one conversations with Russian President Vladimir Putin. And just yesterday, the U.S., along with our European Union and NATO allies, condemned China for its state-sponsored cyber activities, including ransomware attacks.

While the administration's actions are promising, the public sector cannot defeat ransomware on its own. For example, following a ransomware attack, too often we hear of lax cybersecurity requirements or known vulnerabilities that were ignored. We have had a number of classified briefings where we heard about that. And it is critical that companies of all sizes address chronic underinvestment in cyber defenses. Better cyber hygiene, more cyber ex-

pertise, and meaningful information sharing will address this threat.

And Congress also has an important role to play in this. Just last week, key government cyber experts indicated that additional executive authorities may be needed to ensure the private sector gets to where it needs to be.

As a committee, we must ensure that the executive branch has the tools and authorities to mandate effective cybersecurity requirements for vulnerable industries, modernize our defenses, and ensure that we are postured to compete with those threats. There is no shortage of policy proposals being discussed. Those include mandatory reporting of ransomware attacks, prohibitions on ransom payments, and increased regulation of critical industries and cybersecurities.

This morning, I want to say, we have a terrific panel of experts who have spent decades addressing ransomware and other cyber crimes, and I am really looking forward to hearing from all of you.

One thing is certain: This problem is not going away. The problem has grown exponentially over the last decade, and we must respond in kind. We must do everything we can to fix our vulnerabilities and to protect our critical industries.

[The prepared statement of Ms. DeGette follows:]

PREPARED STATEMENT OF HON. DIANA DEGETTE

Good morning. It is good to see many of you in person, after being remote for so long.

Today's oversight hearing tackles a growing threat to our national security, economic security, and public safety, which is ransomware.

In short, a ransomware attack occurs when criminals break into a network, lock it down, steal data, and then extort everyday Americans into often massive ransom payments.

These digital thieves are infiltrating our schools, hospitals, food suppliers, and critical infrastructure companies.

The seriousness of the issue is hard to overstate. All you need to do is look at the front page of the newspaper to see that the problem is getting worse.

Earlier this year, the country watched as a single attack on Colonial Pipeline's information technology system shut down the gas and fuel supply to nearly the entire eastern seaboard.

This attack alone caused massive gas lines, hoarding, and many stations ran out of fuel.

Last year, more than 560 healthcare organizations—many of which were already reeling from the COVID–19 pandemic—found themselves victims of ransomware.

Hospital systems had to cancel appointments and surgeries, reroute ambulances, and delay critical treatment for cancer patients.

Our food supply was recently in the crosshairs, too. Just a few weeks ago, cyber criminals attacked the company JBS, the largest meat producer in the world, threatening a vital link in the nation's food supply.

And these are just the attacks we know about.

Companies and organizations wanting to save face and maintain the confidence of the public often meet the ransom demands in secret, almost always paying in hard-to-trace cryptocurrency.

Like many of the issues we have examined in the last year and a half-such as vaccine confidence and the state of our public health infrastructure-the ransomware challenge is not new, but it has been exacerbated by the COVID–19 crisis.

Cybercriminals thrive on exploiting vulnerabilities in our networks. The explosion of remote work and remote school during the COVID–19 pandemic greatly expanded those vulnerabilities.

For example, experts are projecting our K 0912 schools will face a nearly 90 percent increase in the number of ransomware attacks just this year.

And it is not just the breadth of targets that is growing. The average size of ransom payments has also increased, reaching an estimated $312,000 per organization in 2020.

Simply put, the time to address this issue is now.

To win this fight, we need not just a whole-of-government approach, but a whole-ofsociety approach. Both the public and private sectors have important roles to play.

First, the public sector must continue to develop and lead a well-coordinated response.

This includes coordination across US government agencies and private industry and working closely with our international partners.

With President Biden's recent actions, we are seeing the outlines of such a response take shape, and the Administration is rightfully treating the issue as a national security threat.

For example, our nation's first National Cyber Director was sworn in just last week. And our federal agencies are conducting a series of collaborations with the private sector to address ransomware and other critical cyber issues.

I applaud the efforts that the Cybersecurity and Infrastructure Security Agency (CISA) announced last week. CISA is working to ensure that small-to-medium sized businesses across our country that are victimized by ransomware attacks have the resources needed to minimize harm and restart operations.

Internationally, it is imperative that countries no longer provide safe haven for these criminal organizations, and President Biden has vowed that America will take any necessary action to defend its people and its critical infrastructure.

In fact, we have already seen the President address the international part of this issue head-on, both at the G7 summit and in multiple one-on-one discussions with Russian President Vladimir Putin. And, just yesterday, the United States, along with our European Union and NATO allies, condemned China for its state-sponsored cyber activities, including ransomware attacks.

While the Administration's actions are promising, the public sector cannot defeat ransomware on its own.

For example, following a ransomware attack, we too often hear of lax cybersecurity requirements or known vulnerabilities that were ignored.

It is critical that private companies of all sizes address chronic underinvestment in cyber defenses. Better cyber hygiene, more cyber expertise, and meaningful information sharing will be necessary to address this threat.

And Congress has an important role to play in this. In fact, just last week, key government cyber experts indicated that additional executive authorities may be needed to ensure the private sector gets to where it needs to be.

As a Committee, we must ensure the executive branch has the tools and authorities it needs to mandate effective cybersecurity requirements for our vulnerable industries, modernize our defenses, and ensure we are postured to compete with these threats.

There is no shortage of policy proposals being discussed. These include mandatory reporting of ransomware attacks, prohibitions on ransom payments, and increased regulation of critical industries and cryptocurrencies.

This morning we have a terrific panel of experts who have spent decades addressing ransomware and other cybercrimes, and I look forward to hearing from our witnesses on these and other ideas. One thing is certain: this problem is not going away.

The ransomware threat has grown exponentially over the last decade, and our response must grow in-kind. We must do everything we can as a nation to fix our vulnerabilities and protect our critical industries.

Thank you.

Ms. DEGETTE. And I want to thank all of you and recognize our ranking member for 5 minutes for the purposes of an opening statement.

OPENING STATEMENT OF HON. H. MORGAN GRIFFITH, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF VIRGINIA

Mr. GRIFFITH. Thank you very much, Chair DeGette, for holding this hearing, and especially considering the recent increase in ransomware attacks across our Nation, including high-profile attacks such as Kaseya, Colonial Pipeline, and SolarWinds.

I also want to thank the witnesses for taking your time to join us today.

Cybersecurity is integral to all organizations,and should be treated as a priority for maintaining the health and security of an organization as well as any other individuals or entities that are affiliated with that organization. The need for more rigorous cybersecurity protections exists across all industries, including healthcare, oil, gas, water, and electricity. Any network with vulnerabilities can be subject to a cyber threat, and the frequency of cyber attacks is increasing exponentially.

The reach of most recent cyber attacks demonstrates how serious this issue is. For example, the Colonial Pipeline, one of the most critical pieces of energy infrastructure, was the target of a ransomware attack in May. The attack halted all pipeline operations and caused supply disruption up and down the East Coast for over a week, which led to higher gas prices and longer lines. More recently, over the Fourth of July holiday, the Kaseya supply chain ransomware hack affected medium and small-sized businesses globally, including in my district. Both of these attacks appear to be Russia linked, which is the most recent showing of cyber threat Russia poses to the United States.

Although the recent attacks appear to be linked to Russia, adversaries of cyber attacks originate in different foreign nations, varying in the size of the criminal enterprises. And their approaches to gaining access to systems range in their level of sophistication.

However, no one industry or part of our Nation's critical infrastructure is immune to the threats posed by these malicious actors. Cyber attacks have the potential to cause real harm, depending on the severity and the target. In healthcare in particular, direct harm is almost a certainty. Any time information in the—in healthcare and public sector is compromised, it poses a risk to providers, patients, and those who serve and supply them.

But it is not just data and privacy that are compromised. Ransomware attacks can have a significant impact on patient health. For example, in May a ransomware attack hit a San Diego-based healthcare system, Scripps Health, and the cyber criminals stole data on close to 150,000 patients. This forced Scripps Health to not be fully up and running until a month after the cyber attack—or cyber—ransomware attack. These types of incidents are detrimental to the care available to the community and put a major strain on the surrounding healthcare system and the region. As the ransomware recovery timeframes increase from days to months, the amount of damages skyrockets. In a hospital's case, that can mean the difference between life and death.

The recent ransomware attacks are providing lessons about the importance of cybersecurity. These systems are fragile. Although it is impossible for a system to be completely resilient against any cyber attack, there is much more the Federal Government, cybersecurity organizations, cyber victim organizations, and the private sector can do to detect, respond, and recover from ransomware threats. This is a shared responsibility, and we need everyone to do their part.

The United States has great cyber experts found in both the Federal Government and the private sector that supply the key build-

ing blocks to revamping our Nation's cybersecurity. The Federal Government has strong resources to prevent attacks, respond to attacks, and hold criminals accountable. We just need to see more of it, and we need to make better uses of our resources.

Coupled with the Federal Government resources, we have private-sector firms that offer cybersecurity consulting for a range of organizations at different entry points in the cybersecurity cycles and at different levels of cybersecurity risk. Moreover, we have experts that focus exclusively on industrial control systems and operation technology cybersecurity. We also have nonprofit networks that design solutions for emerging threats, and private companies with specialized professionals to disrupt criminal enterprise.

We need to ensure an open line of communication, coordination, and information sharing in the cyber world and delineate proper responsibilities for developing cybersecurity strategies to the appropriate entities.

It is impossible to eliminate all cyber threats to our Nation. However, we need to do more to better prevent and detect ransomware attacks so that we can thwart the worst-case outcomes and scenarios, especially when it comes to critical infrastructure.

I look forward to hearing from the witnesses here today, given their expertise and experiences in this space, and I am eager to learn more about what we can do to help prevent and detect future ransomware attacks.

I yield back. Thank you, Madam Chair.

[The prepared statement of Mr. Griffith follows:]

PREPARED STATEMENT OF HON. H. MORGAN GRIFFITH

Thank you, Chair DeGette, for holding this hearing, especially considering the recent increase in ransomware attacks across our nation, including high-profile attacks such as Kaseya, Colonial Pipeline, and SolarWinds. I also want to thank the witnesses for taking the time to join us today.

Cybersecurity is integral to all organizations and should be treated as a priority for maintaining the health and security of an organization, as well as any other individuals or entities that are affiliated with that organization. The need for more rigorous cybersecurity protections exists across all industries, including health care, oil, gas, water, and electricity. Any network with vulnerabilities can be subject to a cyber threat, and the frequency of cyberattacks is increasing exponentially.

The reach of the most recent cyberattacks demonstrates how serious this issue is. For example, the Colonial Pipeline, one of the most critical pieces of energy infrastructure, was the target of a ransomware attack in May. The attack halted all pipeline operations and caused supply disruption up and down the East Coast for over a week - which led to higher gas prices and longer lines. More recently, over the Fourth of July holiday, the Kaseya supply chain ransomware hack affected medium and small-sized business globally. Both of these attacks appear to be Russia-linked, which is the most recent showing of the cyber threat Russia poses to the U.S.

Although the recent attacks appear to be linked to Russia, adversaries of cyberattacks originate in different foreign nations, vary in the size of the criminal enterprises, and their approaches to gaining access to systems range in their level of sophistication. However, no one industry or part of our nation's critical infrastructure is immune to the threats posed by these malicious actors. Cyberattacks have the potential to cause real harm, depending on the severity and target.

In health care in particular, direct harm is almost a certainty. Anytime information in the health care and public health sector is compromised, it poses a risk to providers, patients, and all those who serve and supply them. But it is not just data and privacy that are compromised - ransomware attacks can have a significant impact on patient health.

For example, in May, a ransomware attack hit a San-Diego based health system, Scripps Health, and the cybercriminals stole data on close to 150,000 patients. This forced the Scripps Health system to not be fully up and running until a month after

the ransomware attack. These types of incidents are detrimental to the care available to the community and put a major strain on the surrounding health care system in the region. As the ransomware recovery timeframes increase from days to months, the amount of damage skyrockets. In a hospital's case, that can mean a difference between life and death.

The recent ransomware attacks are providing lessons about the importance of cybersecurity. These systems are fragile. Although it is impossible for a system to be completely resilient against any cyberattack, there is much more the federal government, cybersecurity organizations, cyber victim organizations, and the private sector can do to detect, respond, and recover from ransomware threats. This is a shared responsibility and we need everyone to do their part.

The United States has great cyber experts found in both the federal government and the private sector that supply the key building blocks to revamping our nation's cybersecurity. The federal government has strong resources to prevent attacks, respond to attacks, and hold criminals accountable. We just need to see more of it-and we need to make better use of these resources.

Coupled with the federal government resources, we have private sector firms that offer cybersecurity consulting for a range of organizations at different entry points in their cybersecurity cycles and at different levels of cybersecurity risk. Moreover, we have experts that focus exclusively on industrial control systems (ICS) and operations technology (OT) cybersecurity. We also have non-profit networks that design solutions for emerging threats and private companies with specialized professionals to disrupt criminal enterprises. We need to ensure an open line of communication, coordination, and information sharing in the cyberworld and delineate proper responsibilities for developing cybersecurity strategies to the appropriate entities.

It is impossible to eliminate all cyber threats to our nation. However, we need to do more to better prevent and detect ransomware attacks so that we can thwart worst-case outcomes, especially when it comes to critical infrastructure. I look forward to hearing from the witnesses here today given their expertise and experiences in this space and am eager to learn more about what we can do to help prevent and detect future ransomware attacks. I yield back.

Ms. DEGETTE. I thank the gentleman. The Chair now recognizes the chairman of the full committee, Mr. Pallone, for 5 minutes.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you. Thank you, Chairwoman DeGette.

The Energy and Commerce Committee has a long history of examining cybersecurity on a bipartisan basis. Over the past several years, we have held hearings on strengthening cybersecurity in the healthcare and energy sectors. We have also been regularly briefed by agencies on a variety of critical concerns related to both previous and recent cybersecurity threats and attacks. While we have made progress, it is clear much more needs to be done to address the ongoing threats we see nearly every day.

One area of particular and growing concern is ransomware, the topic of today's hearing. Ransomware is a malicious cybersecurity attack that paralyzes victim organizations. The attack freezes computer systems and holds data hostage until a ransom payment is received. Ransomware used to be considered a nuisance crime, impacting only an individual computer. But in recent years it has evolved to affect the entire networks of organizations and even governments, extorting entities for enormous sums of money.

Increasingly, criminals deploying ransomware are not just freezing the data of victim organizations but are also pilfering sensitive business and consumer data. On top of locking down computer networks, they also threaten to release the stolen data as an additional method to leverage a ransom payment.

Just in the past few months, we have seen a surge of ransomware attacks that at times have brought aspects of normal life and commerce to a standstill. The ransomware attack on the Colonial Pipeline disrupted oil and gas supplies on the eastern seaboard, causing many gas stations to run out of fuel, prices to skyrocket, and grounding air traffic. Other recent attacks have threatened local police departments, including the DC Metropolitan Police, and victimized schools, local governments, and hospitals already grappling with the COVID–19 pandemic.

I also want to underscore that the challenges brought on by these attacks are particularly acute for small businesses, many of which lack dedicated information technology staff and the resources and are just trying to keep their businesses operating. And these victims may have no idea who to turn to if their data is subject to a ransomware attack. We simply can't leave victim organizations on their own in figuring out how to defend against and respond to these cyber criminals.

So given the huge scale and scope of these threats, I am pleased that President Biden is taking decisive steps to tackle this challenge. Just last week, the administration announced a new website, StopRansomware.gov, that is meant to provide a one-stop hub of ransomware resources for individuals and businesses. The website outlines the simple steps small businesses can take to protect their networks and provides guidance to these organizations on how to respond to ransomware incidents.

The President is also leading a whole-of-government effort to disrupt ransomware campaigns and go after the criminals who launch them. The administration's strategy announced last week builds on an effort launched by the White House in May that will make it more difficult for criminals to transfer funds using cryptocurrency, helping make U.S. institutions more resistant to hacking, and urge international cooperation.

But the Biden administration can't address this enormous challenge on its own. Congress must also take action, and that is why this oversight hearing is so important today. I look forward to hearing from our witnesses who have dedicated their careers to cybersecurity. They are uniquely positioned to make recommendations on the types of policies needed to defend against future attacks, and I am interested in their ideas as we explore potential solutions that will help further protect our Nation's critical infrastructure networks, businesses, and consumers.

So with that, I thank the chairwoman for holding this hearing. I yield back, Madam Chair.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

The Energy and Commerce Committee has a long history of examining cybersecurity on a bipartisan basis. Over the past several years, we have held hearings on strengthening cybersecurity in the health care and energy sectors. We have also been regularly briefed by agencies on a variety of critical concerns related to both previous and recent cybersecurity threats and attacks.

While we have made progress, it is clear much more needs to be done to address the ongoing threats we see nearly every day.

One area of particular and growing concern is ransomware, the topic of today's hearing. Ransomware is a malicious cybersecurity attack that paralyzes victim orga-

nizations. The attack freezes computer systems and holds data hostage until a ransom payment is received.

Ransomware used to be considered a nuisance crime impacting only an individual computer. In recent years, however, it has evolved to affect the entire networks of organizations and even governments, extorting entities for enormous sums of money.

Increasingly, criminals deploying ransomware are not just freezing the data of victim organizations but are also pilfering sensitive business and consumer data. On top of locking down computer networks, they also threaten to release the stolen data as an additional method to leverage a ransom payment.

In just the past few months, we have seen a surge of ransomware attacks that at times have brought aspects of normal life and commerce to a standstill.

The ransomware attack on the Colonial Pipeline disrupted oil and gas supplies on the eastern seaboard, causing many gas stations to run out of fuel, prices to skyrocket, and grounding air traffic.

Other recent attacks have threatened local police departments, including the DC Metropolitan Police, and victimized schools, local governments, and hospitals already grappling with the COVID–19 pandemic.

I also want to underscore that the challenges brought on by these attacks are particularly acute for small businesses, many of which lack dedicated information technology staff and resources and are just trying to keep their businesses operating. These victims may have no idea who to turn to if their data is subject to a ransomware attack. We simply cannot leave victim organizations on their own when figuring out how to defend against and respond to these cyber criminals.

Given the huge scale and scope of these threats, I am pleased that President Biden is taking decisive steps to tackle this challenge. Just last week the Administration announced a new website, StopRansomware.gov, that is meant to provide a one-stop hub of ransomware resources for individuals and businesses. The website outlines the simple steps small businesses can take to protect their networks and provides guidance to these organizations on how to respond to ransomware incidents.

The President is also leading a whole-of-government effort to disrupt ransomware campaigns and go after the criminals who launch them.

The Administration's strategy announced last week builds on an effort launched by the White House in May. It will make it more difficult for criminals to transfer funds using cryptocurrency, help make U.S. institutions more resistant to hacking, and urge international cooperation.

But the Administration cannot address this enormous challenge on its own. Congress must also take action, and that's why this oversight hearing is so important today. I look forward to hearing from our witnesses who have dedicated their careers to cybersecurity. They are uniquely positioned to make recommendations on the types of policies needed to defend against future attacks. I am interested in their ideas as we explore potential solutions that will help further protect our nation's critical infrastructure networks, businesses, and consumers.

With that, I thank the Chair for holding this hearing and I yield back.

Ms. DEGETTE. I thank the gentleman. The Chair now recognizes the ranking member of the full committee, Mrs. Rodgers, for 5 minutes for an opening statement.

OPENING STATEMENT OF HON. CATHY MCMORRIS RODGERS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WASHINGTON

Mrs. RODGERS. Thank you, Madam Chair. In recent months we have seen a significant increase in the ransomware attacks coming from Russia. In May, DarkSide, a ransomware group operating out of Russia, attacked the Colonial Pipeline, which accounts for about 45 percent of the East Coast's fuel. In June, REvil, another ransomware group operating in Russia, attacked GBS USA, which temporarily knocked out plants that process roughly one-fifth of our Nation's meat supply. Earlier this month REvil executed another ransomware attack, this time on American IT management

software company Kaseya, which affected hundreds of businesses across the globe.

While Russian—while the Russian President Putin may not be directly connected to these attacks, he refuses to crack down on them. White House Press Secretary Jen Psaki recently said that "responsible states do not harbor ransomware criminals." Well, Mr. President, Russia is not a responsible state, and greenlighting a pipeline for Putin after Russian cyber criminal attacks on one of the most critical pipelines in the United States certainly will not deter Russia.

But this threat is not unique to Russia. We know the Chinese Government engages in malicious cyber behavior too. Just yesterday the Biden administration publicly blamed hackers affiliated with China's main intelligence service for a far-reaching cyber attack on Microsoft. While this administration must do more, I applaud them for taking this step and publicly addressing the threat China poses.

The White House also recently announced a cross-government task force to combat the rise in ransomware attacks. President Biden's nominee to lead the Cybersecurity and Infrastructure Security Agency, Jen Easterly, was also unanimously concerned—confirmed, sorry. These are welcome steps.

I caution this administration, though, and this Congress, from consolidating cyber at one agency. Doing so is a wrong and dangerous approach, because it weakens an agency's ability to leverage their expertise in cyber preparedness for their specific and unique sectors. I urge the Biden administration to lean on that expertise.

Director Easterly, I urge you to rely on your colleagues at HHS, DOE, FCC, FTC, DOT, and others to address cyber threats in their sectors.

As the committee which oversees our economy's most critical sectors, we know firsthand the work of many of these Federal agencies around cyber. This committee itself has a history of working on cybersecurity issues to strengthen America's defenses against bad actors. The committee has conducted significant oversight over cyber incidences dating back to Target, the Target hack in 2013 and 2017. We brought in the Equifax CEO to answer for the hack of their systems that resulted in the loss of 143 million Americans' personal information.

In 2018, following dozens of briefings, hearings, letters, reports, and roundtables, the Republicans on this committee issued a cybersecurity strategy report that provided specific priorities for more effective protection against vulnerabilities.

Earlier this year we sent bipartisan letters to the Department of Energy, the Department of Commerce, the Department of Health and Human Services, the Environmental Protection Agency, and the National Telecommunications and Information Administration following the SolarWinds attack.

Cyber threats and ransomware attacks will only continue to grow, and it is important for this committee to continue to lead on cyber issues. The Colonial Pipeline attack underscored the committee's long work to ensure the secure, reliable delivery of energy. The Pipeline and LNG Facility Cybersecurity Preparedness Act, reintroduced by Energy Subcommittee Republican Leader Upton and

Chairman Rush, will provide DOE with strong, clear coordinating authorities to respond to future threats. And soon, our Consumer Protection and Commerce Subcommittee Republican leader, Gus Bilirakis, will introduce a bill to ensure the FTC is focused on ransomware attacks from abroad and working with foreign law enforcement agencies to hold those cyber criminals accountable.

Yet there is more to do. Energy and Commerce should continue to explore ways to identify and patch cybersecurity vulnerabilities before they are exploited. We should also encourage reporting by entities of cyber attacks to the Federal agencies who oversee them and consider certain liability protections for our critical infrastructure. This is an important and timely discussion.

Thank you, Madam Chair. I look forward to hearing from our esteemed witnesses.

Thank you, everyone. I yield back

[The prepared statement of Mrs. Rodgers follows:]

PREPARED STATEMENT OF HON. CATHY MCMORRIS RODGERS

RISE IN ATTACKS

In recent months, we have seen a significant increase in ransomware attacks coming from Russia.

• In May, DarkSide—a ransomware group operating out of Russia—attacked the Colonial Pipeline—which accounts for about 45 percent of the East Coast's fuel.

• In June, REvil [are-evil]—another ransomware group operating in Russian—attacked JBS USA, which temporarily knocked out plants that process roughly one-fifth of our nation's meat supply.

• Earlier this month, REvil [are-evil] executed another ransomware attack. This time on American IT management software company Kaseya [KUH-SAY-AH]—which affected hundreds of businesses across the globe.

While President Putin may not be directly connected to these attacks, he refuses to crack down on them.

White House Press Secretary Jen Psaki (saw-key) recently said that quote ″responsible states do not harbor ransomware criminals.″

Well, Mr. President, Russia is NOT a responsible state.

And greenlighting a pipeline for Putin after Russian cyber criminals attack one of our most critical pipelines certainly will not deter Russia.

But this threat is not unique to Russia.

We know the Chinese government engages in malicious cyber behavior too.

Just yesterday, the Biden administration publicly blamed hackers affiliated with China's main intelligence service for a far-reaching cyberattack on Microsoft.

While this administration must do more, I applaud them for taking this step and publicly addressing the threat China poses.

ADMIN RECENT ANNOUNCEMENTS

The White House also recently announced a cross-government task force to combat the rise in ransomware attacks.

President Biden's nominee to lead the Cybersecurity and Infrastructure Security Agency—Jen Easterly—was also unanimously confirmed.

These are all welcomed steps, but only if done right.

I caution this administration and this Congress from consolidating cyber at one agency.

Doing so is a wrong and dangerous approach because it weakens an agency's ability to leverage their expertise in cyber preparedness for their specific and unique sectors.

I urge the Biden Administration to lean on that expertise.

Director Easterly, I urge you to rely on your colleagues at HHS, DOE, the FCC, the FTC, DOT, and others to address cyber threats in their sectors.

E&C Cyber Work

As the Committee which oversees our economy's most critical sectors, we know firsthand the work many of these federal agencies have done on cyber.

This Committee itself has a history of working on cybersecurity issues to strengthen American defenses against bad actors.

The Committee has conducted significant oversight over cyber incidents dating back to the Target hack in 2013.

In 2017, we brought in the Equifax CEO to answer for the hack of their systems that resulted in the loss of 143 million Americans' personal information.

In 2018, following dozens of briefings, hearings, letters, reports, and roundtables, the Republicans on this committee issued a Cybersecurity Strategy Report that provided specific priorities for more effective protection against vulnerabilities.

Earlier this year, we sent bipartisan letters to the Department of Energy, the Department of Commerce, the U.S. Department of Health and Human Services, the Environmental Protection Agency and the National Telecommunications and Information Administration following the SolarWinds attack.

Cyberthreats and ransomware attacks will only continue to grow and it is important for this Committee to continue lead on cyber issues.

The Colonial pipeline attack underscored the Committee's long work to ensure the secure, reliable delivery of energy.

The Pipeline and LNG Facility Cybersecurity Preparedness Act, reintroduced by Energy Subcommittee Republican Leader Upton and Chairman Rush will provide DOE with strong, clear coordinating authorities to respond to future threats.

And soon, our Consumer Protection and Commerce Subcommittee Republican Leader Gus Bilirakis will introduce a bill to ensure the FTC is focused on ransomware attacks from abroad and working with foreign law enforcement agencies to hold those cybercriminals accountable.

Yet, there is more to do.

Energy and Commerce should continue to explore ways to identify and patch cybersecurity vulnerabilities before they are exploited...

...and we should also encourage reporting by entities of cyberattacks to the federal agencies who oversee them and consider certain liability protections for our critical infrastructure.

This is an important and timely discussion and I look forward to hearing from our esteemed witnesses. Thank you. I yield back.

Ms. DEGETTE. The Chair now asks unanimous consent that the Members' written opening statements be made part of the record. And without objection, so ordered.

I now want to introduce our witnesses for today's hearing: Kemba Walden, who is the assistant general counsel for Microsoft Corporation; Robert M. Lee, who is the chief executive officer of Dragos; Dr. Christian Dameff, assistant professor of emergency medicine, biomedical informatics and computer science, University of California, San Diego, medical director of cybersecurity, U.C. San Diego Health—we are not going to refer to that entire title every time we discuss it with you, but congratulations; Charles Carmakal, senior vice president and chief technology officer, FireEye-Mandiant; and Philip Reiner, chief executive officer, Institute for Security and Technology.

I want to thank all of you for appearing today, as I have said.

And I know you are aware the committee is holding an investigative hearing. And when doing so, we have the practice of taking testimony under oath. Does anyone here object to testifying under oath?

Let the record reflect the witnesses have responded no.

The Chair will then advise you that, under the rules of the House and the rules of the committee, you are entitled to be accompanied by counsel. Does anyone request to be accompanied by counsel today?

Let the record reflect that the witnesses have responded no.

If you would, please rise and raise your right hand, so that you may be sworn in.

[Witnesses sworn.]

Ms. DEGETTE. Let the record reflect that the witnesses have responded affirmatively.

Please be seated, and you are now under oath and subject to the penalties set forth in title 18, section 1001 of the U.S. Code.

The Chair will now recognize our witnesses for a 5-minute summary of their written statements.

There is a timer on the screen that will count down your time, and it will turn red when your 5 minutes have come to an end.

Let me first recognize Ms. Walden for 5 minutes.

STATEMENTS OF KEMBA WALDEN, ASSISTANT GENERAL COUNSEL, MICROSOFT CORPORATION DIGITAL CRIMES UNIT; ROBERT M. LEE, CHIEF EXECUTIVE OFFICER, DRAGOS; CHRISTIAN DAMEFF, M.D., ASSISTANT PROFESSOR OF EMERGENCY MEDICINE, BIOMEDICAL INFORMATICS, AND COMPUTER SCIENCE, UNIVERSITY OF CALIFORNIA SAN DIEGO; CHARLES CARMAKAL, SENIOR VICE PRESIDENT AND CHIEF TECHNICAL OFFICER, FIREEYE MANDIANT; AND PHILIP JAMES REINER, CHIEF EXECUTIVE OFFICER, INSTITUTE FOR SECURITY AND TECHNOLOGY

STATEMENT OF KEMBA WALDEN

Ms. WALDEN. Chair DeGette, Ranking Member Griffith, and members of the subcommittee, thank you for the opportunity to testify today. My name is Kemba Walden, and I lead our ransomware analysis and disruption program within Microsoft's Digital Crimes Unit. Our unit is an international program of technical, legal, and business experts that has been fighting cyber crime to protect victims since 2008.

It is estimated that last year over 2,400 organizations were victims of ransomware attacks, with a financial impact of nearly half a billion dollars. I fear that we are only seeing the tip of the iceberg, as likely many attacks and corresponding losses go unreported. This recent proliferation of ransomware attacks impacts our national security, our economic security, our public safety, and our health.

In my oral comments today I will focus on what ransomware is, how the ransomware process works. I also wanted to share some of the key trends Microsoft is observing.

So what is ransomware? Well, it is malicious software that, once deployed in a victim's network, locks that network and the information in it, making it inaccessible to the victim unless the victim pays a ransom. You may have heard of different strains of ransomware, such as REvil and DarkSide, Conti, Ryuk, and so on. These are different types of ransomware, malicious software that lock a victim's network. Ransomware is installed after a series of criminal actions, so no single criminal gang is associated with any particular type of ransomware. It is simply the tool of choice for profit.

Today's ransomware attacks are different than the ones we experienced only a few years ago, where criminals deployed ransomware, often on a single computer in a predictable manner, and then demanded ransom in exchange for a decryption key to unlock that computer. Today's criminal has figured out how to use human intelligence and research to not only lock entire networks for a higher profit but to commit double or, in some cases, triple

extortion. We at Microsoft call this human-operated ransomware, otherwise known as big-game ransomware.

Ransomware is a profitable business, with few barriers to entry. It takes no specialized skill to profit from this crime. Here's what we are seeing in recent cyber criminal attacks. They customize their attacks and can be patient. Human-operated ransomware has evolved over the past few years, such that cyber criminals select specific networks to attack and then hunt for entry vectors. Criminal gangs are performing massive, wide-ranging sweeps of the internet, searching for vulnerable entry points, such as through unpatched software or successful phishing. Then they wait for a time that is advantageous to their purpose.

Because cyber criminals want to move laterally from one computer to the entire network, they focus on gaining access to highly privileged account credentials. They have developed a modular business model that we refer to as ransomware as a service. A manager or ransomware developer will recruit affiliates who have collected access, or collected credentials, or otherwise specialize in some other crime, offering a cut of the profits of an attack.

Make no mistake, these are fully fledged criminal enterprises. They find opportunities to double- or even triple-extort victims. So, before locking down a victim's system, they will find high-value information and steal it. Not only will they demand payment to unlock a victim's network, they will demand payment in exchange for not leaking the victim's data. In some cases, they will extort a victim a third time in exchange for not committing even more crimes, such as a DDos attack. They demand victims pay in cryptocurrency, thus taking advantage of the anonymous nature of this payment system.

While the movement of money is transparent, the crypto economy values privacy of the persons and the circumstances behind each transaction. So when cryptocurrency is used, criminals can easily verify when a victim has paid the ransom but hide behind the opaqueness of a crypto wallet. Importantly, this blockchain technology does not cause cyber criminals to commit this crime. Rather, elements of the crypto ecosystem make payments a bit easier, facilitating the crime.

In fact, while working with the Ransomware Task Force, I learned that compliance stakeholders within the crypto economy are just as eager as anyone to eliminate the nefarious use of their platforms.

So what do we do about it? Well, there is something for everyone to do. The Ransomware Task Force Report does a great job laying this out, so I won't go into detail here. However, I want to underscore the importance of partnership and actionable information sharing.

Criminals are smart, they are creative, they are well financed, and they are not limited by borders. The security community must match this. At Microsoft, our impact is greatest when we work collaboratively with government and others in the private sector.

In conclusion, government has law enforcement and intelligence resources that private sector cannot match. The private sector has access to data and technological resources that governments cannot match. We must work together to find innovative solutions.

Thank you, and I look forward to your questions.
[The prepared statement of Ms. Walden follows:]

Written Testimony of Kemba Walden
Assistant General Counsel, Microsoft Corporation Digital Crimes Unit

United States House Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
Hearing on "Stopping Digital Thieves: The Growing Threat of Ransomware"

July 20, 2021

Chair DeGette, Ranking Member Griffith and Members of the Subcommittee, my name is Kemba Walden, and I am an Assistant General Counsel in Microsoft's Digital Crimes Unit ("DCU"), where I lead our Ransomware Analysis and Disruption Program. I am also the co-chair of the Disruption working group of the Institute for Security and Technology (IST) Ransomware Task Force, which brings together experts across industries to combat the threat of ransomware.[1] Prior to Microsoft, I spent a decade in government service at the U.S. Department of Homeland Security. At DHS, I held several attorney roles, specifically as the lead attorney for the DHS representative to the Committee on Foreign Investment in the United States and then as a cybersecurity attorney for the Cybersecurity and Infrastructure Security Agency, and its predecessor. I want to thank you for the opportunity to discuss ransomware attacks and illustrate why increased and meaningful information-sharing and public private partnerships are critical to combatting this latest virulent example of costly cybercrime.

I'm also pleased to share information about how Microsoft is combatting ransomware. We believe the best strategy to decrease ransomware attacks is through targeted disruption campaigns along with increased cyber security hygiene. I will close by highlighting several key opportunities for more effective disruption of this cybercrime, opportunities to raise the collective security of public sector and private sector organizations, and the importance of partnerships.

Ransomware attacks pose an increased danger to all Americans as critical infrastructure owners and operators, small and medium businesses, and state and local governments are targeted by sophisticated criminal enterprises and nation-state proxies, operated by distinct criminal organizations. A sustainable and successful effort against this threat will thus require a whole-of –government strategy executed in close partnership with the private sector.

I. Microsoft's Approach to Cybercrime

Microsoft plays offense against online threats. Working through robust partnerships, we strive to take down criminal infrastructure and pursue both financially motivated and nation state supported cybercriminals. This work helps us to protect our customers and to improve the safety of the global internet community so that all users – enterprises, consumers, and governments – can trust the technology and online services on which we rely for commerce and communication. The Microsoft Digital Crimes Unit (DCU) is an international team of technical, legal, and business experts that has been fighting cybercrime to protect victims since 2008. We use our expertise and unique view into online criminal networks to act. We share insights internally that translate to security product features, we uncover

[1] The Task Force recently published a framework of actionable solutions aimed to mitigate ransomware as a malicious cyber activity and criminal enterprise: Institute for Security and Technology (IST) » RTF Report: Combatting Ransomware

evidence so that we can make criminal referrals to appropriate law enforcement throughout the world, and we take legal action to disrupt malicious activity.

As part of the DCU, Microsoft's new Ransomware Analysis and Disruption Program, which we launched in 2020, strives to make ransomware less profitable and more difficult to deploy by disrupting infrastructure and payment systems that enable ransomware attacks and by preventing criminals from using Microsoft products and services to attack our customers. The program is based on Microsoft's decade-long experience and history of success driving a sustained fight against other types of cybercrime.

In addition to partnering with law enforcement to disrupt cybercriminals involved in ransomware attacks, such as the recent disruption of the payment system of the cybercriminals that attacked Colonial Pipeline, Microsoft also uses our expertise to inform cybercrime legislation and global cooperation that advances the fight against cybercrime. We provided substantial support to IST and participated in all four working groups of the Ransomware Task Force. I personally co-chaired the Task Force's Disruption working group. My colleagues and I are also active participants in the World Economic Forum's Partnership Against Cybercrime, focused on global policy efforts to combat ransomware.

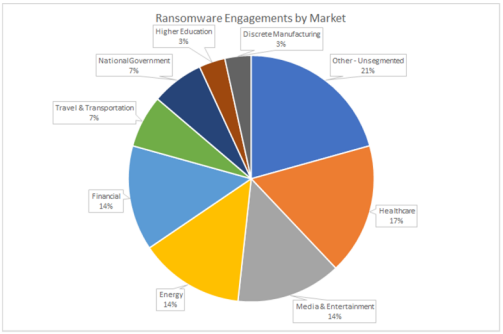
Through Microsoft's observations of ransomware deployment and attacks, our active collaboration with the U.S. Government to date, and Microsoft's thought leadership in the global discussion on policy and operational opportunities to counter ransomware, I will next address opportunities for more effective disruption of this cybercrime, opportunities to raise the collective security of public sector and private sector organizations, and the importance of partnerships.

II. Defining Ransomware

A. What is a Ransomware Attack?

Ransomware is a specific kind of malicious software or "malware" used by cybercriminals to render data or systems inaccessible for the purposes of extortion—i.e., ransom. In a standard ransomware attack the cybercriminal achieves unauthorized access to a victim's network, installs the ransomware, usually in locations with sensitive data or business critical systems, and then executes the program, locking files on that network, making them inaccessible to the victim until a ransom is paid. Usually, the ransom demand is for payment in the form of cryptocurrency – such as Bitcoin. Increasingly, attackers also steal sensitive data before deploying the actual ransomware in what is known as a double extortion ransomware attack. The theft of data compels the victim to engage in negotiations and raises the potential reputational, financial, and legal costs of not paying the ransom as the attackers will not only leave the victim's data locked, but also leak sensitive information that could include confidential business data or personally identifiable information.

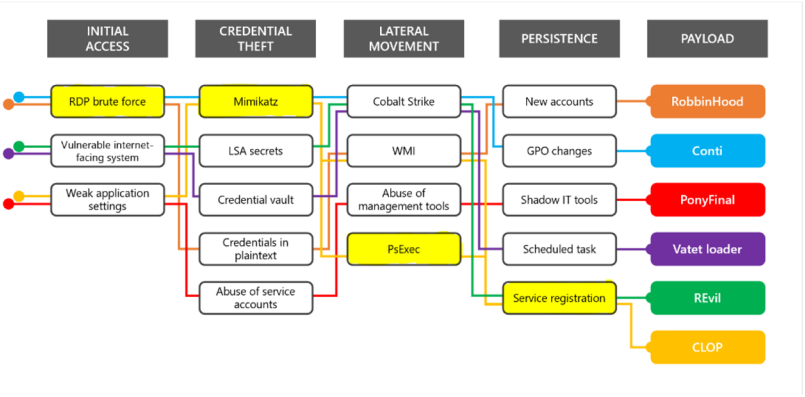
Recent, high-profile incidents such as those involving the Colonial Pipeline, JBS Foods, and Kaseya ransomware attacks drew considerable public attention and illustrate the extent of the threat and the significant, multimillion dollar consequences of ransomware. However, based on Microsoft's data, ransomware is not limited to high-profile incidents. It is ubiquitous and pervasive, impacting wide swathes of our economy, from the biggest to the smallest players. Our data shows that the energy sector represents one of the most targeted sectors, along with the financial, healthcare, and entertainment sectors. And despite continued promises by some cybercriminals not to attack hospitals or healthcare companies during the global pandemic, Microsoft has observed that healthcare remains the number one target of ransomware.



Ransomware engagements by industry

B. How does a ransomware attack work?

The image below depicts the basic steps that typically take place before a cybercriminal installs the malicious ransomware on a victim's network. First, cybercriminals will gain access to the victim's network through phishing, a stolen password, or through an unpatched software vulnerability. Then, the cybercriminals will seek to move laterally within the network to obtain higher level privileges, such as those held by the victim's IT Administrator, to access the entire network. Cybercriminals will then conduct reconnaissance within the victim's network, looking for critical systems and sensitive data, in some cases stealing this data, to facilitate an effective ransom demand. Finally, the cybercriminals will leverage this information to install the ransomware on the network that will lock the victim's files until the ransom is paid.



C. How do cybercriminals ransom targets?

Ransomware has effectively evolved into a highly lucrative business model, with an accompanying advanced intelligence collection aspect. Criminal actors collect and perform research and analyze their intelligence to identify an optimal dollar amount for their ransom demand. Once criminal actors break into a network, they may access and study their target's financial documents and insurance policies to better inform their eventual ransom demand and negotiating position. They may even research the penalties associated with that organization's local breach laws. The actors will then extort money from their victims, not only in exchange for unlocking their systems, but in some cases to prevent public disclosure of the victim's stolen data. Leveraging the significant intelligence they can gather on victim companies, the criminal actor will then launch their attack, identifying what they regard as an "appropriate" ransom amount.

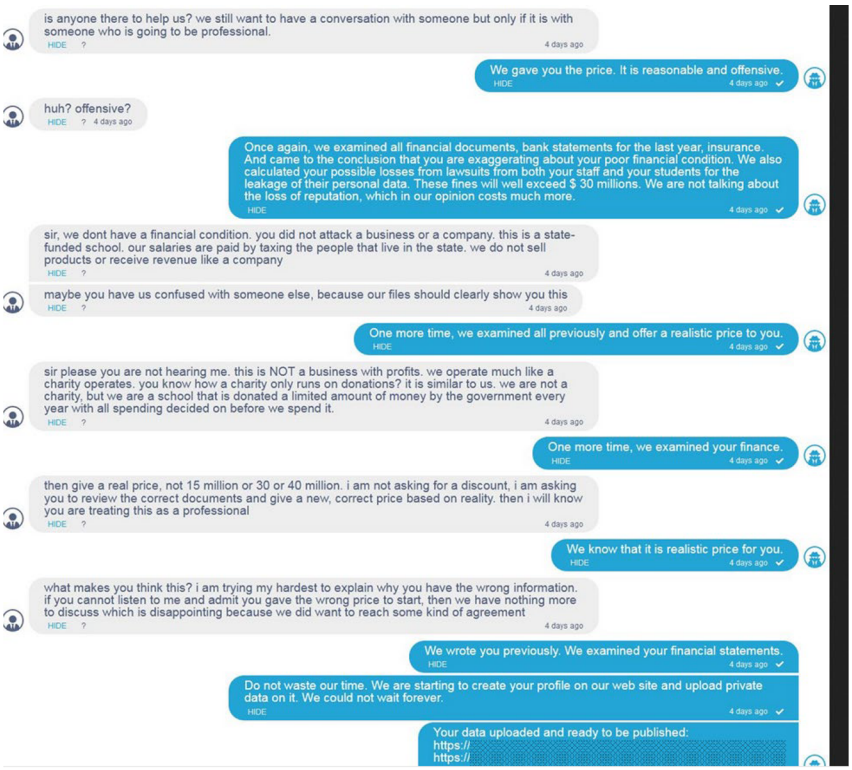
Once the criminal actor installs the ransomware and uses it to lock the victim's system, the victim will have access only to a ransom note. The ransom note provides instructions to the victim on how to communicate with the criminal actor. In the example below, the criminal used the ransomware strain known as Ryuk – one of many popular ransomware software packages in wide-spread use today. The criminal directs the victim to access the deep web using the tor browser, a special means for accessing the deep web. At this point, the victim can open communications with the criminal to negotiate the ransom or pay it.

```
contact balance of shadow universe Ryuk
INSTRUCTION:
Download tor browser.
Open link through tor browser: " http://rk2zzyh63g5avvii4irkhymha3irblchdfj7prk6zwy23f6kahidkpqd.onion"
Fill the form, your password: "oPY9epzf"
We will contact you shortly.
Always send files for test decryption.
```

The negotiation process and back-and-forth communications are often surreal and disturbing in the nonchalance with which some criminal actors offer to "help" companies recover from the very attack they have orchestrated. The example below depicts a negotiation chat with a public school district in which the criminals attempt to extort cash in exchange for a key to unlock the ransomware deployed on its network. The interaction demonstrates the research performed by the criminal in advance of the negotiation, as the criminal actor explained that they had

> "examined all financial documents, bank statements for the last year, insurance. And came to the conclusion that you are exaggerating about poor financial condition. We also calculated your possible losses from lawsuits from both your staff and your students for the leakage of their personal data. These fines will exceed $30 million. We are not talking about the loss of reputation, which in our opinion costs more."[2]

[2] See also Parents were at the end of their chain — then ransomware hit (nbcnews.com)



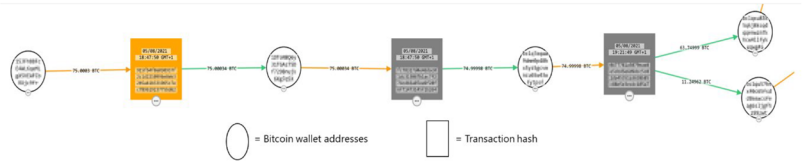
D. What barriers to entry exist to executing a ransomware attack?

Very few. A cybercriminal does not need specialized computer coding skills to profit from ransomware. The only cybercriminal in the entire ransomware lifecycle who requires specialized code development skills is the originator who develops the malicious software in the first place. There are hundreds, if not thousands of different ransomware variants, such as Ryuk, Darkside, REvil, Maze, and Conti. Attacks are often misleadingly named after the malicious software that was installed on a victim's network though the cybercriminals involved in the attack may not have any link to creator of that particular ransomware. A single cybercriminal may use any number of ransomware variants in conjunction with other tools to attack victim networks.

Increasingly, cybercriminals who use ransomware have moved to a "Ransomware as a Service" business model that is driven by human intelligence and research. This has further decreased the barriers to entry for any cybercriminal. Ransomware as a Service is a "modular" business model where individuals with limited technical skills can leverage the malware developed by others to conduct their own attacks.

Developers or managers will use hacker forums to recruit affiliate hackers. For example, as Bleeping Computer reported last fall, REvil developers used hacker forums to actively recruit affiliate hackers. To facilitate the business aspect of the relationship, developers create and run ransomware and payment sites with affiliates who hack businesses and lock their devices. Developers typically get 20-30% of any ensuing ransom, with affiliates receiving 70-80%. This is effectively a crime syndicate where each member is paid for a particular expertise.

The below example, following the flow of cryptocurrency, shows how a criminal enterprise split its bitcoin (BTC) "earnings" such that approximately 25% of the earnings flowed to the developer/manager and 75% of the "earnings" flowed to the attacker.



Transaction hashes and wallet addresses intentionally blurred for publication

III. Opportunities for Disruption

Disruption of criminal activity does not eliminate the problem, but it raises the cost of committing the crime. Arrests and prosecution in cybercrime can be difficult, disrupting the infrastructure that is used by cybercriminals in ransomware attacks is therefore a key part of deterrence. In the case of ransomware, there are opportunities for both the public and private sector to focus on making the crime more difficult to commit (infrastructure disruption) and opportunities to focus on making the crime less profitable (payment disruption). The hope is that by shifting this balance, criminal actors will abandon this crime.

A. Disrupt the Infrastructure by targeting the criminal actor's ability to communicate with the victim or publicly disclose stolen data.

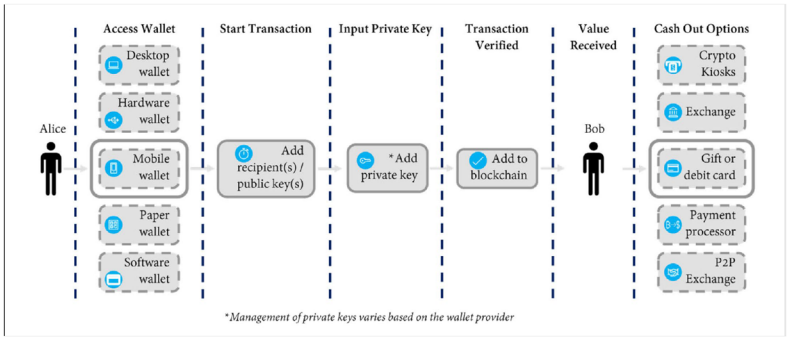
There is not a "one size fits all" infrastructure disruption that will eliminate ransomware; rather, disruption will make it more difficult for the criminal actor to accomplish their goals, thereby raising the cost of committing this crime. Generally, infrastructure disruption focuses on removing the infrastructure such as websites, servers or email accounts that enable the criminal actor to negotiate the ransom with the victim and for publicly disclosing the victim's sensitive data. Ransomware attacks often use the same infrastructure for multiple campaigns. Cybercriminals decide how to conduct their attack based on what security tools were present, whether the network had good cyber hygiene, and which data the cybercriminals wanted to exfiltrate from the network.

Although the new Ransomware as a Service business model relies on a variety of tools and ultimate choice of ransomware, all of them need to operate in a similar manner to effectively extract payment from victims. The infrastructure used is rather consistent. For example, every double extortion ransomware scheme needs a location to publicize the stolen data and an opportunity to establish communication with their victims to negotiate the terms of the ransom. This provides a disruption opportunity.

B. Disrupt the Payment Distribution System by targeting intermediaries that support the vulnerable elements of the system.

Disrupting the payment distribution system that supports this crime makes ransomware attacks less profitable. Improving our technical means and legal process for disrupting the infrastructure that supports payments earned through ransom will significantly impact the profitability (and thereby prevalence) of this crime. Because the payment distribution system and the intermediaries that support the money flow ranges across international borders, disrupting the payment distribution system will require a global strategy.

The infographic below demonstrates the flow of payment and opportunities for disruption: a victim (Alice) will obtain a wallet that is able to send cryptocurrency. There are several types of wallets – wallets that are held by a service provider on behalf of the owner (otherwise known as a "hot" wallet) or wallets that are in the sole custody of the owner and are not accessible by any other party (otherwise known as a "cold" wallet). Victims usually obtain "hot" wallets while criminals will often have both "hot" and "cold" wallets. There are a series of actions that are taken to send cryptocurrency in a pseudonymous manner ultimately resulting in its receipt by the criminal (Rob). Rob then has a variety of choices to convert his cryptocurrency payment into traditional fiat currency, like U.S. Dollars. Those options include going through a crypto kiosk (which is akin to an automated teller machine), using a crypto exchange, using a peer-to-peer exchange or using an over-the-counter trading desk. Other options include purchasing gift cards, gambling, or going through some other payment processor. It is these on-ramps (obtaining a "hot" wallet) and the off-ramps (exchanging digital currency into traditional currency) where the criminal actor is most vulnerable and the opportunity for disruption is greatest.



Infographic taken from the U.S. Department of Justice Report of the Attorney General's Cyber Digital Task Force

Regardless of where ransomware is deployed, typically the threat actors will demand payment via crypto currency. Though the underlying blockchain technology facilitates transparent cryptocurrency flows, the owners of wallets remain pseudonymous. To achieve this pseudonymity, first a threat actor must obtain a crypto wallet from a wallet services company and second, the threat actor will seek to cash out its crypto currency through some sort of platform. At its core, the criminal actor needs to append the blockchain with a transaction and ultimately find a way to cash out. Most stakeholders in this cryptocurrency system do not want their platforms used for nefarious purposes. Those that are compliant with U.S. laws are interested in partnering with the security community to make it more difficult for criminal actors to use

their platforms. However, some wallet service providers and crypto currency exchanges can exist in jurisdictions that are either unwilling or unable to effectively police these service providers. It's these intermediaries that facilitate the flow of ill-gotten earnings from ransomware. The private sector through civil litigation, and the government through criminal seizure, regulatory enforcement, and international collaboration can take coordinated action to disrupt these weak points in the payment process. We applaud the U.S. Department of Justice's formation of its internal Ransomware Task Force and recent operation to seize a wallet and crypto currency from the criminal gang that attacked Colonial Pipeline.

IV. Raising Awareness for Potential Victims.

Although disruption is important, preventing criminal actors from getting into networks in the first place and making organizations resilient to attacks are equally important. Potential victims, governments, organizations, and businesses of all sizes are at varying levels of preparedness maturity. Ensuring that all potential victims increase their security and resilience is key.

Cybercriminals who install ransomware use tried and true methods for access. Often, applying basic cybersecurity hygiene can prevent a cybercriminal's ability to ransom a system. Consider, for example, the recent ransomware attack against EDGAR, the Securities and Exchange Commission's Electronic Data Gathering, Analysis, and Retrieval system. Cybercriminals were able to access the network through an IT Administrator's password that was compromised in an earlier breach.[3]

Microsoft recommends that the government produce clear useable guidance to address common points of confusion around ransomware attacks, clarifying what organizations should do first, next, and after that (1-2-3 style guidance). Although NIST has done an excellent job of addressing many aspects of these attacks, organizations still struggle with where to start (especially smaller organizations with limited staff and experience). Any government guidance should clearly state top security priorities, and why they are important. For example, a simple three step approach could be effective: (1) Make it harder to get in, (2) Limit the scope of damage and (3) Prepare for the worst.

Making it harder to get in. There are several basic cybersecurity hygiene steps that can be taken to make it much harder for attackers to gain access to the victim's network. The most important of these steps is the use of multi-factor authentication. A study done at Microsoft estimates that more than 99% of all cyberattacks would have been prevented if multi-factor authentication were deployed. Multi-factor authentication is important to raising friction for entry but will take time to complete as part of a larger security journey. Other steps can be taken to identify and close off vulnerable entry points. **Limiting the scope of damage** forces the attackers to work harder to gain access to multiple business critical systems by establishing least privileged access and adopting Zero Trust Principles. These steps make it harder for an attacker who gets into a network to travel across the network in order to find valuable data to lock up. There are many resources that describe how to do this effectively, and simple free tools, like those from the Cyber Risk Institute, can help even small and medium size businesses do this work. Finally, encouraging potential victims to **prepare for the worst** is designed to minimize the monetary incentives for ransomware attackers by making it harder to access and disrupt systems and easier for victims to recover from an attack without paying the ransom.

The recently launched Stop Ransomware website hosted by DHS/CISA is a fantastic resource for explaining ransomware, providing a step by step guide to responding to a ransomware attack, and providing best practices for preparedness.

---

[3] Hiltzik: The threat of ransomware - Los Angeles Times (latimes.com)

V. The importance of Public – Private Partnerships

Just as committing ransomware attacks requires collective effort, countering ransomware attacks needs the same focus and global coordination. As these attacks have evolved to more sophisticated enterprise-like operations involving multiple players, countering these efforts requires a multi-stakeholder approach. Each of us has an important role to play, with the foundation of our efforts being reliable information and operational collaboration. The private sector and the U.S. government have engaged in and experimented with technical and legal models, globally, to disrupt and dismantle cybercrime infrastructure. Efforts to date illustrate that a collaborative multi-stakeholder approach – sharing actionable information and leveraging the combined capabilities of the private sector and the government – yields the best opportunity to disrupt cybercrime quickly and at scale.

The recent take down of Emotet, a botnet known to support the distribution of the Ryuk ransomware, involved law enforcement around the world as well as private sector security researchers. Individual computers infected with malicious software are called bots. These bots are controlled by the cybercriminal to create a botnet –that can be used to engage in further criminal activity. These botnets can range from a few hundred to tens of millions of compromised systems. In taking down the Emotet botnet, law enforcement seized assets and arrested the cyber criminals in Ukraine while researchers working with law enforcement took down Emotet's command and control infrastructure used to operate the botnet and cleaned the individual computers in the botnet. The effort involved a worldwide coalition of law enforcement agencies across the U.S., Canada, the UK, the Netherlands, Germany, France, Lithuania, and Ukraine to disrupt and take over Emotet's infrastructure which was located in more than 90 countries [4]— while simultaneously arresting at least two of the cybercriminals.

As the U.S. government has recognized, for example, with the creation of the new interagency ransomware taskforce and the FBI's new cyber strategy, unilateral action, whether public or private, is not a sustainable solution against nation-state sponsored or financially motivated sophisticated organized cybercrime. To combat ransomware we recommend:

- Clearly understanding the problem: Cybercriminals currently take advantage of the internet and the limitations of sovereignty to carry out crime against victims located anywhere in the world. While the internet and technological tools enable cybercriminals to operate with almost absolute anonymity.
- Focusing on what can be done to address the problem: Disruption of malicious infrastructure, even when arrest is not possible, through global cooperation between the private sector and governments.
- Increasing focus on critical areas: To increase the scope and scale of disruptions, and to have success similar to Emotet, public-private information sharing, strong global Mutual Legal Assistance, technical operational capabilities and training, threat tracking and prioritization, and victim remediation needs to be improved.

A collaborative, multi-stakeholder approach to countering cybercrime, including ransomware must be nimble and function at scale. Though the bulk of government efforts have been driven by traditional law enforcement objectives and tactics (e.g., indictment and arrest), we now see a shift in the U.S. government and foreign governments to actions to disrupt cybercriminal infrastructure. Traditional enforcement mechanisms are a critical piece of global cybersecurity and U.S. national security; however, we must continue to focus on the more immediate "takedown" or disruption of infrastructure, which more

[4] Cops Disrupt Emotet, the Internet's 'Most Dangerous Malware' | WIRED

strategically aligns with the needs and priorities of many victims and is a significant public interest. This focus on disruption should be a primary strategy to combat ransomware.

VI. Conclusion

I am pleased to see that the U.S. Government, the security community, state and local governments, and the international community are coming together for a coordinated response to ransomware. There is much work that needs to be done but I am optimistic that we collectively have the thought leadership to accomplish our goals. The IST Ransomware Task Force published a set of thoughtful and measured policy and operational recommendations, including several that may require legislative action. I encourage all stakeholders involved to act where they can to reduce the incidence of ransomware attacks.

Ms. DEGETTE. Thank you so much.

Now I am now pleased to recognize you, Mr. Lee, for 5 minutes.

STATEMENT OF ROBERT M. LEE

Mr. LEE. Thank you. Chairwoman DeGette, Ranking Member Griffith, and members of the committee, thank you for providing me the opportunity to testify before you today.

I started my career as an Air Force officer and spent most of that time tasked at the National Security Agency, where I built and led a first-of-its-kind mission to hunt for and analyze threats targeting industrial control systems. At that time, cyber threats towards industrial systems were seen as a possibility, but not as a reality.

The problem, though, is everyone was looking in the wrong location. Analysts around the community were hunting for threats in enterprise IT, or information technology, networks, such as those that people depend on for personal computer usage and email. What we were not doing is looking at industrial and operations networks themselves, such as those in power plants, pipelines, water utilities, and manufacturing sites. Broadly, I will refer to this as operations technology, or OT.

The easiest way to explain OT is to consider that everything we have in IT, plus physics. When adversaries target IT networks, they often steal data. And when they disrupt them with malicious software such as ransomware, it impacts workers' ability to do their job. When adversaries target OT networks, they can, intentionally or not, create unsafe conditions that cause damage to the world around us, up to and including the loss of human life.

As I mentioned, though, we did not see the various OT threats that existed, because the broader community was looking for OT threats in IT networks. We lacked the visibility in OT to determine what was happening. In essence, we had the equivalence of Schrodinger's OT. We did not look inside the box to determine if the cat was alive or not. In my time at the NSA we started looking inside that box. To our surprise, we found a wide variety of state actors targeting these systems.

Today, at Dragos, we track 15 state actors targeting OT around the world, including many operations in the United States. Specific to the topic of ransomware, we have responded to numerous incidents and ransomware incidents in OT. Each company has done the right thing. They have sought out help. However, these incidents happen far more often than people realize. Across all the cases, though, we continue to see that a lack of visibility in the OT networks leads companies to believing that they are in a better place than they actually are.

Our hearing today, appropriately, is on ransomware. But I want to underscore that it is just one risk facing our infrastructure and, if anything, highlights that, if criminals can be successful in breaching and disrupting our networks, state actors will find much more success.

However, the threats are worse than we realize, but not as bad as we want to imagine. And, ultimately, defense is doable. Today I want to highlight a few key points.

Number one, to defend against ransomware, we must first find a way to harmonize the roles and responsibilities of the private sector with government.

Number two, there must be a simplified, unburdened process and single point of contact with the government. CISA, as an example, could be the front door of government, who could then coordinate the interagency and communicate clearly to the private sector. There are recommendations in the National Infrastructure Advisory Council and Cyberspace Solarium Commission to improve analyst collaboration, as well.

Ransomware in OT, my third point, is exposing the underinvestment in cybersecurity in many organizations. My prediction is, as we look to counter the ransomware threat, we will start to gain more insights, and those insights will lead us to find more state actors and other threats. We must be prepared for what we find and think about the ransomware strategy as an overall portion of our cybersecurity strategy.

Number four, critical infrastructure companies stand ready to do the right thing and partner with government fully. However, differing regulation regimes and requirements can distract from the focus. Whatever regulations and standards manifest, they should be thought of together so that companies do not have overly burdensome requirements on them as we all try to achieve the same goal.

And lastly, government should communicate the why and the what to the private sector, but leave the how to the experts in those entities. We have seen this work very well.

This administration and the Department of Energy launched a 100-day action plan earlier this year focused on OT. They did that in the electric sector. The goal was increasing real-time information sharing, visibility, detection, and response capabilities in OT networks. The government laid out the requirements and why they wanted companies to do this, but they did not dictate the solution or how they had to achieve it. This was done in collaboration with the electric sector leaders, as well.

The electric sector coordinated, evaluated what was on the market, and chose Neighborhood Keeper, a technology made by Dragos in collaboration with the Department of Energy. They then deployed it quickly, voluntarily, and at their own costs. As a result, we went from less than 5 percent of the electric system monitored in the United States to more than 70 percent of the electric system monitored in OT networks in under 100 days. This is the exact type of visibility and success useful in preventing ransomware and those issues.

Government setting requirements and amplifying them is important. Letting the private sector figure out innovative ways in how to achieve those requirements is paramount. I thank the committee for providing me the opportunity to testify today and welcome any additional questions or information.

[The prepared statement of Mr. Lee follows:]

COUNTERING RANSOMWARE IN CRITICAL INFRASTRUCTURE

PREPARING FOR THIS CYBER THREAT AND THOSE THAT WE WILL UNCOVER

HEARING
BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS OF THE COMMITTEE ON ENERGY AND COMMERCE OF THE HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

---

20 JULY 2021, RAYBURN HOUSE OFFICE BUILDING

---

https://energycommerce.house.gov/committee-activity/hearings/hearing-on-stopping-digital-thieves-the-growing-threat-of-ransomware

Robert M. Lee[1]

I. Background

Chairman Pallone, Jr., Chairwoman DeGette, Ranking Members Rodgers and Griffith, and members of the committee, thank you for providing me the opportunity to testify before you today. It is an honor to be here before you to talk about cyber attacks in our critical infrastructure. My name is Robert M. Lee, and I am the CEO and co-founder of Dragos, a cybersecurity technology and services firm focused explicitly on the operations and industrial systems that our critical infrastructure depend on. I also currently serve on the Department of Energy's Electricity Advisory Committee as the Vice Chair of the Grid Resilience for National Security subcommittee and on the World Economic Forum's electricity and oil and gas cybersecurity subcommittees.

I started my career as an Air Force officer and spent most of that time tasked to the National Security Agency where I built and led a first-of-its-kind mission to hunt for, identify, and analyze state and non-state actors targeting industrial control systems. At that time, cyber threats towards industrial systems were seen as a possibility but not as a reality. The problem though is everyone was looking in the wrong location. Analysts around the community were hunting for threats in Enterprise information technology (IT) networks such as those that people depend on for email and personal computer usage. What we

---

[1] CEO and Co-Founder of Dragos, Inc.
@RobertMLee

were not doing is looking in the industrial and operations networks themselves. Broadly I will refer to this as operations technology (OT).

The easiest way to explain OT is to consider everything we have in IT networks plus physics. We have purpose-built control systems, different communications, and application programs you will not find in IT networks. But even if all the systems and networks converged the difference would fundamentally be the mission and its interaction with the physical world around us. When adversaries target IT networks they often steal data such as personnel records and emails and when they disrupt them with malicious software such as ransomware it impacts workers' ability to perform their job. When adversaries target OT networks they can steal data such as intellectual property as well, but they can, intentionally or not, also create unsafe conditions that cause damage in the world around us up to and including the loss of human life. The mission in OT is different. The threats to OT are different. Thus, the security and approach we take to those environments must also be different.

For decades, critical infrastructure companies have spent significant number of resources protecting their enterprise IT environments as they were asked to do. The belief was that OT networks were disconnected or highly segmented from other systems and that by protecting IT you would protect OT. As I mentioned though, we did not see the various OT threats that existed because the broader community was looking for OT threats, in IT networks. We lacked the visibility in OT to determine what was going on. In essence we had the equivalence of Schrödinger's OT believing that as long as we did not look in the box the cat was alive.

In my time at the NSA, we started looking in the box. To our surprise, we found a wide variety of state actors, beyond even the normal ones we refer to, targeting and performing reconnaissance against these systems. Leading critical infrastructure companies that were communicated to by various government agencies sharing our findings began to increase their defenses as good stewards of public interest and national security. Unfortunately, many of the efforts were essentially copy/pasted IT security approaches and standards into OT. Many of these approaches predictably failed or under delivered. That is what led me to leave the US government and found Dragos so that we could take an OT specific approach to our cybersecurity software and services.

Since the founding of Dragos the threat landscape has become far more illuminated though we are still in the early days of fully scoping the problem. In 2015 the first ever cyber attack to cause an electric power outage took place in Ukraine and I was privileged to lead up a portion of that investigation with other wonderful individuals to include Michael Assante, Tim Conway, and Tim Roxey. In 2016 the second ever cyber attack to cause a power outage took place again in Ukraine and my firm was involved in analyzing the malicious software leveraged. In 2017 my team was again involved in analyzing malicious software at the center of a major attack, this time it was against a Saudi Arabian petrochemical company, and it was the first time ever that a cyber attack explicitly targeted human life. The adversary made a mistake, otherwise dozens of people would likely have lost their lives. Over the next few years my team tracked those same threats and others as they carried out operations in other countries across the Middle East, Australia, New Zealand, Europe, and numerous operations in the United States. Today we track over 15 different state actors that explicitly target industrial and operations systems across numerous critical infrastructure industries. We have also begun to seen OT specific ransomware.

In the last year things have continued to accelerate. The SolarWinds supply chain compromise that gained a significant amount of attention in IT networks was also widely leveraged in OT. While this fact

remained unreported, Dragos responded to numerous incident response cases in OT where companies significantly lacked the visibility and data collection to determine if they were compromised or not. While the espionage that took place in SolarWinds made people uncomfortable, what should have scared people is the fact that a hostile foreign adversary had direct access, whether or not they knew it, to sensitive critical infrastructure sites across the US and that broadly we were unprepared to identify if the adversary was even still present. We are fortunate it was an espionage operation and not a destructive one.

Again, in a concerning development, an adversary targeted a water facility in Oldsmar, Florida. While the technical details of the case are not all that interesting or advanced the underrepresented point is that a foreign actor attempted to poison American citizens' water. Targeting human life should always be off limits and unacceptable. The fact that adversaries are already trying continues to cross any of our imagined red lines as they become bolder and more capable. Unfortunately, my assessment is we will have a loss of human life scenario as a direct result of cyber operations against OT in the future. I do not know when, and what we must work together on is ensuring that when it occurs it is as limited as possible understanding that no loss of life scenario is acceptable.

Specific to the topic of ransomware, my firm has responded to numerous ransomware incidents in OT that have gone unreported. Each company has done the right thing to get help and remediate the issues at their own cost. However, these incidents happen far more often than people realize. These cases tend not to make the news because the disruption does not rise to a level that is noticeable especially when companies have resiliency in their industrial operations and what they produce. Across all the cases though we continue to see that a lack of visibility in the OT networks leads companies to believing they are in a better place than they are and when the incident occurs, they do not have the appropriate plans or investments made to prevent breaches, detect threats, and when necessary, respond and recover efficiently. These companies are often resource strained. There is not a need for a moonshot project, no buzzwords like AI or blockchain are necessary, instead these companies need to understand the problem better and they require resources to adopt commercial technologies and services already available while increasing and resourcing their security staff appropriately.

Our hearing today appropriately is on ransomware as it is far reaching, accelerating, and impactful to daily life in this country especially for its disruptive qualities in critical infrastructure. But I want to underscore that it is just one risk facing our infrastructure and if anything highlights that if criminals can be successful in breaching and disrupting our OT environments, state actors will find much more success.

However, there are successes we can and should point to and emulate. The threats are worse than we realize, but not as bad as we want to imagine. And ultimately defense is doable.

To do this today I want to highlight five key points all inside of a theme of harmonizing roles and responsibilities between private sector and government. I think this can help us address ransomware in OT and set us up for success and derivative effects against state actors.

II. The Five Key Points

1. To defend against ransomware, we must first find a way to harmonize the roles and responsibilities of the private sector with government and the government's need to be aware

of critical breaches. There are significant and important roles and responsibilities that government has but there are also significant expertise and capability that the private sector can bring. Sometimes this can be confusing in messaging to the private sector on what the government can and should be doing in any given case. As an example, when a breach happens that is made public, companies often get asked why they did not bring in government agencies for incident response. But if those companies have already engaged reputable private sector incident response teams that should not matter. The government should be made aware of any incidents that can impact national security or critical infrastructure's ability to deliver their goods and services but do not need to be an on the ground team responding to incidents. Candidly, those teams are amazing people and ready to help but have less expertise and experience on the topic than the top end incident response firms that specialize in those cases. It is good for the private sector to be able to leverage government resources but the most important mission for government cybersecurity teams is protecting government networks and systems and then sharing what they have learned while amplifying the risks they see to educate others.

2. There must be a simplified unburdened process and single point of contact with the government. Whichever government agency is on lead does not matter as much to the private sector though it seems the right answer is CISA. The important thing is that there is only one front door to the government who can then coordinate the interagency and communicate clearly to the private sector entity. Right now a typical power company CEO as an example can expect to hear from the DOE, DHS, National Guard, FBI, DOD base commanders in their service territory, and others on when and why they should contact that government agency, often with conflicting guidance, and their focus areas which amount to a differing set of goals across government. A front door to government communicating the government's strategy, requirements, and assistance would greatly reduce the confusion that can occur.

3. Ransomware in OT is exposing the underinvestment in cybersecurity in many organizations. My prediction is as we counter this threat together the community will gain much more insight into the state intelligence and military units' activity in this space. We must be prepared for what we find and think about the ransomware strategy as part of the overall cybersecurity strategy. Ransomware cannot simply be the flavor of the day but instead a rallying effort of the community to increase cybersecurity overall.

4. Critical infrastructure companies stand ready to do the right thing and partner with government fully. However, differing regulation regimes and requirements can distract from the focus. Whatever regulations manifest they should be thought of together so that companies do not have overly burdensome requirements on them as we all try to achieve the same goal of security. As an example, some power companies have natural gas operations as it is a significant fuel source in our electric system. A power company may already comply with NERC CIP cybersecurity regulations. Many of those companies have extended their security practices proactively into non-NERC CIP covered assets including distribution substations and gas pipelines just trying to do the right thing. Yet new requirements such as TSA's pipeline regulations do not consider this and at times are in conflict with already existing regulations and

cybersecurity standards or not appropriately tailored to OT. This puts those power companies and others in a position where they have rip and replace their already existing security standards that have worked for them with new guidance they are unfamiliar with in practice. This can have a net negative security impact on an already strained security workforce at these companies. Policy actions around regulation should look to drive outcomes such as the reliability of critical services instead of being prescriptive and ignoring existing efforts.

5. Government should communicate the *why* and the *what* to private sector but leave the *how* to the individual entities. We have seen this work very well. This Administration and the Department of Energy launched a 100-day action plan earlier this year focused on OT cybersecurity in the electric sector. The goal was increasing real time information sharing, visibility, detection, and response capabilities in OT. The government laid out the requirements and why this was important. It was not a laundry of list of asks but instead a straightforward assessment of the problem and a few direct asks to the private sector. This was done in concert with the private sector leveraging the Electric Sector Coordinating Council which is a CEO led group across the electric system. The government asked for the effort to be done but did not dictate how it would be done. The electric sector coordinated, evaluated what was on the market, and chose Neighborhood Keeper, a technology made by Dragos in cooperation with the Department of Energy. They then deployed it quickly, voluntarily, and at their own cost. This was a monumental undertaking that has never been achievable before in OT and was a success because the private sector knew what mattered to the government and the requirements to hit but were left to innovate on how they achieved success in ways that worked for them. As a result, we went from less than 5% of visibility across the electric community to more than 70% of the electric system in the US today being monitored with information sharing across each participant in real time as a collective defense. That information is shared with the Electricity Information Sharing and Analysis Center (E-ISAC). Other industries have paid attention to the electric sector's leadership and the White House's efforts and there are now many in the water and gas sectors that are already adopting the same technology and approach to help national security. As an example, the Downstream Natural Gas ISAC (DNG-ISAC) has signed on to do the same work that the E-ISAC is doing across their community. All of this is done while protecting the data and identity of the participants. The system is entirely anonymous and all the data stays in the company's networks. This allowed the entities to be comfortable sharing insights with the government including ongoing threats, vulnerabilities, and compromises while protecting themselves and sensitive data. Government setting requirements and amplifying those requirements is important. Letting the private sector figure out how to achieve those requirements in ways that work for them and leverage their expertise running our infrastructure is paramount.

I sincerely thank the Committee for providing me the opportunity to testify today and welcome any questions or additional information.

Ms. DEGETTE. Thank you so much.

Dr. Dameff, I am now pleased to recognize you for 5 minutes.

STATEMENT OF CHRISTIAN DAMEFF, M.D.

Dr. DAMEFF. Madam Chair DeGette, Ranking Member Griffith, distinguished members of the subcommittee, thank you for this opportunity to speak today on the effects of ransomware on healthcare. My name is Dr. Christian Dameff, and I am a practicing emergency medicine physician. I am also an assistant professor of emergency medicine, biomedical informatics, and computer science at the University of California, San Diego. I also serve as the medical director of cybersecurity for U.C. San Diego Health, the first position of its kind in the United States.

Early in my adolescence, my fascination with computers and networks led me to the hacker community, who taught me to appreciate the complexity and fragility of modern computer systems. Today I use that knowledge to improve the cybersecurity of healthcare. My research focuses on the patient safety and care quality impacts of cyber attacks. At my core, I am an emergency medicine doctor. I am trained to care for any patient who comes through the door, whether they suffer trauma, heart attacks, strokes, or COVID. I am here to tell you that healthcare is not prepared to defend or respond against ransomware threats.

Our hospitals today are increasingly dependent on technology. Doctors admit patients into the hospital, order and review laboratory tests, prescribe medications, and prepare for surgeries, all while using computerized workflows. We have come to implicitly trust and rely on these systems. And when they fail, healthcare grinds to a near halt.

We know ransomware attacks affecting the healthcare sector are increasing in frequency, sophistication, and disruptive potential, in addition to the exposure of sensitive data, severe financial losses, and reputational damage. A cyber attack on a hospital has the potential to threaten life and limb.

When patients suffer from strokes, heart attacks, or severe infections, minutes matter. The best outcome for patients with these time-dependent crises depend on immediate, continuous availability of the same digital systems that ransomware can disrupt. When critical medical systems go offline, our opportunity to save lives diminishes. The risk of error or misdiagnosis increases. We are now learning that cyber attacks impact not just the infected hospitals but the surrounding healthcare ecosystem at large.

Two months ago, a ransomware attack disabled five large hospitals in the San Diego area for an entire month. Adjacent hospitals were quickly overwhelmed with unprecedented numbers of emergency room patients, many of whom had serious, time-dependent illness. Wait times skyrocketed. Hospital beds rapidly filled. Clinicians caring for very sick patients lacked vital medical records from the infected hospitals. I saw firsthand the spillover effects and understood that the vulnerability of one hospital is a vulnerability of many hospitals.

You have heard today from experts with technical and policy recommendations that, if enacted, would improve ransomware defenses across all sectors. However, I hope you now understand that

healthcare has unique challenges and necessitates additional actions.

First, the effects of ransomware attacks on patients' health should be scientifically studied. Most hospitals are not currently equipped to measure or report the impacts of these attacks. I recommend the development of standardized metrics of cyber attack severity on hospitals. Mandatory reporting of patient safety and care quality outcomes should occur for severe attacks. I recommend that Federal agencies such as the National Institutes of Health and the National Science Foundation prioritize funding for research on this topic.

Second, identifying cybersecurity vulnerabilities before they are exploited will protect patients. There is currently disparity between what I call the healthcare cybersecurity haves and have nots. Lesser-resourced, critical-access, and rural hospitals need help when it comes to increasing their preparedness. As we seek to protect vulnerable hospitals, we must also avoid overly punitive measures for those who are unfortunate enough to fall victim to highly complex or novel cyber attacks, understanding that stiff fines or penalties may worsen an already devastating operational impact. We are only as strong as our least-defended communities.

Third, I support software bill of materials as one mechanism to increase transparency around cybersecurity vulnerabilities. Software bill of materials enables manufacturers and healthcare delivery organizations to take more proactive steps to manage their cybersecurity risk.

Furthermore, I recommend ongoing support and legal protections for security researchers engaging in good-faith security research, otherwise known as coordinated vulnerability disclosure. We need help from ethical hackers if we are going to defend against the malicious ones.

Lastly, we must prepare hospitals for inevitable attack. The ability to rapidly deploy backup manual patient care systems is key to reducing patient harm. Such contingency planning takes resources and expertise.

In conclusion, I applaud this committee's leadership on ransomware response and remain optimistic about improving cyber resilience in healthcare. Our patients deserve excellent care. Ransomware and other cyber attacks targeting hospitals threaten our ability to deliver that care as it is needed, when minutes matter.

Thank you for this opportunity to testify today, and I welcome any questions you may have.

[The prepared statement of Dr. Dameff follows:]

Testimony of Dr. Christian Dameff MD

Before the Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

U.S. House of Representatives

"Stopping Digital Thieves: The
Growing Threat of Ransomware."

July 20th, 2021
Washington, DC

Introduction

Madam Chair DeGette, Ranking Member Griffith, distinguished members of the subcommittee, thank you for the opportunity to testify today on the effects of ransomware on healthcare. My name is Dr. Christian Dameff and I am a practicing Emergency Medicine Physician. I am also an assistant professor of Emergency Medicine, Biomedical Informatics, and Computer Science at the University of California San Diego. I also serve as the Medical Director of Cybersecurity for UC San Diego Health, the first position of its kind in the United States. Early in my adolescence, my fascination with computers and networks led me to the hacking community, who taught me to appreciate the complexity and fragility of modern computer systems. Today, I use that knowledge to improve the cybersecurity of healthcare. My research focuses on the patient safety and care quality effects of cyber attacks.

At my core, I am an Emergency Medicine doctor. I am trained to care for any patient who comes through the doors whether they suffer trauma, heart attack, stroke, or COVID. I am here today to tell you healthcare is not prepared to defend or respond to ransomware threats.

Technological Dependence

Our hospitals today are increasingly dependent on technology. Doctors admit patients into the hospital, order and review test results, prescribe medications and prepare for surgeries all while using computerized workflows. We have come to implicitly trust and rely on these systems, and when they fail healthcare grinds to a near halt.

Patient Safety

We know ransomware attacks affecting the healthcare sector are increasing in frequency, sophistication, and disruptive potential. In addition to the exposure of sensitive data, severe financial losses, and reputational damage, a cyber attack on a hospital has the potential to threaten life and limb.

When patients suffer from strokes, heart attacks, or severe infections, minutes matter. The best outcomes for patients with these time-dependent crises depend on the immediate, continuous availability of the same digital systems that ransomware can disrupt. When critical medical systems go offline, our opportunity to save lives diminishes. Our risk of error or misdiagnosis increases.

We are now learning that cyber attacks impact not just infected hospitals, but the surrounding healthcare ecosystem at large. Two months ago, a ransomware attack disabled five large hospitals in the San Diego area for an entire month. Adjacent hospitals were quickly overwhelmed with unprecedented numbers of emergency room patients, many of whom had serious, time-dependent illnesses. Wait times skyrocketed. Hospital beds rapidly filled. Clinicians caring for very sick patients lacked vital medical records from the infected hospitals. I saw firsthand the “spill-over” effects and understood that the vulnerability of one hospital is the vulnerability of many hospitals.

Recommendations

You have heard today from experts with technical and policy recommendations that, if enacted, will improve ransomware defenses across all sectors. However, as I hope you now recognize, healthcare has unique challenges which necessitate additional actions.

First, the effects of ransomware attacks on patients’ health should be scientifically studied, just like diseases such as diabetes. Most hospitals are not currently equipped to measure or report the impact of these attacks. I recommend the development of standardized metrics of cyber attack severity on hospitals. Mandatory reporting of patient safety and care quality outcomes should occur for severe attacks. I recommend that federal agencies such as the National Institutes of Health (NIH) and the National Science Foundation (NSF) prioritize funding for research on this topic.

Second, identifying cybersecurity vulnerabilities before they are exploited will protect patients. There is currently a disparity between what I call the healthcare cybersecurity haves and have nots. Lesser-resourced critical access and rural hospitals need help increasing their preparedness. As we seek to protect vulnerable hospitals, we must also avoid overly punitive measures for those unfortunate enough to fall victim to highly complex or novel cyber attacks, understanding that stiff fines or penalties may worsen

an already devastating operational impact. We are only as strong as our least defended communities.

Third, I support software bill of materials (SBOM) as one mechanism to increase transparency around cybersecurity vulnerabilities. SBOM enables manufacturers and healthcare delivery organizations to take more proactive steps to manage their cybersecurity risk. Furthermore I recommend ongoing support and legal protections for security researchers engaging in good-faith security research, otherwise known as coordinated vulnerability disclosure. We need help from ethical hackers if we are going to defeat the malicious ones.

Lastly, we must prepare hospitals for inevitable attacks. The ability to rapidly deploy backup manual patient care systems is key to reducing harms to patients. Such contingency planning takes resources and expertise.

Conclusion

In conclusion, I applaud this committee's leadership on ransomware response and remain optimistic about improving cyber resilience in healthcare. Our patients deserve excellent care. Ransomware and other cyber attacks targeting hospitals threaten our ability to deliver that care, as it's needed- when minutes matter.

Thank you for this opportunity to testify today and I welcome any questions you may have.

Ms. DEGETTE. Thank you so much.

The Chair now recognizes Mr. Carmakal for 5 minutes.

STATEMENT OF CHARLES CARMAKAL

Mr. CARMAKAL. Thank you. Chairman DeGette, Ranking Member Griffith, and members of the subcommittee, thank you for this opportunity to share our observations on the ransomware threat. My name is Charles Carmakal, and I am a senior vice president and CTO at Mandiant.

Mediant is an organization that helps other organizations across the globe deal with incredible cybersecurity challenges. We have got over 1,000 security professionals within 25-plus countries that help organizations deal with a variety of threats, including those threats that are orchestrated by foreign governments and organized criminals.

My colleagues here have done a pretty good job of talking about the ransomware overview, but I would like to provide a little bit more details on what the problem is like today. Ransomware is the number-one cybersecurity threat that we all face today. But what the—the problem that we are dealing with today is much more than just ransomware.

We call the problem "multifaceted extortion." This is how organizations get compromised by threat actors, and they deal with types of attacks where threat actors will steal data from organizations, disrupt business operations, will embarrass those organizations. They will reach out to partners of those organizations and extort them. They will reach out to customers and extort them, thus applying pressure to the victim organizations to pay substantial extortion demands. Extortion demands often will range, sometimes starting in six figures. But very often, for larger organizations, it could turn into seven figures, or even eight-figure demands.

Unfortunately, we work with organizations that are compelled to pay substantial extortion demands—not because they want to, not because they feel like that is the best option—because they really have no choice.

We work with organizations to really think about what are the things that they need to consider before paying extortion demands. I would like to share some of the observations and the learnings that we have acquired working with thousands of organizations dealing with this type of threat.

I think there is a lot of misconceptions about why threat—why victims pay threat actors. I think there is an assumption that organizations that have to pay don't have good cybersecurity hygiene, or they don't have good backups in place. And let me just dispel a few myths. A lot of times we find victim organizations pay threat actors because they want to accelerate the process of recovering their business operations. If you think about a situation where a municipality loses access to their emergency services, or a hospital can no longer treat patients and have to divert patients to other hospitals, it becomes incredibly important to get access to systems as quickly as possible. And so we sometimes find that victim organizations feel compelled to pay, because they feel that it is quicker to pay and to recover systems than it is by just using their backup infrastructure.

We also find that backup infrastructure generally isn't resilient enough to restore every single computer that was impacted over a short period of time during a ransomware and a multifaceted extortion operation.

The second thing that organizations need to think about before paying is how reliable is the threat actor. And I know it sounds kind of silly, thinking about the reliability of a threat actor, but today we find that a lot of criminals, they do demonstrate a certain level of reliability because they have recognized their business model actually depends on that.

You also need to understand whether or not the threat actors stole data from the organization before deploying decrypters—or before deploying encrypters across the enterprise. And if they stole data, there is obviously the risk of publishing that information. And we find that many victim organizations choose to pay because they feel that it is in their best interest to protect the sensitivity and the privacy of their customers and their business partners' information from being exposed on the internet.

The next thing that organizations need to think about is does the threat actor still have active access to the environment, and, if they do, can they escalate their attack and conduct more disruption?

You also need to understand whether or not cyber insurance will cover the claim.

And finally, you really need to think about is the threat actor sanctioned by the United States Government, and is it actually legal to pay the threat actor?

So those are some of the considerations that we talk to our clients about. And it is always our clients' decisions as to whether or not they should pay or not. But we want to actually walk them through the considerations.

So let me actually share some of the observations that we have learned when victims have actually paid threat actors.

Well, first of all, you can't just pay a threat actor and hope they go away. Technically, they have multiple different back doors to get access back into the environment if they want to. Many times we do find that they tend to move on, and move on to the next victim. They don't tend to come back, once they are paid, but technically, they do have the ability to do that.

You don't know who you are paying. You have no idea if you are paying a sanctioned entity. You have no idea if you are paying a terrorist organization. You don't know who you are paying. It is typically a responsibility of a separate company that engages in the negotiations with a threat actor and actual facilitation of payment. And a lot of times they are the ones that are actually trying to figure out who is being paid. But at the end of the day, you never know who is actually getting the money.

As I mentioned before, many threat actors are actually reliable because, again, they are—their business model depends on it. Reliability certainly, you know, depends on who the threat actor is. Many times we find that threat actors will provide working tools to be able to recover your systems and data. And they also provide a promise to delete the data that they have stolen from the victim environment. Of course, you never actually have any real guaran-

tees that the data was actually deleted that was stolen from the victim environment.

We do anticipate, at some point in time, that some of the data that was stolen—and for those threat actors that were paid, we do anticipate that they will likely publish information and the stolen data at a later point in time, especially as time goes on.

In conclusion, I would like to thank you for this opportunity to testify before the subcommittee. The ransomware and the multifaceted problem has become at a level that is completely intolerable, and we need to come together as a community to better address the problem. Thank you.

[The prepared statement of Mr. Carmakal follows:]

Prepared Statement
Charles Carmakal, Senior Vice President and Chief Technology Officer
FireEye Mandiant
Before the United States House Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
July 20, 2021

Introduction

Chairwoman DeGette, Ranking Member Griffith, and Members of the Subcommittee, thank you for the opportunity to share our observations and experiences regarding this important topic, as well as for your leadership on cybersecurity issues. My name is Charles Carmakal and I am a Senior Vice President and Chief Technology Officer at FireEye Mandiant ("Mandiant").

We commend the Subcommittee for holding this hearing to further examine recent ransomware and multifaceted extortion events. Both governmental and corporate responses to these attacks continue to evolve, and the Subcommittee plays an important role in overseeing these efforts.

As requested by the Subcommittee, I am going to discuss the ransomware landscape, including the threat actors, motivations, general aspects of this criminal enterprise, and recommendations for what organizations should do to mitigate this threat.

Background

In my role at Mandiant, I oversee a team of security professionals that help organizations respond to complex security breaches orchestrated by foreign governments and organized criminals. My team and I have had the opportunity to help organizations across the globe deal with some of the most significant and catastrophic cybersecurity incidents in history.

Mandiant employees are on the front lines of the cyber battle, actively responding to computer intrusions at some of the largest organizations on a global scale. We employ more than 1,000 cybersecurity experts in over 25 countries, with skills in digital forensics, malware analysis, intelligence collections, threat actor attribution, and security strategy and transformation. Over the last 17 years, we have responded to thousands of security incidents. It is unfortunate, but we receive calls almost every single day from organizations that have suffered a cybersecurity breach. For the security incidents we respond to, our mission is to help our clients investigate the attack, contain the incident, eradicate the attackers, guide them through the recovery of their environments, and help them become more resilient to future attacks.

Ransomware Overview

Ransomware is the most prolific cybersecurity threat today. Financially motivated threat actors primarily monetize their cyber intrusions by deploying ransomware and conducting multifaceted extortion. Organizations across all sectors and sizes are impacted. In the earlier days of ransomware, around 2013, ransom demands were low, often under $1,000. As the years progressed, around 2015, a threat group by the name of SamSam started asking for ransom demands around $20,000. Today, victim organizations are often coerced to pay six, seven, and

eight-figure extortion demands to recover business operations and mitigate the disclosure of stolen sensitive information. Many high-profile cyber intrusions over the past few years have involved ransomware and multifaceted extortion.

The term ransomware refers to the software used by threat actors to encrypt data on victim computers. It is also called a "ransomware encryptor." However, the industry often uses the term "ransomware" to describe any cybersecurity incident that involves extortion or destruction, even when ransomware encryptors were not used.

Many ransomware operations are run as a "Ransomware as a Service." This means there are different groups responsible for different functions. As an example, one group may be responsible for building ransomware encryptors and maintaining the victim shaming websites. Another group may be responsible for phishing employees and obtaining the initial access into a victim environment. Another group may be responsible for conducting the hacking actions within a company network, stealing data, and deploying the ransomware encryptor. The extortion payments are divided up between the groups involved. Ransomware as a Service lowers the barrier to entry for criminals that want to get started in ransomware.

The Evolution of Disruptive Intrusions: Ransomware to Multifaceted Extortion

In 2015, Mandiant observed a notable surge in disruptive intrusions in which threat actors deliberately destroyed critical business systems, leaked confidential data, taunted executives, and extorted organizations. We anticipated that intrusions would become more disruptive over time given the high impact and low cost to threat actors. Over the next few years, financially motivated threat actors began shifting away from stealing payment card information to deploying ransomware. Threat actors asked for ransom payments in exchange for the key to decrypt their data.

In late 2019, a hacking group by the name of Maze changed the way financially motivated threat actors would conduct their intrusions. Maze would find and steal sensitive corporate and customer information in addition to encrypting data on systems. They launched a website to publicly shame the victim organizations that they compromised and publish the stolen information. They would demand money in exchange for tools to recover the data that they encrypted, a promise to not publish the data they stole, and details of how they compromised the organization. The shaming site served as a warning to those who did not comply. Extortion demands were often in the six- and seven-figure ranges, but sometimes went up to eight-figures. Shortly after, many other cyber-criminal groups followed suit. There is a distinct upward trend in both the number of victims that have appeared on these victim shaming sites and the number of groups using this methodology to pressure victims.

Last October, the cyber threat in the United States reached an unprecedented level. Hospitals across the U.S. were disrupted by a group of eastern European threat actors. Hospital technology systems were taken offline, and medical professional and administrative staff had to rely on paper and pen to record data. Many hospitals had to divert patients and ambulances to emergency departments at other hospitals. The impact of cyber intrusions to human lives has never been more dire.

Most of today's intrusions by financially motivated threat actors involve multifaceted extortion. Threat actors will apply immense pressure to coerce victims to pay substantial extortion demands – often in the seven to eight-figure range. Some threat actors will convince news and media organizations to write embarrassing stories about victims. They may call and harass employees. They may notify business partners that their data was stolen due to a breach of their partner, creating friction in business relationships. They may also conduct denial of service attacks to create further chaos and disruption.

Ransomware and multifaceted extortion events have reached an intolerable level and we must come together as a community to defend our nation.

Extortion Payments – Considerations for Paying

Mandiant does not negotiate with threat actors or pay extortion demands on behalf of our clients. Nor do we make recommendations or provide advice on how to respond to such demands. However, we are often asked to help executives and board members evaluate their options with respect to recovering from disruptive intrusions. We advise our clients to discuss with their outside counsel and to think through several considerations before deciding whether or not to comply with extortion demands.

Some of the considerations are outlined below:

1. **How quickly can you recover your systems and data on your own?**
   Organizations may not be able to recover their systems and data on their own. This could be due to not having mature backup processes or the threat actor destroying their backups. Often, organizations have good backups, but the restoration process is slow due to the volume of systems that were encrypted and need to be recovered.

2. **How reliable is the threat actor?**
   Many threat actors recognize their business model requires them to be reliable and credible. If a victim paid a threat actor, and the threat actor did not provide a working decryption tool or published stolen data anyway, the threat actor would develop a negative reputation. This would decrease the likelihood of them being paid by other victims in the future.

3. **Did the threat actor steal data before they deployed their encryptors? How sensitive is the data that they stole?**
   Nowadays, most threat actors steal large volumes of sensitive data from victim organizations. Many organizations feel compelled to pay not because they need tools to recover their data, but because they feel obligated to do everything they can to protect their customer and partner data.

4. **Does the threat actor still have active access to your network?**
   Threat actors almost always establish multiple backdoors into victim environments, enabling them to escalate their attacks if they do not get paid.

5. **Will cybersecurity insurance cover the claim?**
   Cybersecurity insurance helps many organizations recoup some of the cost associated with the painful decision of paying threat actors.

6. **Is the threat actor sanctioned by the U.S. Department of Treasury?**
   Paying sanctioned threat actors is illegal and organizations need to take appropriate actions to ensure that they do not pay a sanctioned entity. This usually requires support from firms or third party experts and law enforcement.

Extortion Payments – What Have we Observed When Victims Pay?

There are many assumptions about what happens when a victim organization pays a threat actor. Here is a summary of observations based on hundreds of incidents that Mandiant has investigated:

1. **Threat actors usually deploy multiple backdoors within victim environments**.
   Unless the backdoors are removed and incident containment and remediation steps are taken, the threat actor may have the ability to re-compromise the environment. If a victim chooses to pay the threat actor, they must also take steps to block their access and eradicate them from the environment. This may require investments in cybersecurity tools, processes, and people.

2. **Many threat actors provide working decryption tools when they are paid.**
   Threat actors realize their business model requires them to provide positive outcomes to victim organizations, or they would develop a negative reputation and they would not be paid in the future. Threat actors often provide decryption tools that work, however, the decryptors often have unintentional bugs that may not effectively decrypt every single file. Additionally, many decryptors are slow.

3. **Many threat actors do not publish stolen data when they are paid.**
   Some threat actors may provide proof that they discarded the data they stole if they are paid, however, there is no guarantee that the proof was authentic, or they don't have other copies of the data. Prior to 2019, we observed many threat actors that publicized stolen data and re-extorted victims after being paid. Over the next 24 months, Mandiant anticipates some threat actors will re-extort victims and publish stolen data at a later time, despite being paid.

4. **Many threat actors don't re-compromise entities that paid them.**
   Today, threat actors can opportunistically compromise other organizations easily. They often move on to the next target when they are paid.

Recommendations for Organizations to Mitigate the Risk of Ransomware and Multifaceted Extortion Events

In September 2019, Mandiant published a technical whitepaper[1] outlining the most common and high priority steps Mandiant incident responders use to help organizations respond to and contain ransomware events. The document provides detailed recommendations that organizations should implement immediately following a ransomware event – or ideally before a ransomware event – to limit the impact. It includes detailed tactical recommendations for endpoint hardening, credential exposure and usage hardening, Windows domain controller isolation and recovery planning, and Windows Group Policy Object (GPO) permissions and monitoring.

Conclusion

On behalf of FireEye Mandiant, I thank you for this opportunity to testify before the Subcommittee. The ransomware and multifaceted extortion challenge has become so prolific and dire, that we should no longer view it as a mere nuisance or business risk—we should consider it a significant threat to global security. The number of attacks continues to rise at an alarming rate. We stand ready to work with you and other interested parties to devise effective solutions to deter malicious behavior in cyberspace and to build better resiliency into our networks.

[1] https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wp-ransomware-protection-and-containment-strategies.pdf

Ms. DEGETTE. Thank you so much.

The Chair now recognizes Mr. Reiner for 5 minutes.

STATEMENT OF PHILIP JAMES REINER

Mr. REINER. Madam Chair DeGette, Ranking Member Griffith, Chairman Pallone, members of the subcommittee, thank you for the opportunity to testify today on the pervasive threat that ransomware poses to our national security. My name is Philip Reiner, and I am the chief executive officer of the Institute for Security and Technology.

Our mission at IST is to create trusted venues where national security policymakers can engage with technology leaders to work together to devise solutions to emerging security threats. That is what allowed us to convene the Ransomware Task Force, of which I was the executive director. We were pleased to convene representatives from more than 60 public and private organizations to devise a comprehensive framework for combating the ransomware threat.

I will focus my testimony here today on three areas: first, on the top-line recommendations of that task force report; second, note some positive steps we have seen taken since that report launched in April; and third, note some items from the report that will require congressional action.

As is often repeated, there is no single solution to this challenge. It poses too large of a threat for any one entity to address alone. The timing of this hearing is thus incredibly important. This is an international cybersecurity crisis, the scale and magnitude of which demands leadership and action. The task force determined four goals that should frame a comprehensive approach to deter, disrupt, prepare, and respond. These goals are interlocking and mutually reinforcing. This framework should be considered as a whole. To achieve these goals, the priority recommended actions were as follows.

Number one, coordinated international diplomatic and law enforcement efforts must prioritize ransomware and work to eliminate criminal safe havens.

Number two, the United States should and must lead by example and execute a sustained, aggressive, whole-of-government, intelligence-driven antiransomware campaign, coordinated by the White House and in close collaboration with the private sector.

Number three, governments should establish cyber response and recovery funds, mandate that organizations report ransom payment, and require organizations to consider alternatives first, before making any such payments.

Number four, a clear, accessible framework must be developed to help organizations prepare for and respond to ransomware attacks.

And then number five, the cryptocurrency sector must be better understood and more closely regulated to prevent further facilitation of ransomware.

Since April, encouraging actions have been taken, some of which have been noted already. These include the recent White House launch of an interagency Ransomware Task Force. This is a critical initial step, as the United States needs to execute a campaign that leverages all tools of national power: diplomatic, economic, intel-

ligence, law enforcement, and military. Again, this must be done in close cooperation with the private sector in order to be successful.

Additionally, the call for leader-level diplomatic prioritization of these issues, in some ways, has been heated. President Biden has repeatedly asserted that ransomware is a top priority and included this as a top-three item in his recent summit with Russian President Putin. Similar prioritization by the United Kingdom, the G7, the EU, Australia, and others continues this necessary trend. These declarations are great initial steps and need to be followed up on with action. DOJ and DHS have their own internal ransomware-focused efforts. The National Institute of Standards and Technology has released an initial ransomware profile. Also, seven large U.S.-based insurers have established a consortium to share data. Followthrough will be the key for all of these steps and, hopefully, for many more that are to come.

Finally, a number of recommended steps from the report can be highlighted that necessitate congressional action, which include but are not limited to requiring organizations to report ransomware payment information prior to payment, requiring further steps to shore up the cryptocurrency ecosystem, providing clarification of lawful defensive measures that private-sector actors can take, requiring local governments and managed service providers to adopt limited baseline security measures, and creating a ransomware response fund to help incentivize the nonpayment of ransoms.

Congress has a critical role to play in a whole-of-government response to this threat, and the Institute for Security and Technology welcomes the opportunity to inform the work of this committee. Thank you for your leadership, and I look forward to your questions.

[The prepared statement of Mr. Reiner follows:]

Testimony of

Philip James Reiner
Chief Executive Officer
Institute for Security and Technology

Before the
United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

July 20, 2021

"Stopping Digital Thieves: The Growing Threat of Ransomware"

Chair DeGette, Ranking Member Griffith, Chairman Pallone, Ranking Member McMorris Rodgers, members of the Subcommittee on Oversight and Investigations, thank you for the opportunity to testify today on the scourge of ransomware and the pervasive threat that it poses to our critical infrastructure, public health and safety, and overall national security. It is an honor to join such an illustrious panel of witnesses here today. It is my hope that I can contribute insights to this discussion in support of the Subcommittee's investigation into what has become a national - and international - cybersecurity crisis.

My name is Philip Reiner, and I am the Chief Executive Officer of the Institute for Security and Technology (IST). I am a former Pentagon civil servant that served in the Office of the Secretary of Defense for Policy in the Pentagon for almost a decade, the last four years of which I was detailed to the National Security Council, where in my final role I served as the Senior Director for South Asia. I have been challenged over my career to devise and execute strategies meant to stop nuclear weapons from falling into the hands of terrorists, prevent attacks against the American homeland, build international partnerships in support of vast, complicated missions, and now in my role as CEO of IST, to create trusted venues where national security policymakers can directly engage with technology leaders and those engaged in trusted public-private operational cooperation. At IST, our mission is to work across these communities, bridge gaps, build relationships, and catalyze novel solutions to technology-driven emerging national security threats.

I appear before you today not just as the CEO of IST, but also as the Executive Director of the Ransomware Task Force,[1] which was convened by IST earlier this year. The effort was undertaken from January to April, with the express purpose of developing a comprehensive framework for action to combat the ransomware scourge.[2] We were extremely pleased to welcome representatives from 60+ public and private organizations, to whom IST and myself are deeply indebted - and without whom I would not be here testifying to you today on these matters. Together with this amazing group, we "sprinted a marathon" and devised 48 recommended actions across four main areas of focus: to deter attacks, to disrupt ransomware actors, to help organizations prepare, and to improve ransomware response. In the end, ransomware is a solvable problem - but currently it is metastasizing at an alarming rate.

In large part, IST stood up the Ransomware Task Force because we were frustrated with what we perceived to be a lack of coordinated action as the ransomware threat was clearly rising in 2019 and 2020. And indeed, just a week after the Task Force released its report, the Colonial Pipeline cyberattack struck. As others have testified elsewhere and spoken to at length in public fora, the priority recommendations from the Task Force include the topline need for sustained,

[1] The Ransomware Task Force. https://securityandtechnology.org/ransomwaretaskforce.
[2] Combating Ransomware. *A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*. 27 April 2021. https://securityandtechnology.org/ransomwaretaskforce/report/.

coordinated, and collective action among governments, industry, academia, and civil society to substantially reduce the ransomware threat.

I want to make clear right up front that there are professionals - both in public and private roles - who are toiling night and day to prevent, mitigate, and respond to the ransomware threat which today leaves no domain untouched - from critical infrastructure and key resources to hospitals and schools. These information security professionals are overworked and often outgunned. Our country is indebted to them for their tireless efforts, and it is our hope to improve the odds against which they are pitted, while we aim to decrease the threat to our national security posed by these criminals. These professionals deserve every element of support we can muster.

I will focus my testimony today on three main areas: first on an overview of the topline recommendations of the Task Force report, which lays out a comprehensive framework to address ransomware; second, on steps already taken since the launch of the report in April; and third, I will highlight Action items from the the Task Force report that will require Congressional action. The most critical element of this conversation is not the report we released, but the urgent need for the adoption of its recommendations, with speed, priority, and resources. The timing of this hearing is thus incredibly important: unless the actions recommended by the Ransomware Task Force are broadly and quickly implemented, the scourge of ransomware and the threat it poses to critical infrastructure and our national security will only continue to worsen.

To clarify, when I assert that the ransomware problem will only continue to worsen if not addressed in a comprehensive fashion, it is instructive to highlight recent attacks against the Colonial Pipeline Company[3] and the information technology management platform provider Kaseya.[4] The Colonial Pipeline example is instructive in that it is relatively clear that the Darkside criminal group behind the attack likely had no idea their extortion target was such a critical element of U.S. energy infrastructure. The "ransomware as a service" business model provides ransomware capabilities to would-be criminals who do not have the skills or resources to develop their own malware. This creates distributed opportunities with a low barrier to entry to conduct ransomware attacks, which may occur indiscriminately and without consideration for the consequences of the victim in question.[5] What happens when a ransomware attack shuts down water treatment facilities for a large metropolitan city, or attacks against healthcare systems escalate even further? These are not hypothetical assertions of possibility - it is simply only a matter of time that these attacks will happen if we don't take concerted action now.

---

[3] Sanger, David E, and Nicole Perlroth. "Pipeline Attack Yields Urgent Lessons about US Cybersecurity." *New York Times*, 14 May 2021, www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.
[4] Satter, Raphael. "Up to 1,500 Businesses Affected by Ransomware Attack, U.S. Firm's CEO Says." Reuters, 6 July 2021, www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/.
[5] Palmer, Danny. "Ransomware as a Service Is the New Big Problem for Business." ZDNet, 4 Mar. 2021, www.zdnet.com/article/ransomware-as-a-service-is-the-new-big-problem-for-business/.

The Kaseya incident is doubly instructive. As part of the Ransomware Task Force process, we took time as part of a sub-working group to game out some of the worst case scenarios. One imagined scenario was a ransomware gang massively scaling the distribution of their malicious payload through the exploitation of a vulnerable managed service provider - an increased level of sophistication with devastating effect on a much larger scale than previously seen. That is what we've just witnessed in the attack against Kaseya - except it was this scenario on steroids, targeting the information technology (IT) management capabilities provided to a range of Managed Service Providers (MSPs), instead of an attack against just one. Now that this use case has been proven effective, other criminal groups will follow suit - likely with even more critical companies compromised through supply chain-style ransomware attacks. Ransomware actors have every incentive to continue escalating their tactics to find the situations most effective at extorting ransoms, ones that put enormous pressure on essential functions. These are not scenarios we are ready to withstand.

As mentioned above, ransomware is not a new threat. This is a long-standing type of cybercrime and malware attack. People have been working to stop these attacks for years. The dynamic has drastically changed, however, and ransomware is no longer just an economic cybercrime. Today it has become a malicious form of online activity that has immense real world effects: it has taken on the scale and virulence of a threat to our national security, to our societal and economic well being, to our critical infrastructure, and to our public health and safety.

The costs of ransomware also go far beyond the ransom payments themselves, incurring much broader societal harm. Cybercrime is typically seen as white-collar, but while ransomware is profit-driven and "non-violent" in the traditional sense, that has not stopped these attackers from routinely threatening supply chains, risking human lives by shutting down hospitals with critical patients, diverting vital public resources, threatening the loss of data/privacy, disrupting schools and colleges, exposing the data of minors, placing entire cities under siege, and extorting exorbitant and destructive ransoms in the millions of dollars. These criminals, on the whole, do not care who they victimize - whether it's a gas pipeline, a managed service provider, an elementary school, or a large hospital system. They do not care if people die - and it is clear based on the medical literature that these attacks against hospitals and health care systems increase the risk of severe outcomes for patients unable to receive care. These criminals clearly do not care if essential services are disrupted. In fact, they count on it - the more desperate the victims, the more inclined they may be to pay the ransom.

What has changed to make ransomware a significantly more virulent threat than it was before? A few factors can be clearly identified:

1. The affiliate "ransomware as a service" business model has created efficiencies and deniability through the distributed, outsourced specialization of tasks
2. Vast increases in digital attack surfaces, offering almost neverending opportunities for exploitation of vulnerabilities, including through increasingly distributed operations due to rise of work from home during the COVID pandemic
3. Anonymous, ubiquitous, and decentralized payment infrastructures have made cross-border payments vastly more efficient and inexpensive, while significantly increasing the challenge of tracing the laundering of digital currencies
4. Massive increases in computing power and access to distributed cloud resources exacerbated the pre-existing challenge posed by botnets, and
5. Finally, with each of these capabilities, actors are more able to operate with impunity from safe havens out of the reach of law-enforcement in the nations where attacks occur

This is important to make clear: efforts to mitigate ransomware have been effective in some cases. But the nature of the threat itself has evolved to such an extent that our response must evolve as well - the criminals rely on the seams between our Departments and Agencies, our classifying these types of attacks only as crimes instead of national security threats, and the gaps between public and private abilities to collaboratively prepare and respond.

Ransomware criminals have also come to count on there being no sustained follow through on disruptive activities: for example, the public-private effort to disrupt the Emotet infrastructure[6] earlier this year was an immense success in its breadth and creativity. However, criminals were almost immediately reconstituting the technical infrastructure that had been disrupted.

Despite the dire reality and complexity of the current situation, I believe, and the Ransomware Task Force agrees, that this is a solvable problem. There is no single solution to this set of challenges: this is an international cybersecurity crisis that demands that countries and companies work closely together on a range of historically difficult tasks. The combination of the actions needing sustained attention compound the challenge in blunting the trajectory of these attacks. Ransomware has become too large of a threat for any one entity to address, and the scale and magnitude of this challenge urgently demands coordinated global action.

The Comprehensive Framework to Combat Ransomware

In response to the overall challenge, the Ransomware Task Force process resulted in 48 recommended actions within four focus areas. We debated the most effective framework and determined those four focus areas to be the most salient as part of a comprehensive approach:

[6] Federal Bureau of Investigation. "FBI, Partners Disarm Emotet Malware." News release, 1 Feb. 2021, https://www.fbi.gov/news/stories/emotet-malware-disrupted-020121.

1. **Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy:** ransomware can be deterred if conducting an attack becomes more risky, less likely to succeed, and more costly. This includes holding criminals accountable, promoting international prioritization and collaboration, and eliminating safe havens where criminals operate with impunity.
2. **Disrupt the ransomware business model and decrease criminal profits:** ransomware can be disrupted when threat actors are pushed out of the business and the appeal to new threat actors is reduced. This includes increased targeting of the criminals themselves, their technical infrastructure, and the cryptocurrency payment process they rely on for funds.
3. **Help organizations prepare for ransomware attacks:** organizations will be better prepared for an attack with clear directives, adequate resources, and the right incentives. This includes providing a single, clear ransomware framework for preparation and response, and incentivizing businesses and governments to increase their cyber hygiene and defend their networks.
4. **Respond to ransomware attacks more effectively:** better information sharing and victim support will improve our collective resilience to ransomware. This includes providing greater resources for victims, enhanced reporting mechanisms, and clear guidelines for what to do after a ransomware attack.

At its core, the intent is to do all we can to disrupt the ransomware business model. These goals are interlocking and mutually reinforcing. For example, actions to disrupt the ransomware payments system will decrease the profitability of ransomware, thereby helping to deter other actors from engaging in this crime. In a similar vein, many actions taken to better prepare organizations for ransomware attacks, such as informing them about the risks, will also improve their ability to respond, while understanding more about how organizations are responding to ransomware attacks will help improve organizations' collective preparedness. Thus, this framework should be considered as a whole, not merely a list of potential disparate actions.

The only area where I and other Task Force members did not come to a concise conclusion was in regard to the payment of ransoms. The question of whether to prohibit payment of ransoms has become increasingly pressing, and was raised by every working group in the Task Force. Practical implementation of such a ban would be challenging at this time: the ecosystem is vulnerable, and without steps to shore up defenses and disrupt ransomware criminals, it would be overwhelmed with attacks. Simply banning payment in the immediate term will do little to stop ransomware attacks, and place significant onus on victim organizations.

The Ransomware Task Force did not reach consensus on recommending a prohibition on paying ransoms. However, it did develop a proposed phased approach to potentially reach prohibition which members agreed would be necessary to obtain the desired impact. The Task Force

concluded that the most reasonable and effective approach would be a multi-year, conditions-driven approach based on milestones, with prohibitions beginning within two years. The priority considerations must be the timeline, the phasing of steps, and victim protection and support. Proposed milestones, such as hardening security of critical infrastructure, should be pursued concurrently. If pursued vigorously, the necessary milestones could be met much more rapidly than the proposed timeline.

The overall topline recommendations from the Ransomware Task Force report are below. These priority recommendations are the most foundational and urgent; many of the other recommendations were developed to facilitate or strengthen these core actions:

1. Coordinated, international diplomatic and law enforcement efforts must proactively prioritize ransomware through a comprehensive, resourced strategy, including using a carrot-and-stick approach to direct nation-states away from providing safe havens to ransomware criminals.
2. The United States should lead by example and execute a sustained, aggressive, whole of government, intelligence-driven anti-ransomware campaign, coordinated by the White House. In the U.S., this must include the establishment of 1) an Interagency Working Group led by the National Security Council in coordination with the nascent National Cyber Director; 2) an internal U.S. Government Joint Ransomware Task Force; and 3) a collaborative, private industry-led informal Ransomware Threat Focus Hub.
3. Governments should establish Cyber Response and Recovery Funds to support ransomware response and other cybersecurity activities; mandate that organizations report ransom payments; and require organizations to consider alternatives before making payments.
4. An internationally coordinated effort should develop a clear, accessible, and broadly adopted framework to help organizations prepare for, and respond to, ransomware attacks. In some under-resourced and more critical sectors, incentives (such as fine relief and funding) or regulation may be required to drive adoption.
5. The cryptocurrency sector that enables ransomware crime should be more closely regulated. Governments should require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws, including Know Your Customer (KYC), Anti-Money Laundering (AML), and Combatting Financing of Terrorism (CFT) laws.

Encouraging Actions Are Being Taken - But More is Needed

Since the launch of the Task Force's recommended comprehensive approach in April 2021, it has been encouraging to see international, national, and industry steps taken in the direction of some of the recommended actions. Most immediately, the announcement from the White House on

July 15th that it has launched an interagency Ransomware Task Force is extremely encouraging. From the list of 48 recommendations in the Task Force report, my personal assertion is that this is the most critical step necessary in order to move all elements of national power in the right direction: that the United States needs to execute a relentless, sustained, well resourced, international counter-ransomware campaign that leverages all tools of national power: diplomatic, economic, intelligence, law enforcement, and military. While the announcement from the White House indicates the process is just getting started, it is encouraging to know top-down leadership has been instituted. The areas of focus as part of that effort will apparently also include a number of priority areas recommended by the Task Force: coordinating with international allies, disrupting ransomware operators, improving visibility into the cryptocurrency ecosystem, developing ways to halt ransom payments, promoting resilience among critical infrastructure providers, coordinating interagency ransomware resources via http://stopransomware.gov, and using the Rewards for Justice program to offer cash payments for tips leading to arrests of ransomware operators. These are all really fantastic steps in the right direction as part of an overall, coordinated, whole of government effort.

Additionally, the Ransomware Task Force's call for leader-level prioritization of ransomware in many ways has been heeded - exemplified by President Biden's repeated assertions that ransomware is a top priority for his Administration, as well as the White House's inclusion of ransomware as a top three priority during President Biden's summit with Russian President Vladimir Putin. Increased political, diplomatic, economic, and law enforcement pressure on President Putin to take action against those groups acting with impunity from Russian soil was a topline recommendation of the Task Force. As it entirely remains to be seen as to whether the Russian leader will ever take action against these groups, it is a powerful signal to both the international community that this is a national level priority, and begins the process of sending the necessary deterrent signal to the ransomware criminals themselves that they will no longer be left to simply get away with these crimes. The prioritization of ransomware by the leadership in the United Kingdom[7] and as was expressed by the G7 leaders in June of this year continues the necessary trend of making declarative policy that the trajectory of these attacks must be dampened.[8] Those declarations need to be followed up with strategies and action plans - most of which can be taken from the recommendations of the Task Force and repurposed for national decision making around the world.

Additionally, in June the U.S.-EU Ministerial Meeting on Justice and Home Affairs included the launch of a U.S.-EU joint working group on prevention and enhanced law enforcement

[7] National Cyber Security Centre. "Cyber security sector leaders to appear at CYBERUK." News release, 5 May 2021. https://www.ncsc.gov.uk/news/leading-figures-from-uk-politics-to-appear-at-cyberuk; Corera, Gordon. "Foreign Secretary issues warning to Russia on ransomware." *BBC News*, 12 May 2021, https://www.bbc.com/news/technology-57084943.

[8] Reuters Staff. "G7 demand action from Russia on cybercrimes and chemical weapon use." Reuters, 13 Jun. 2021, https://www.reuters.com/world/europe/g7-demand-action-russia-cybercrimes-chemical- weapon-use-2021-06-13/.

cooperation to address the rise of ransomware attacks in the United States and Europe.[9] Again, these are positive steps in the right direction, but it remains to be seen what work will be undertaken and with what areas of focus.

As all these steps have been undertaken, the U.S. Department of Justice and the Department of Homeland Security from early on initiated their own internal ransomware-focused task force efforts. The recommendations in the Task Force report were for U.S. Departments and Agencies to ramp up actions against the ransomware threat through prioritization and resourcing solutions, which is exactly what can be seen by these sets of actions. The Department of Justice has continued to engage in an internal effort to prioritize ransomware response and investigations, exemplified by a wallet seizure and the recovery of extorted funds in the Colonial Pipeline instance.[10] The DOJ elevation of investigations of ransomware attacks to a similar priority as terrorism shows the level of intensity these criminal activities now will be addressed with - and how the necessary resources will be made available as well. These are exactly the types of steps recommended by the Task Force. As noted above, the Department of Homeland Security took the initiative to launch www.stopransomware.gov,[11] which is directly in line with the Task Force recommendation to consolidate resources into a one-stop-shop / single source of truth, and focused its first cybersecurity sprint on ransomware. These steps are but a part of the clear emphasis that DHS and its leadership are placing on this pernicious threat.

Additionally in line with the recommendations of the Task Force, the National Institute of Standards and Technology (NIST) released an initial ransomware profile based on the Cybersecurity Framework, with a public call for comment, and hosted an initial workshop on July 13th, 2021 to garner insights from partners and the public.[12] Finally, also in line with the recommendations put forward in the Task Force report, seven large U.S.-based insurers combined forces to establish a consortium called CyberAcuView[13] to share data and broaden the industry's collective understanding of the threat so as to more effectively underwrite cyber insurance policies going forward. The threat is so significant that we need to see many more such actions, but these are all moves in the right direction. Follow through will be key.

---

[9] Underwood, Kimberly. "U.S. and EU To Collaborate Against Ransomware." *The Cyber Edge*, 24 Jun., 2021, https://www.afcea.org/content/us-and-eu-collaborate-against-ransomware.
[10] Department of Justice. "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside." News release, 7 Jun. 2021. https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.
[11] Department of Homeland Security. "United States Government Launches First One-Stop Ransomware Resource at StopRansomware.gov." News release, 14 Jul. 2021, https://www.dhs.gov/news/2021/07/14/united-states-government-launches-first-one-stop-ransomware-resource.
[12] National Institute of Standards and Technology. *Cybersecurity Framework Profile for Ransomware Risk Management (Preliminary Draft)*. By William Barker, Karen Scarfone, William Fisher, and Murugiah Souppaya. NISTIR 8374 (Draft). Jun. 2021. https://csrc.nist.gov/publications/detail/nistir/8374/draft.
[13] CyberAcuView. "Consortium of Leading Cyber Insurers Announce the Launch of CyberAcuView." News release, 17 Jun. 2021. https://cyberacuview.com/press-release-june-2021/.

A particular point of contention has been the use of offensive cyber actions to address the ransomware threat. The Task Force recommended that national governments, working closely through coordinated action, should consider all tools of national power. In my personal opinion, the authorities typically relied upon to address ransomware attacks are not commensurate with the level of harm these attacks are currently causing nor sufficient to deter their continued increase going forward. That does not mean that new authorities are needed to provide the options necessary to deter these activities. Rather, through the recommended interagency coordinated Joint Ransomware Task Force, the U.S. government can more effectively take advantage of the array of authorities and other tools that are already available.

The Ransomware Task Force report makes clear, for example, that while the Computer Fraud and Abuse Act (USC Title 18 §1030) is perhaps an appropriate tool for prosecuting some ransomware attacks, it can be made more powerful when combined with alternate tools of national power and already existing prosecutorial options. The Task Force recommended Action 2.3.3, for example, stated that any federal counter-ransomware framework should "apply strategies for combating organized crime syndicates to counter ransomware developers, criminal affiliates, and supporting payment distribution infrastructure." This could include other federal statutes covering Racketeer Influence and Corrupt Organizations (RICO - Title 18 §1962), money laundering, commercial extortion, homicide - and even terrorism. The Department of Justice's recent internal memoranda to this effect point to a move in this direction already. These could potentially add significant deterrent value to an overall counter-ransomware strategy.

In my personal opinion, the full U.S. response to ransomware attacks must expand beyond reliance on USC Title 18 for criminal investigation and prosecution. The authorities provided under USC Titles 10, 31, and 50 should all be invoked as necessary to provide more effective and robust options to deter and disrupt ransomware actors and the infrastructure used to attack U.S. critical infrastructure and hold our public health and safety hostage. Title 31 allows the Treasury Department, through the Office of Foreign Asset Control (OFAC), to put financial sanctions on foreign entities that have conducted or facilitated cyber attacks against U.S. organizations. Titles 10 (military authorities) and 50 (intelligence authorities) can improve domestic cyber defenses by putting the United States on the offensive. They could be invoked to take an "active" or "forward" defensive posture to proactively disable and disrupt foreign-based cyber threats - as was seen as part of coordinated interagency activity during the 2020 Presidential elections.

Finally, the Intelligence Community must be used to augment and support these counter-ransomware actions, in sequenced and coordinated operations as part of an overall national strategy, as has been done in the ongoing fight against transnational terrorist threats. There are clear differences between the two sets of challenges - ransomware vs. counterterrorism - but structural similarities exist. This all again points to the need for a top-down, intelligence-driven coordinated effort that deploys all tools of national power.

It is important to note that deploying and executing offensive cyber operations through the appropriate authorities will primarily be successful in that they can create a window of opportunity for other actions to take place. By no means, however, will Title 10 and 50 actions alone eliminate the ransomware threat. As noted, the ransomware actors will quickly reconstitute, and other actors will rise to take the place of those who may end up taken into custody. New groups will coalesce with new tools in response to disruptive actions - which points to the clear need in the window of time that is created for assertive action to shore up defenses and raise the level of seriousness that is afforded to cyber hygiene. Cybercrime persists in large part due to poor cyber hygiene - thus the rest of the applicable solutions recommended by the Task Force must be implemented as well.

Priority Considerations for Congress

Within the Actions recommended by the Ransomware Task Force, a number can be highlighted that are items that will necessitate Congressional action, and I would like to highlight them here:

1. Action 2.1.2. Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws
2. Action 2.2.2: Clarify lawful defensive measures that private-sector actors can take when countering ransomware
3. Action 3.3.1: Update cyber-hygiene regulations and standards
4. Action 3.3.2/3: Require local governments and managed service providers (MSPs) to adopt limited baseline security measures
5. Action 3.4.2: Expand Homeland Security Preparedness grants to encompass cybersecurity threats
6. Action 3.4.5: Investigate tax breaks as an incentive for organizations to adopt secure IT services
7. Action 4.1.2: Create a Ransomware Response Fund to support victims in refusing to make ransomware payments (incentivize non-payment of ransoms)[14]
8. Action 4.2.4: Require organizations and incident response entities to share ransomware payment information with a national government prior to payment

Congress will have a critical role to play here in implementing these proposals, and the Institute for Security and Technology looks forward to working with members of this Committee on advancing legislation pertaining to these proposals. Ransomware succeeds in large part due to a broad underinvestment in cybersecurity by both industry and government. As noted, this highlights the need for strengthening the incentive structures, but also to redouble outreach

[14] The United States Innovation and Competition Act of 2021 (USICA), passed in June 2021, includes the creation of a Response and Recovery Fund, the funds from which could be utilized for asset response and recovery purposes in the event of a significant cyber incident. See United States Innovation and Competition Act, S. 2160, § 4251-4252, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1260.

through entities such as NIST and the Small Business Administration - which requires greater resources. When considered in light of the scope of the threat from ransomware, this outreach and resources become all the more important as small businesses drive our economy.

It is important to note that conversation as part of the Task Force process focused on the clear need to ensure the recommendations were not perceived as condoning "hackback" activities, but it was also clear from an industry perspective that expectations of what defensive actions can be taken under CISA 2015 could be further clarified. This would provide greater levels of confidence to an array of different stakeholders interested in playing as proactive a role as possible in efforts to disrupt ransomware criminal network behaviors.

Finally, this set of recommended Actions point clearly to the challenge of raising the bar for expectations from industry - and from government - in terms of the level of commitment and resources applied against these threats and the vulnerabilities that drive them. The scale and breadth of the ransomware threat demands a reprioritization of attention, effort, and resources at the same levels we once saw for counterterrorism. The need to establish the right investment structures would be greatly assisted if the steps recommended in the Task Force report were undertaken, to include those listed above that would likely require Congressional action.

Conclusion

The actions detailed in the Task Force report need to be enacted together as soon as possible, and must be coordinated at a national and international level. If this framework is implemented in full, the international community could see a decrease in the volume of these types of attacks in one year's time. With every recommended action we worked through the practical implications, and in most cases we presented immediately actionable recommendations. Ransomware has become too large of a threat for any one entity to address, and the scale and magnitude of this challenge urgently demands coordinated global action - no one can do this on their own.

The Institute for Security and Technology offers a unique perspective on these issues, as a neutral 501c3 non-profit that straddles the national security and technology communities. Our ability to translate between both public and private leaders across domains through deep, trusted interactions allows for creative solutions and the ability to work directly with both federal leaders and industry partners on the implementation of necessary actions. We are privileged to provide this platform to facilitate communication and cooperation between the government and the private sector in our common interest to collectively defend against ransomware attacks.

This bears repeating - Congress has a vital role to play here. We welcome the opportunity to inform the work of this committee in this capacity and stand ready to assist as needed.

Ms. DEGETTE. Thank you so much, and thank you to the entire witness panel for excellent testimony. It is now time for our questioning, and the Chair will recognize herself for 5 minutes.

As I said in my opening statement, senior cyber experts from the government have expressed concern about some of the private sector's compliance with cyber hygiene requirements, and the limits of——

VOICE. This meeting is being recorded.

Ms. DEGETTE. Thank you. And the limits of the Federal Government's existing authorities to manage the problem.

So, as Congress, it is our job to make sure that the executive branch has the authorities it needs. I want to hear from each one of you about this.

Mr. Reiner, your testimony identifies eight priority considerations for Congress. Which two or three of those would be the most impactful, and why?

Mr. REINER. Madam Chair, thank you for the question. I appreciate the sentiment that there is much more that companies can be doing. I think——

Ms. DEGETTE. Sir, I have 5 minutes. So if you can tell me which two or three of the actions you identify would be most impactful, I think that would be helpful.

Mr. REINER. Yes, ma'am.

Ms. DEGETTE. Thank you.

Mr. REINER. As the report laid out, I think one of the steps that can be taken for organizations, as part of potential grants that can be provided, that they need to expand a certain percentage of their efforts on cybersecurity——

Ms. DEGETTE. OK.

Mr. REINER [continuing]. To basically raise their baseline application of their own funds in order to receive national grants.

Ms. DEGETTE. Federal.

Mr. REINER Another element that the task force put forward was that, in order to receive grant funding, was that a company would have to meet the baseline requirements that are put forward in the framework that we described in the report, that NIST put forward——

Ms. DEGETTE. So—but basically, what you are saying is tie government grants to good hygiene.

Mr. REINER. Yes, ma'am.

Ms. DEGETTE. Ms. Walden, I wanted to ask you, your testimony cites a Microsoft study which estimates "more than 99 percent of cyber attacks would have been prevented if multifactor authentication were deployed." So do you think that we should mandate basic cyber hygiene requirements through legislation? And if so, which ones?

Ms. WALDEN. Thank you, Chair. Yes, so we published a report that 99 percent of cybersecurity attacks would not have happened without—because of multifactor authentication. So I think that you should encourage basic cyber hygiene principles like multi——

Ms. DEGETTE. Do you think we should mandate it?

Ms. WALDEN. I think I agree that we should require it, yes.

Ms. DEGETTE. OK, thank you.

Ms. WALDEN. Yes.

Ms. DEGETTE. Now, Mr. Lee, in your testimony you seem to agree that additional cybersecurity requirements could be helpful but cautioned that we shouldn't be regulating the "how." Can you explain very briefly what you mean by that?

What do you think the most effective legislative or regulatory requirements would look like?

Mr. LEE. Absolutely, thank you. Generally speaking, we need to be more outcomes-driven. And so a lot of times companies will be told "you must install antivirus," "you must do the patching within seven days," or whatever that kind of prescriptive requirement is. But across our different infrastructure, especially in our operations side of the house, things can be so varied. And we need to tell them what are we actually trying to solve for.

Ms. DEGETTE. OK——

Mr. LEE. "We want you to be able to respond this quickly," or so forth.

Ms. DEGETTE. To be results oriented.

Mr. Carmakal, your testimony cites to a white paper published by Mandiant that outlines the priority technical actions companies should take—ideally, prior to a ransomware event. And I am wondering if you have seen widespread adoption of those recommendations. And if not, what can we do to help companies implement those actions?

Mr. CARMAKAL. Thank you, Chairwoman. So we basically built that white paper as a documentation of the playbook that we use when we conduct incident response exercises. And so these are the types of things that we recommend to organizations after a breach. But certainly, those could be applied beforehand.

Unfortunately, not enough organizations are taking that knowledge and applying it within the organizations. We would love to see greater adoption. Unfortunately, a lot of the things that we see day in, day out, from a response perspective, shows that they——

Ms. DEGETTE. So what can we do to either encourage or mandate them to——

Mr. CARMAKAL. I would certainly love for more encouragement of organizations to try to learn from other breached entities. And that white paper is a good example of those learnings.

I don't know that I would necessarily say that you need to mandate it, but more encouragement——

Ms. DEGETTE. But Mr. Reiner has a good suggestion, though, which is to tie it to government grants. So you need to meet a certain standard if you are going to get your public funding. What do you think of that idea?

Mr. CARMAKAL. Generally, I think that sounds like a good idea.

Ms. DEGETTE. Great. Finally, Dr. Dameff, as a medical doctor and cyber researcher, you have an interesting perspective to share. I am wondering if you can talk if there are specific issues in the healthcare industry, and what this committee—we have jurisdiction over healthcare policy—what we can do to ensure good cyber compliance. Briefly.

Dr. DAMEFF. Thank you, Madam Chair. One of the most important things I can articulate today is the need for additional information. It is very difficult to measure the impacts of a cyber attack on a patient. In other industries you can measure the cost in dol-

lars and cents. That is immediately understandable. Or downtimes resulting in increased gas prices. But in healthcare we do not have the infrastructure in place to get the basic data, to measure what happens to our patients.

And what really matters is whether or not they walk or talk after a stroke, or whether or not they survive after a heart attack. Without measuring those very basic things through things like NIH funding, scientific inquiry, we don't even know the magnitude of the problem or the impact on our patients.

Ms. DEGETTE. Thank you. The Chair now will recognize Ranking Member Griffith for the purposes of asking questions for 5 minutes.

Mr. GRIFFITH. All right, Dr. Dameff, and this is not on my list of questions, but it came up as a part of feeding off of Chairwoman DeGette's questions.

Ms. Walden said, you know, we could have prevented a lot of these hacks with multifactor identification. You are an emergency room doctor. How is that going to work? Because it is easy to say here, but how is it going to work in your emergency room?

Dr. DAMEFF. That is a great, great insight. Thank you for the question. There are technical controls that will definitely improve the cybersecurity posture of hospitals. Those should be employed, right? Many hospitals are deploying multifactor authentication, or already have, for protecting patient data.

You identify a key element here, which is that patient care cannot be hindered in the emergency sense by overly—over-security controls that impact patient care. I will say this, though. It is not necessarily about which controls can prevent the infection. Honestly, I am of the belief that we should prepare for an inevitable attack and then have a backup system in place to restore patient care as quickly as possible, and rely on that until you can restore that. That is how you save lives. That is what you do, is focus on your immediate response to restoring patient care, while those technological systems come back online.

Mr. GRIFFITH. All right. So my next question would be how expensive is that going to be?

And let me give you a reason why I am concerned about this. I represent a large rural district. In a portion of my district the previously competing hospital chains, for financial reasons, were forced to merge, and they were given clearance by both State of Virginia, the Federal Government, and the State of Tennessee to basically have a monopoly in that area. So I have got one hospital system serving many counties in east Tennessee and southwest Virginia. How expensive is it going to be for them, because they are under financial stress already, to set up this good hygiene?

And do they—how are we going to fix that? I mean, how expensive is what you are talking about? Because, in this case, should what happened in San Diego happen there, there are no hospitals to send these folks to that aren't at least an hour to an hour and a half away, maybe further than that for some of the folks. What are we going to do? Help me.

Dr. DAMEFF. Again, thank you for that fantastic question. The consolidation of healthcare, exactly as you mentioned, has increased the risk to patient safety from ransomware attacks because of the shared infrastructure and technology among many hospitals

in a specific geographic location. We have seen that. That is what happened 2 months ago, is that a single healthcare delivery organization that was infected, five hospitals in a geographic location were devastated. That exactly would impact patient care, potentially.

And your identification of critical-access hospitals as being a target, potentially, of attack, as well as the patient harm implications cannot be overstated.

Specifically, how are they going to afford this? Really, two things. One, that disaster resiliency that I mentioned before, restoring technical systems in the background but having a manual, nontechnical process to take care of patients in the meantime, that already exists at most hospitals. That is emergency response. That is disaster medicine. They prepare for earthquakes and hurricanes and have plans in place to do that. They should enact that—or they should prepare for that in a cyber context.

The second thing is that, it is true, it is going to be costly for a lot of the technical controls, and there are hospitals out there that cannot afford it. They will simply not be able to. I worked at hospitals and took care of COVID patients in resource-stricken hospitals, wherein they were concerned they were going to run out of ventilators. How do we expect them to be able to defend against cyber attackers and spend millions of dollars, potentially, to increase their cybersecurity posture?

It is going to require some creative solutions. Quite frankly, I don't see any——

Mr. GRIFFITH. So what you are saying is that is a problem we are going to have to solve.

Dr. DAMEFF. Yes, I think that is going to be a big, big problem you have to solve.

Mr. GRIFFITH. I appreciate that, and I tend to be tight with Federal dollars, but this may be one area we don't have any choice.

Let me say also, for us to provide assistance to an organization, we need to know in advance, or we need to know when it happens, if they are being attacked. And of course, there are many reasons for not telling us. And you and Mr. Carmakal want to—might want to tag-team on this one, if I have time—I am running out.

But particularly related to hospitals, should we be looking at, if not mandating, having a minimum requirement that would then give the hospitals some protection? If they have done their cyber—the good cyber hygiene to a minimal requirement that perhaps the Federal Government sets up or industry sets up, that they would then be limited on liability in any suits that might follow, where a patient's health was affected, do you think that is—that idea would work?

Dr. DAMEFF. I am definitely in support of ways we can incentivize instead of slowly penalize hospitals for trying to take care of patients. That is really key. Perhaps tying it to reimbursement, for example, wherein if you meet a certain cybersecurity threshold of protections, you can see increased reimbursements for some of your medical care as a way to incentivize. I could see that as one potential mechanism where we can achieve even the most rural and critical-access hospitals achieving the appropriate amount of cybersecurity protections.

Mr. GRIFFITH. All right, and if Madam Chair will give me just the patience for a second, Ms. Walden, if you can get to me in writing later, what do we do about cryptocurrencies and its involvement in all of this?

Just—if you can cite me some articles later or whatever, and we will probably send you a written question on that, as well, and I yield back.

Ms. WALDEN. I am happy to.

Ms. DEGETTE. I thank the gentleman. The Chair now recognizes the full committee chairman, Mr. Pallone, for 5 minutes.

Mr. PALLONE. Thank you, Chairwoman DeGette. One of my concerns is that ransomware is a very sophisticated form of attack, and it is not clear to me that smaller companies and, to some extent, even larger companies have the resources or tools needed to deal with these threats. So I was pleased to see the StopRansomware.gov website that was launched by the Biden administration last week, and—because it provides a new resource hub for small businesses and other organizations.

But I mean, that is a good start, but I am wondering if we can and should be doing more to assist U.S. companies, particularly small to medium-sized businesses, to deal with these threats. So let me start with Mr. Carmakal.

Given your experience in incident response, can you explain the types of resources that companies need, once they find themselves in the midst of a ransomware attack?

Mr. CARMAKAL. Yes, absolutely. Unfortunately, a lot of these small organizations, some of them don't even have security staffs. Some of them rely on IT resources to perform security functionality.

When I think back to October of 2020, when we saw an acute problem against healthcare organizations, I talked to a lot of hospitals that were taken offline, couldn't take care of patients leveraging digital technology. They ended up having to divert patients to other hospitals. And I ended up talking to the IT resources, who were trying to desperately get their systems back online. They didn't know anything about digital forensics. They didn't know anything about threat actors. They didn't know how to respond to the intrusions. And so it was a very difficult situation for those organizations to face, and I really do feel for a lot of the smaller organizations that don't have dedicated security teams.

So, look, to the extent possible I want organizations to do the best that they can, from a, you know, cyber hygiene perspective. But I don't believe the onus is fully on the organizations themselves. I think there is a shared responsibility——

Mr. PALLONE. Well, what kind of resources would they need is what I am asking.

Mr. CARMAKAL. Yes, I think they would need—well, I think they would need government support. And, from a government support perspective, I think there are things that government could do in terms of indictments, arrests of individuals that are behind these attacks.

I think there is more information sharing that could occur for victim organizations that could be applicable to other organizations out there.

I think there are, you know, things in terms of disruption that government can do to curb the problem of ransomware, so that these smaller organizations that don't have the resources and the staff have some additional government support.

Mr. PALLONE. But I guess—and let me go to Mr. Reiner. I know that there's, you know, law enforcement agencies that assist, and a lot of what Mr. Carmakal mentioned relates to that. But are we providing—are there a variety of resources beyond just, you know, the traditional—or some of the law enforcement, you know, such as technical expertise that the government can or should be providing, or can the government provide help in assessing the scope of their situation?

I know he discussed some of that, but if you would respond also, Mr. Reiner.

Mr. REINER. Yes, Mr. Chairman. I think, through the process that we conducted for the Ransomware Task Force, I mean, there was an array—really, a list of things that we put forward that we believe could be done to get ahead of this, right? So to get to the left of boom, so that you better equip companies to be able to defend themselves.

As has been discussed, though, a lot of those organizations really don't have the capability to do so. So CISA and other departments and agencies, I believe, can be very well positioned to help share that information, provide those tools in advance for free. But folks don't know about it. They are not even aware that it exists. So how do you get it to them?

Awareness campaigns are often belittled as not effective enough and not quick, but there needs—there can be a lot more to get the information out there that there are tools that are available. StopRansomware.gov, for example: great idea, fantastic amalgamation of government resources. How do you tell people that that is something that they can turn to and utilize?

I think there is one piece here that is incredibly important that came up over and over again through the process that we conducted, which was that departments and agencies that are responsible for doing this don't have the resources that they need in order to develop those tools to engage those private-sector partners to actually get that word out. NIST, DHS, other departments—Commerce, other departments and agencies really could use buttressing of resources, so that the folks who are really specifically responsible for that training and that piece of it have more capacity to do so.

Mr. PALLONE. OK. Just quickly, Ms. Walden, when you talk about cybersecurity—I mean cryptocurrency, I am sorry—again, I don't think the small business owner knows much about how to purchase or trade that. So how do you see—in other words, if a small business is faced with having to pay ransom, for example, in cryptocurrency, how likely is it they are going to be able to navigate that? And what resources would they need?

There's only 20 seconds left, but if you could just comment.

Ms. WALDEN. Well, first, hopefully, small business would opt not to pay the ransom.

Mr. PALLONE. Right.

Ms. WALDEN. But if they chose to pay the ransom, the criminal actors are actually quite helpful. They have a bit of customer serv-

ice. Their ransomware notes will instruct the victim on how to or where to obtain, usually, Bitcoin, because Bitcoin is a lot easier to obtain than other types of cryptocurrency. But there are avenues for small businesses to be able to obtain cryptocurrency.

Mr. PALLONE. Your recommendation is don't pay, though, sure.

Ms. WALDEN. But my recommendation is do not pay.

[Laughter.]

Mr. PALLONE. Right, thanks a lot. Take care.

Ms. DEGETTE. I thank the gentleman. The Chair now recognizes Mr. Burgess for 5 minutes.

Mr. BURGESS. I thank the Chair, and I thank our panel for being here today.

It is, obviously, not the first hearing we have had on this. It is a little remarkable to me that we don't have law enforcement as part of the panel, however. It has come up in previous panel discussions that law enforcement can only go after people that they know they need to go after. And it has also come up in the past that there are disincentives to report.

Dr. Dameff, you have kind of mentioned that it could be—the reputational damage can be significant from your hospital or hospital network.

In the past I have wondered if the construction of the Office of Civil Rights, the data breach reporting that was created as part of the HITECH Act back in 2009, if this is a disincentive to reporting. Once a company becomes listed, or once a healthcare entity becomes listed on that, it is—they are, essentially, archived forever. And I have wondered if we should have a statute of limitations, or a statute of repose or some remedial actions that can be taken by an organization that would allow them to extricate themselves from that list. Is that something that has come up in any of your discussions? For anyone on the panel.

Dr. Dameff, I will just ask you specifically, since you work in a hospital.

Dr. DAMEFF. Thank you. The question of whether or not reporting record breaches—as part of their mandatory reporting, whether or not that inhibits potential reporting of ransomware impacts, I think is still unknown. I will say, anecdotally speaking, I could see how that would prevent individual organizations from wishing to report or perhaps delay the impact of the reporting until they are—to anticipate what might potentially be a large punitive fine.

There also—when a hospital is hit with ransomware, they are also trying to restore operational capacity to take care of patients.

Mr. BURGESS. Yes.

Dr. DAMEFF. And there are so many competing things happening at that exact moment, it is difficult to then report.

Mr. BURGESS. Let me ask you about that, because you brought that up. And we have spent a lot of time in this subcommittee and other subcommittees talking during the pandemic about the Strategic National Stockpile. Of course, the creation of the Strategic National Stockpile was in an emergent situation. You could deliver a set of things to an institution that they would need to function in whatever the emergency—earthquake, hurricane, flood.

So is it possible to have an urgent deliverable of what you would need to run your—say, your emergency room at your hospital, if

you were just completely shut down with a ransomware attack? Is that something that we should look at?

Dr. DAMEFF. I definitely agree it is something we should look into.

One of my recommendations is coming up with metrics to measure the impact to a hospital. And hospitals that have severe attacks that would be devastating to patient care might benefit from such a resource, akin to something like the FEMA DMAT response, in which——

Mr. BURGESS. Right.

Dr. DAMEFF [continuing]. Outside resources, personnel, systems, tents, et cetera, could be deployed rapidly to help alleviate those patient care constraints, while they are restoring systems. It is definitely something that should be looked into. We have never seen anything like that before.

Mr. BURGESS. So at this point we don't even know—if there is a major hospital system that gets attacked, we don't know, downstream, is there a loss of life, was there—as you pointed out, during the course of treatment of a stroke, is there a loss of function that could have been preserved? We just don't know the answer to those questions, do we?

Dr. DAMEFF. And that is why I recommend in my testimony here that there be mandatory reporting for severe attacks on patient safety implications.

One of the barriers to that is that systems in which we measure care quality and patient safety are themselves targets of the ransomware.

What do I mean? The way that we measure the quality about a stroke care or a heart attack or something else is measured and recorded in the electronic health record. The electronic health record is ransomed.

Mr. BURGESS. Yes.

Dr. DAMEFF. So we don't even have tools to measure that, because they are also collateral damage from the actual attack.

Mr. BURGESS. Let me ask you this. And, you know, in order to get the proper metrics, in order to get the proper—be able—for us to make proper decisions, you are going to have to get proper information. It is hard to get proper information if people are scared to report.

You and I—I am a physician, also—we live in the world of the National Practitioner Data Bank, right? There is a central location that a hospital credentialing committee can query as to whether or not we have had a problem in other cities and we are just taking our problems from town to town. Do you think there would be a benefit from having something structured along the lines of a National Practitioner Data Bank for data breaches, for ransomware attacks?

Dr. DAMEFF. Forgive me, for individual physicians or for healthcare delivery organizations?

Mr. BURGESS. For the healthcare organization writ large.

Dr. DAMEFF. I do believe that we should get visibility on the differences in organizations that are under attack. But to penalize them, or to fine them significantly would reduce their ability to bounce back from that attack, deliver care. And so, whether or not

it should be like a National Provider Data Base but for healthcare ransomware attacks, I would support any efforts that collect additional metrics on ransomware attacks and to make that data transparent and public.

Mr. BURGESS. Yes, the difficulty there is, though, when we get—then you drive—you are driving a fear factor: I don't want to report, because I don't want to be included.

Ms. DEGETTE. The gentleman's time has expired. The Chair now recognizes——

Mr. BURGESS. I am going to send you some questions in writing on that, as well as other members of the panel.

I appreciate you——

Ms. DEGETTE. The Chair now recognizes Ms. Kuster for 5 minutes.

Ms. KUSTER. Thank you very much, Chair DeGette. I appreciate you holding this hearing today.

Today's discussion regarding ransomware attacks and the growing threats that they pose presents a unique opportunity for this subcommittee to identify existing vulnerabilities and gather information on actions Congress can take to respond to this emerging threat.

As we have heard today, ransomware attacks are not new, but they are certainly increasing in number and sophistication in recent years. We continue to see front-page news reports on this attack, but it is not just the high-profile ones that are occurring. The implications of these attacks have a far-reaching effect beyond the companies that are being targeted.

The attack on Colonial Pipeline's information technology system a few months ago had a significant disruption in energy distribution on the entire East Coast that led to delivery delays for businesses, and gas stations closed for over millions of Americans. This is just one example of why we need to explore what makes these companies vulnerable to begin with, and what they can do about it.

Ms. Walden, you state your testimony that "applying basic cybersecurity hygiene can prevent a cyber criminal's ability to ransom a system." For the benefit of the business owners who may be watching this hearing, Ms. Walden, what are the most common vulnerabilities that put companies at risk of a ransomware attack?

Ms. WALDEN. Thank you for the question. Yes, that is true. You—the best way to resolve a ransomware is to make sure that it can't get into the system in the first place.

So there are some simple things that are just true for preventing cyber attacks in general: enabling multifactor authentication; doing better training of your employees and staff on identifying phishing and preventing the click; segmenting your network—and those are tools for CISOs to take, but segmenting your network so that cyber criminals, once they are in, can't laterally move. But these are some of the simple cyber hygiene activities that small and medium businesses can and should take to prevent ransomware or any other cyber criminal attack.

Ms. KUSTER. Thank you. And I know, as Members of Congress, we are learning to do our best in that regard, as well.

It is clear that companies need to be giving increased attention to cybersecurity. But the amount of threats and vulnerabilities can be overwhelming. Mr. Carmakal, if you were running a medium-sized company, what are two or three things that you would do right away, across the board to protect your systems and data?

Mr. CARMAKAL. Yes, thank you, ma'am. Great question. There's a few things I would do.

Number one, to the best of my ability, I would try to enable multifactor authentication on all remote access into my organization.

Number two, I would try to educate my employees as best as they can to identify phishing emails. But I do need to recognize that employees will always fall victim to phishing emails at some point in time, so I need to provide technology to block as many of those malicious emails as possible, and also provide technology and processes so that, if something does get past the initial security system, we have got other checks and balances to be able to identify the attack as it occurs.

The third thing I would do is try to, to the best of my ability, install all the security patches that I can and that I know about across my environment.

Ms. KUSTER. Very helpful, thank you.

I note that some cybersecurity measures are very expensive, especially if they involve reconfiguring entire networks, but the cost of these attacks is also increasing. Mr. Reiner, is it fair to say that investments in cybersecurity are good returns on investment?

And what more can be done to incentivize companies to make these changes or spread the word about the necessity of addressing vulnerabilities?

Mr. REINER. You know—thank you for the question. As we have spoken about extensively as part of the Ransomware Task Force, is that—investing in this up front is much more affordable than having to, as you describe, having to reconstitute your entire organization after an attack. So absolutely, putting the investment up front in order to stay left of boom and make sure that these are not attacks that can actually get into your system, is absolutely where folks should be putting their resources.

I think the thing that can be reverted back to a little bit is what we were talking about before, which is getting the information out to those folks who don't really have the resources. One of the things that we delved into was in this spectrum of organizations there are companies that know, that have resources, but choose not to invest. How do you help inform their decision making, so that they choose to do so? You incentivize them through some of the steps that we have spoken about here today, tying grant making, relieving penalties if they are compliant, et cetera.

I think there are organizations out there, though, that simply do not know that this is happening, and they do not have the resources in order to prepare in advance. We have to do better, I think, in terms of getting to them and letting them know what it is that they can be doing better.

Everything that was just described—multifactor authentication, et cetera—those are simple things that folks can be considering. We need to get that information to them——

Ms. KUSTER. Sorry to cut you off——

Ms. DEGETTE. The gentlelady——

Ms. KUSTER. I need to yield back. Thank you.

Ms. DEGETTE. The Chair now recognizes Mrs. Rodgers for 5 minutes.

Mrs. RODGERS. Thank you, Madam Chair.

Earlier this year Scripps Health was hit with a ransomware attack. In the attack, the cyber criminals stole data on about 150,000 patients and caused significant disruptions in operations. A family member of mine—or a family member of, really, a constituent of mine—was directly affected by this attack, and so I have heard firsthand how devastating it was and the impact on their health. The Scripps attack is a stark reminder of the stakes of cybersecurity. When the hospitals are hit, it can literally be life or death.

Mr. Dameff, these attacks can have a direct impact on patient health and outcomes. Can you help us better understand the cyber threat hospitals face today, and provide a few examples of situations where a patient's health was negatively impacted by a cybersecurity or ransomware attack?

Dr. DAMEFF. Thank you. It is true that, in some medical conditions, minutes matter. For example, we have sometimes minutes to hours to treat a stroke, wherein our medications and our treatments will no longer benefit that patient after a certain amount of time. The same is true for things like certain heart attacks. And our ability to diagnose a patient is tied to the technology that we use every day, as clinicians, that technology we are so dependent on.

So you can imagine, during a large ransomware attack, wherein these technical systems are no longer available, that we can't do our jobs as clinicians. I jokingly say I am the generation of doctors that has never used paper records. Until early on in my fellowship training, I had never had written a prescription.

The future of healthcare is not going back to the days of antiquated systems. In the future, we are only more technologically tied to our systems that we use. That—when it is not there, we can't do our jobs well enough. It takes longer to get test results, to make decisions to give things like antibiotics in severe infections, or to identify when patients have certain conditions.

So you can imagine at that—at a scale of not just one or two patients, but of a—you know, 5 or 6 or 10 hospitals down at once, where you could imagine that would impact care along the continuum, not just patients in the emergency department, patients in clinics, patients in the ICU, patients that are in ambulances that have to be transported longer distances because hospitals under attack are on diversion. These are all examples of how patients could potentially be impacted by this.

I will say, though, we do not have the ability to measure that impact. As mentioned previously, the systems in which we measure care quality and patient safety themselves are digital, are affected by the ransomware attacks. So I fear we don't even have the tools now to answer that basic question.

Furthermore, I would say that these types of attacks are exceptionally chaotic, and there's a lot of things happening at once. The

ability for hospitals to report on that type of thing is nearly impossible as they attempt to restore their systems.

Mrs. RODGERS. OK. As a followup, you have expertise in the field of medicine and cybersecurity. In your opinion, what steps should hospitals take to better secure their networks against cyber attacks?

Dr. DAMEFF. I think it is shared among many of the panel, the same types of technical controls: multifactor authentication, focusing on rigorous backup, and restorations. But there is—my number-one recommendation would be to prepare for an inevitable ransomware attack, to practice and prepare for taking care of patients without systems, and to be able to do that at—within 2 or 3 hours of an attack.

There are a lot of hospitals in this country that have not considered this type of attack on their systems, have not prepared adequately for it, have not put in place how to take care of 1,000 patients without technology. That is the number-one thing I would encourage most hospitals across the country to do now. There is a framework for that at every hospital. And that type of preparation, at least in its beginning, doesn't cost a dime.

Mrs. RODGERS. Thank you.

Ms. Walden, what are the ways the private sector can partner with government to address ransomware attacks?

Ms. WALDEN. Thank you for that question. The government has legal authorities that the private sector doesn't have, right? They have law enforcement authorities, they have intelligence authorities. The private sector, frankly, has a lot of signals. But if you match those things together, we can do coordinated actions to bring cyber criminals to justice.

So law enforcement can bring the criminal to justice. Private sector can work along with law enforcement to identify those criminals. But we can also work with law enforcement to tear down the infrastructure that they use.

Mrs. RODGERS. So what do you believe we need to be doing, as far as coordinating between the two, then?

Ms. WALDEN. I believe that we need—and I know I keep saying it over and over again, but we need actionable information sharing. I like to be able to exchange ideas and signals and technology with my government partners to be able to get at the problem together.

Mrs. RODGERS. So how are we doing?

Ms. WALDEN. From the digital crimes perspective, we have great relationships with all of U.S. law enforcement, but we also have great relationships with other countries and their law enforcement. I think this administration is taking the—cyber crime and cybersecurity seriously, and they are signaling the right things, the right messages to would-be cyber criminals and cyber criminals across the globe. And I think working with our allies is working pretty well. There is still a lot to do, but I think we have taken the best first step that we can.

Mrs. RODGERS. OK, thank you. I yield back.

Ms. DEGETTE. I thank the gentlelady. The Chair now recognizes Miss Rice for 5 minutes.

Miss RICE. Thank you, Madam Chair.

Mr. Carmakal, can you speak more about ransom payments, and how we should be treating them?

And, you know, you talked a little bit about what the motivation is to pay them or not to pay them. Can you just expand on that a little bit?

Mr. CARMAKAL. Yes, absolutely. Thank you for the question, ma'am.

So, look, most organizations, they don't want to pay an extortion demand. They just feel that they have no other option. And, you know, for whatever reason, you know, maybe they feel like they need to accelerate the process of being able to recover their business operations, or perhaps they feel like they are doing the right thing to minimize the impact to their customers, or to their partners, or to maybe the intellectual property that they have, where they don't want that information to be published on the internet for anybody to be able to download.

And so, you know, I have had an evolving position on ransom payments. Many years ago I was in the camp of, absolutely, you never want to pay an extortion demand, because we all grew up learning that, and we all grew up understanding you don't pay criminals, you——

Miss RICE. Yes.

Mr. CARMAKAL [continuing]. Don't give in to terrorist demands.

But what I have learned is, over the years, many of my clients, against my recommendations, made payments and they actually saw relatively positive outcomes. They got access to their data, or perhaps they paid because they didn't want that information that was stolen to get published on the internet.

And so I recognize that there are certain situations in which a company may choose to pay, and they might get some temporary benefit out of it. It is not necessarily going to be a long-term benefit. So the temporary benefit may be companies get access to their systems and data through the decryption tools that are provided by the threat actors. The potential long-term benefit is that the data that was stolen may never end up being published on the internet.

But again, there's no guarantees that things won't show up down the road. And I do anticipate, over time, we will start to see threat actors that have been paid will end up publishing the data at some point down the road. And that was a pretty common thing, prior to 2019, for us to observe.

Miss RICE. Mr. Reiner, that kind of brings me to one of the issues that you have raised, which is the need to understand and regulate cryptocurrency. Can you talk more about what we can do here, as a body, in that area?

Mr. REINER. Thank you for the question. It was a pillar of the conversations that we engaged in, as part of the of the Ransomware Task Force. This is a major facilitating element of what really has accelerated what we are dealing with, in terms of the ransomware threat today.

The—from my perspective—and it really has been a learning experience for me to better understand specifically what are the choke points when it comes to cryptocurrency, the ecosystem. Where exactly can we focus our efforts to try and make it so that criminals cannot abuse these systems?

These are incredibly innovative capabilities. I think that is a separate conversation.

What can we actually do, though? We can work much more closely with the community that understands these systems and how they work, and get into the weeds as to how they are being abused. I do not think that that is very clearly and well understood broadly within government, but also in the private sector. And I think that would afford a great deal of opportunities, if we have that sort of information exchange and transparency, and understand it. You will see more clearly where it is that we can do more to stop criminal abuse of those payment systems. It is an incredibly complex web, because so much of it is really outside of jurisdictions.

So there is this notion that we came up—or that was often noted in the process, this jurisdictional arbitrage. The United States is not alone in this effort. We have partners internationally that we can work very closely with, who have the ability to do things that we can't.

Miss RICE. Well, who is doing it right?

And, I mean, I think you mentioned that the—for Federal agencies that have jurisdiction over this issue——

Mr. REINER. Yes.

Miss RICE. Is it a resource issue? Is it an intellectual capacity issue? Are we not able to hire the best and the brightest? What—where is the deficit?

Mr. REINER. I would argue, from the—so from where I sit, we see a wide variety of technologies that disrupt various elements of our society. This is a technological ecosystem that is very disruptive and it is incredibly innovative, and we are just behind the curve. We haven't—really quite yet understood what it—how it works, and how to get ahead of that, from a policy perspective. I think the policy is really playing catchup here.

There are folks, I think, who are out there that can be relied upon, as Ms. Walden noted earlier, who are interested in playing a role to make sure that they are—they don't want their systems being abused. They want to be seen as legitimate, and they are willing to engage in these conversations. It is a conversation that we need to engender, though.

To your question of who is doing it well, I think there is a lot of work that still needs to be done. Internationally, I don't know that there really is one that I would point to that is really doing it well yet. I think there is a lot of growth that we need to see happen there. But we can help lead on that effort, from the United States.

Miss RICE. Thank you very much.

Ms. DEGETTE. I thank the gentlelady. The Chair now recognizes Mr. McKinley for 5 minutes.

Mr. MCKINLEY. Thank you, Chairwoman DeGette. Thank you for the panel.

I am a little frustrated that you all have put together a lot of efforts to try to help out and guide us, but even Johnny Wooden used to say there is some confusion over efforts versus accomplishments. And I am frustrated over the lack of accomplishments, because our U.S. laws on cyber crime were originated in 1987. And then our last international cyber agreement originated in 2001. So cyber

criminals are exploiting these outdated laws, clearly, and they are targeting our critical infrastructure, as we have all talked about here, so far with it.

And it is not just in America. Just in the last 2 years, we have seen a 500 percent increase in ransomware attacks and a 300 percent increase in the amount of money that is being exchanged with this.

So I looked back on the history of it since we have been chatting about this, these efforts. In the Ukraine, Russia attacked Ukraine in 2015 and 2016 and tried to destabilize their country. The Mexican oil company has been attacked, Pemex, by ransomware. The oil fields in Saudi Arabia were hacked by Iran in a retaliatory move. And then earlier this year, the water system in Florida was attacked. So—and then what you have heard also is the Colonial Pipeline. It was held for a ransom payment. And we understand, as was noted earlier, it provides oil for half the East Coast in this. And we saw the consequences. We saw increased prices and shortages with it.

Yet these attacks on our critical infrastructure certainly, I think, could be mitigated with updated reforms to our international treaty, including some stiff, enforceable penalties. But—and also—and I believe it was you, Mr. Carmakal, was talking about cryptocurrency, understanding and getting control over cryptocurrency.

But—so what I am saying to you, as an alternative, while you all work your magic and efforts, what about an accomplishment—if we could develop a redundancy in our energy system, a backup system?

For example, earlier this year Texas suffered massive outages after an electric generation failure. It could have been avoided if they had had the ability to go backup, to connect to their neighboring States, to get electricity. This lack of redundancy in their electric grid has served as a—to me, a stark reminder as an alternative to avoiding problems like this.

So—but President Biden and his people on the left, unfortunately, seem to be continuing to block this optional exchange of building additional pipelines as a redundant system. In this report that was just printed back in May, it talks about how this environmental council is not recommending any creation, maintenance, or expansion of pipelines in America. That is going to make us more vulnerable, to where hackers can get into our system.

We look at the Keystone pipeline, Line 5 in Michigan; Williams Pipeline in New York; the Atlantic coastline, the Mountain Valley Pipeline, all in West Virginia, all were part of our critical national security, are under attack or have been canceled with it.

So even Tom Seagal, in 2015, came before our committee, and he said that he could hand pick 10 engineers at Berkeley, and those 10 engineers, within just a matter of a few days, could shut down—4 days, he said—in 4 days could develop a system to shut down our electric grid between Boston and New York. That was testimony for our office. So we know these hacks are going to occur.

But what we need—what I am looking for is, how do we develop—while the magic is developing, how do we deal with it?

What are—how do we develop redundancy on this?

So my question to all of you is would a reliable firewall—while a firewall was being developed, or your systems being developed, would you support development of a redundant energy system for additional pipelines, so that if we do get hacked, we can go around it to—and we—I think it would lessen the attractiveness of attacking our pipelines if we could do a redundant backup system. Would you support that, any of you?

I will start with you—I want to call you "Dammit," but I know that is not right.

Dr. DAMEFF. I would support any efforts to increase healthcare resiliency in the face of cyber attack, broadly. It is quite difficult to build redundant hospitals, for example. But there are——

Mr. MCKINLEY. I am talking about energy. I am primarily talking about energy. I will let the other people on this committee to deal with some of the other matters. But I think on energy, I think, our national security is at risk.

I have run out of time, so I yield back. Thank you.

Ms. DEGETTE. I thank the gentleman. The Chair now recognizes Ms. Schakowsky for 5 minutes.

Ms. SCHAKOWSKY. So this has been pretty frustrating, actually, and I hear remarks like we are playing catchup, that it is—the cyber criminals are getting more and more sophisticated, and it does feel like we are—we have a lot of catching up to do.

And I also heard that there is no one, internationally, that is necessarily doing better than we are.

As a part of a legislative body—and I do believe that Chairman DeGette did ask the question—are there things that come to mind now, where we, as a legislative body—for example, I chair a subcommittee of the Energy and Commerce Committee that deals with consumer protection, and I am wondering if we should be thinking about or getting your advice on legislation that might address the problem that we are facing.

I understand that it is totally multifaceted, that the executive branch has a huge role to play here, that it is beginning to do more of that. But can you advise us on the kinds of things that we could play?

I—really, anybody can jump in. You are looking, you know, ready to go.

Mr. CARMAKAL. I would love to take your question, ma'am.

Ms. SCHAKOWSKY. Mr. Carmakal? OK.

Mr. CARMAKAL. So, first of all, look, I am equally frustrated about the problem. Every week it is exhausting for incident responders to have to deal with highly disruptive attacks against organizations. And it feels like every week it gets worse and worse.

But I do want to take a moment to celebrate the wins, because there has been a lot of wins out there, and I don't think we always celebrate that, or we don't celebrate it enough.

Number one, I think organizations are defending themselves against attacks every single day. We may not talk about that publicly, but it happens a lot.

Number two, I would like to——

Ms. SCHAKOWSKY. Let me just ask. Do you think there should be any requirements for building in these security systems?

Mr. CARMAKAL. I think there is a general expectation for most organizations to have cybersecurity controls and resiliency in place. Whether that is enforced by law or there is—generally expected by customers, I think that does exist.

Ms. SCHAKOWSKY. Go ahead.

Mr. CARMAKAL. Beyond that, I think there's a number of wins. If you look at some of the things that government has been able to do over the past few weeks and months—and I am pretty proud and excited that the Bureau was able to recover some of the funds that were paid by Colonial Pipeline to the threat actors. That was a pretty big win. And it is exciting to be able to see some of those actions taking place.

It is pretty exciting to see some of the disruption to threat actor botnets like TrickBot and Emotet, and some of the more nefarious botnets that are operating out there, and that is a good example of public-private collaboration and coordination.

Ms. SCHAKOWSKY. Well, I——

Mr. CARMAKAL. Just this week——

Ms. SCHAKOWSKY. I want to just interrupt for a second.

Mr. CARMAKAL. Yes.

Ms. SCHAKOWSKY. And then where does responsibility mainly lie?

Should the Federal Government be required, then, to step in if there has been a failure in security that should have been considered by the—either the private sector, or——

Mr. CARMAKAL. I think there is a shared responsibility from victim organizations, from security companies, from government. I don't think any one party can handle the problem on their own. It is going to require a concerted effort from multiple different parties, and I think we all need to step up, and we all need to celebrate the wins, and we need to actually continue to emphasize effort on the wins, on the things that have been happening successfully.

And I look at things that the FBI is doing in terms of notifying victim organizations about upcoming intrusions. It is incredibly powerful when that happens, when somebody from the FBI calls a victim organization and says, "There is a threat actor in your network today, and if you don't do something about it in the next 3 days, they are going to take your business offline." A lot of times that victim organization actually has the ability to call in for help and to disrupt the threat actors and eradicate them from the environment.

So when we see actions like that from the government, I mean, it is incredible. You look at what happened earlier this week, or yesterday, with the indictments of a number of, you know, Chinese individuals that conducted intrusions over the past several years. Those indictments are good steps. They are good tools in the government's capability to try to curb the problem. So we would love to see much more of that happening.

Ms. SCHAKOWSKY. Thank you.

Ms. Walden, you said don't pay, that—so what is the alternative to that?

Ms. WALDEN. Well, I think there are a few things that can take place and that Congress can do in order to prepare the country and to raise the maturity level of potential victims, and one is to create

a recovery fund of some sort so that victims aren't alone in absorbing——

Ms. SCHAKOWSKY. Could you turn on your microphone?

Ms. WALDEN. Sorry, is that better?

Ms. SCHAKOWSKY. Yes.

Ms. WALDEN. Ah, sorry about that. A couple of things that Congress can do to make sure that victims are at a maturity level to be able to not pay, right?

So one of those things, for example, is raising the baseline for cyber hygiene, bringing everybody to a cybersecurity maturity level that can handle it.

Another would be to develop a cost recovery fund that will allow—that will help victims absorb—and the country, really—to absorb the cost of critical infrastructure for having down operations.

On the cryptocurrency piece, if I may, it is helpful to know which department or agency has authority over the crypto economy, whether it is—and the investors, right? Whether it is the SEC or the CFTC, that is a great start.

So I also want to make a shameless plug for the Ransomware Task Force report. I think there are about a dozen or so potential legislative actions recommended in there.

Ms. SCHAKOWSKY. Well, why don't—I would like——

Ms. DEGETTE. I am sorry——

Ms. SCHAKOWSKY [continuing]. To see those.

Ms. DEGETTE [continuing]. The gentlelady's——

Ms. SCHAKOWSKY. And I yield back, I am sorry. Thank you.

Ms. DEGETTE. That is OK. The Chair now recognizes Mr. Dunn for 5 minutes.

Mr. DUNN. Thank you very much, Madam Chair, and thank our panel.

You know, recent ransomware and other cyber attacks have highlighted our vulnerabilities, showing the difficulties in holding those who perpetrate these attacks accountable. And it should not escape any of us that the vast majority of these significant cyber attacks originate from within countries that just happen to be our greatest foreign adversaries: Russia and China. It is my belief that the best defense is a good offense, and that goes for ransomware, as well. You know, we have to put Russia and China on notice that they will be held accountable for these organizations operating freely in their company.

So, you know, I think back to the 2014 OPM hack. It put millions of Americans' records at risk, tens of millions. This was something, you know, that Congress and the American Government simply has to address.

With that, Dr. Dameff, there has been a significant uptick in ransomware attacks on healthcare organizations, certainly since 2016. Now, I was amused when you said you had never written a note in a chart, you had always—EMRs. You know, I actually go back to the days when we had a lot of paper, and we got a lot of work done. So I would say, while technology—and, you know, it certainly has made huge, you know, advantages in medicine—I am concerned that we are not ready for cyber attacks. Is there a single

vulnerability that you would point to that makes us—that is worse than any of our other vulnerabilities in healthcare?

Dr. DAMEFF. Thank you so much for that question. If I could point to a single one, it is at the heart of what you mentioned, which was this hyper connectivity that was accelerated over the last 11 or so years by meaningful use. The thought we would digitize healthcare rapidly to improve care——

Mr. DUNN. Everything is connected to everything.

Dr. DAMEFF. Yes, and I think the commensurate security required for that did not happen, and did not occur. And so we are in a position now where we have a very difficult sector, generally a soft target for cyber attacks and ransomware.

And then on top of that we have a lot of demands, especially over the last year. The COVID pandemic has spread thin many healthcare delivery organizations across this country and across the world. And as a consequence they are left juggling many different constraints, of which only cybersecurity is one of them.

Mr. DUNN. Yes, and I would daresay that we are not paying as much attention to cybersecurity as we were before the pandemic. Everybody is a little tired, I appreciate that.

In the interest of time, I am going to switch gears a bit here. You know, the U.S. Government confirmed just yesterday a mass ransomware attack on Microsoft earlier this year was done at the direction of the Chinese Government. However, even before this acknowledgment, anyone would be naive to believe that these recent ransomware attacks and cyber attacks are truly perpetuated by rogue criminal organizations within authoritarian China and Russia with no connection to or tacit permission from these authoritarian governments.

So, Ms. Walden, Microsoft Research Asia, MSRA, located in Beijing, notes on their website, "Technologies from MSRA have had a large influence within Microsoft and around the world, and new technologies are constantly born from MSRA. MSRA has achieved breakthrough results in many areas of basic applied computer research, and these results are transferred into Microsoft products."

Many experts, regulators around the world, have come to, I believe, the rightful conclusion there is no such thing as a private company in China, that virtually everything that happens in that country happens with at least the—if not the direction of the Communist Party.

Do you believe that the fact that you are making these products in China makes them more or less vulnerable, more or less—or makes us more or less vulnerable?

Yes, or—I mean, are we safer because of that? I don't think so.

Ms. WALDEN. Well, thank you for the question. As you pointed out, there are challenges for doing business in China. And we—right? And we operate on an a zero-trust basis, and we operate with our values. We don't——

Mr. DUNN. They can compel the——

Ms. WALDEN. Right.

Mr. DUNN [continuing]. Your information. I mean——

Ms. WALDEN. We don't store—we store no data, no U.S. data, in China. And we operate on the principle of zero trust and secure that data.

Mr. DUNN. But the code is also yours, right, and theirs. The codes you write, the software code you write, it is theirs as well as yours.

Ms. WALDEN. For Chinese products and services. But I will tell you this. From an investigation point of view—and I am in the Digital Crimes Unit—we go after cyber criminals and their infrastructure wherever they may be, and that will include China or Russia or other unfriendly jurisdictions.

Mr. DUNN. So, I—we are—run out of time, but I would say, I just—like most of us, I think, we are nervous about the fact that you are working so closely with the Chinese Government in China.

I liked your comment on the cryptocurrency, by the way, and it looks more like a security than a currency.

With that I yield——

Ms. DEGETTE. The gentleman's time has expired. The Chair now recognizes Mr. Tonko for 5 minutes.

Mr. TONKO. Thank you, Chair DeGette, and thank you for the hearing.

Our government has an important role in ensuring the Nation's cybersecurity, especially related to critical infrastructure. I am sorry to say that high-profile government entities have also been victims of ransomware attacks themselves. In my district alone, the Albany airport, local 911 systems, police departments, and the Albany City Government have all been among those who have been attacked. So, with many government agencies involved both as targets and as protective actors, I would like to try to get clarity from our witnesses today on just how the government can be better positioned to address this threat and help respond.

So, Mr. Lee, can you first give us a sense of how it works now?

When a critical infrastructure company is attacked with ransomware and they seek assistance from the Federal Government, who do they call? Which agencies get involved?

And most importantly, what services does the government actually provide?

Mr. LEE. Thank you. I think that the candid answer would be that there is a lot of confusion on who to call and how to actually organize that. And each government agency is most certainly helpful: CISA, FBI, DoD, so forth. They try to help out. But the expectation on the power company, energy company, and so forth, is that they have to talk to all of them. And there is a lot of confusion on what is actually going to come back as value.

So, while there are good relationships, I think, ultimately, government would do better to be able to communicate with one face, also be able to handle .gov and the State and local agencies, as well, where there are a lot of cybersecurity issues, and then show the private sector what is working versus trying to go advocate for services and things to do that they may them not—they may themselves not be taking full advantage of.

Mr. TONKO. So who should be that go-to, which face in government?

Mr. LEE. I don't think most companies really care, but in my opinion it would be CISA. CISA is well established, as a civilian agency, to be the front door to government. That doesn't necessarily mean they are the ones that are going to do all the work, but to

be the coordinator of the interagency process would be much more efficient.

Mr. TONKO. Thank you.

And Ms. Walden, you spent nearly a decade working on cybersecurity and other national security issues at the Department of Homeland Security. I heard your interaction with a couple of my colleagues on the subcommittee here. But as we consider solutions, are there more services that the government could provide that are currently either in short supply or not being provided at all?

I heard you encouraging us to provide that full complement, but are there—those in short supply or not being done at all?

Ms. WALDEN. I think—and I agree with Mr. Lee here—that there are services that the government can provide for free, frankly.

I think what is in short supply are the resources, are the workforce, the persons that are able to provide the technical assistance that CISA is authorized to give to private-sector, non-Federal, and Federal entities. There is just a shortage of incident responders, of pen testers, of technical staff that are able to address these issues.

But in terms of authority, legal authority, I think they are—they exist across the government. I think it is our—it is the government's job now to really use the full weight of those authorities that they have.

Mr. TONKO. Thank you. And while it may sound reasonable to have one agency in charge, one concern is that each industry or sector has very specific circumstances and needs. One agency cannot be expected to understand perhaps all the complications of a ransomware attack against a power plant versus a hospital, for example. That is why we have sector-specific agencies to coordinate cyber info sharing with their industry and act as industry partners. Over the years, however, there have been some challenges about how such agencies coordinate with DHS.

So, Mr. Reiner, what improvements can be made regarding coordination between DHS, sector-specific agencies, and the private sector to address the ransomware threats?

Mr. REINER. Mr. Tonko, I think one of the things that we have been most emphatic about, coming out of the Ransomware Task Force effort, is that there may well be—and I think Charles spoke to this earlier—there are efforts that are underway that are, actually, pretty phenomenal. There are folks and departments and agencies and companies and individuals that are out there that are fighting this every day, who are actually doing an incredible job. And we really need to commend them. But they need help.

And one of the things that I think that Rob was alluding to is that having an interagency coordinated effort, where you have that one door to turn to when you need that help, would be immensely helpful. Our argument coming out of the task force is that really needs to be coordinated by the White House. The National Security Council really is in a unique position in order to coordinate all elements of national power in a way that, really, nobody else can.

You can look at elements like the NCIJTF. You can look at the JCPO that has just been stood up in DHS. Those may be helpful in this regard, in terms of coordinating interagency assets. But really, at the end of the day, from our assertion, it has got to be out of the White House.

Mr. TONKO. Thank you very much.

And Mr. Lee, I would ask that you could also respond. I am out of time, but perhaps get word to the subcommittee.

Thank you.

Ms. DEGETTE. I thank the gentleman. The Chair now recognizes Mr. Palmer for 5 minutes.

Mr. PALMER. Thank you, Madam Chairman. I want to take this a little different direction.

We have talked a little bit about law enforcement, but on June 14th the heads of state with NATO—the NATO-allied countries met, and they issued a communique from Brussels and addressed the issue of the increasingly complex security environment that all these nations are dealing with. And they made this statement—they issued 79 statements—number 32, and I will summarize it, that the alliance is "determined to deploy the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats, including those conducted as part of hybrid campaigns, in accordance with international law."

But they reaffirm a decision as to when a cyber attack would lead to the invocation of article 5, which would be taken by NATO-allied nations on a case-by-case basis, and they said they recognize that the impact of significant, malicious, cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack. That is pretty serious, and I think that is one of the things that we have kind of danced around, we really haven't addressed. We treat all these ransomware attacks as criminal activity, when they may not be exactly carried out by nation states, but in some cases—and I think, in particular, Russia and China—they are at least, if not sanctioned, approved.

And Mr. Lee, I want to direct this to you because you have military background. We have tremendous capabilities in our military to address this. Does it make sense for us to counterattack, and particularly in some of the nations where the government is really a group of oligarchs with tremendous financial interests?

Just—could you address that?

Mr. LEE. Thank you for that question. I think most people in the military would generally like to not get to military force. We want to take all mechanisms available before we get there. And I think there are still plenty left.

However, to directly address the question, I think that we do have to draw certain red lines of what we will and will not accept in this country, and how we are going to respond. And when I have looked at the messaging of NATO and others before on that topic, one of the challenges not only is that we don't specify what that red line is, but we don't tell anybody what we are going to do about it. And so it is not deterrence, it is strategic ambiguity.

Mr. PALMER. That is——

Mr. LEE. So if we are going to use military response, we better well define it.

Mr. PALMER. Yes, I am not talking about an armed response. I am talking about in the cyber field, because they are attacking infrastructure. And I think our government may have a different definition of what is critical infrastructure than perhaps your organization does, and that is troubling to me. I don't think that we can

allow these cumulative attacks to continue, when we know that there—these groups are giving safe harbor in these nations. There needs to be a price that has to be paid.

I want to transition a little bit away from that, and Ms. Walden, I do appreciate what Microsoft is doing. You have really stepped up in terms of law enforcement. But I am just not sure that it is enough. And we have had this discussion about whether or not people should pay. And it was mentioned the percentage increase in ransomware attacks, and I just wonder if the fact that people have cyber insurance and we know that some of these ransomware—these hackers have hacked into these insurance companies and they know what certain groups are capable of paying, is the insurance helping or hurting?

I mean, when they know that they have the ability to pay and they negotiate outside of law enforcement, is that helping or hurting?

Ms. WALDEN. Well, quite frankly, I don't know if it is helping or hurting. I am not a cyber insurance expert. But I will say that there is a whole ecosystem out there that supports victims that are attacked by ransom. And cyber insurance companies are just part of that ecosystem. But whether they are helping or hurting, it is the victims that need to make the right business and operational decisions.

Mr. PALMER. Well——

Ms. WALDEN. I would hope that it means to not pay, but I can understand when they do pay.

Mr. PALMER. Well, one of the things that is missing out on the task force website, and that is whether or not people should pay, and the whole issue of the insurance. That seems to be a pretty substantial omission.

Could you address that, Mr. Reiner?

Mr. REINER. Yes, thank you for the question, Mr. Palmer. I think it really, at the end of the day, was the only item that the task force didn't come to a very specific recommendation on, in terms of why. I think there was a general leaning toward, I think, as my colleagues here have noted, making it so that the least amount of money is going to these criminals as possible and to devise a set of steps so that we could actually move in that direction.

If we were to, for instance, want to prohibit payment now, the ecosystem is simply not ready. It is not prepared for that sort of injunction. So how can we get there?

This—the report actually does lay out a number of steps, milestones, potentially, that could be taken on over the course of a couple of years to get us there. That is shoring up the defenses that we are working with, that is going after these criminals so that they don't act with such impunity. There is a good list of steps that need to be taken first, and then maybe we can move in that direction.

Mr. PALMER. I thank the Chair, and I will submit the balance——

Ms. DEGETTE. I thank the gentleman.

Mr. PALMER [continuing]. Of my questions in writing.

And I yield back.

Ms. DEGETTE. I thank the gentleman. The Chair now recognizes Mr. Ruiz.

Mr. RUIZ. Thank you very much, Chair. Today's hearing is focused on ransomware cyber attacks, which are becoming a growing and frequent threat to our businesses, utilities, and government agencies. Ransomware attacks have devastating consequences on their victims. A company or utility being locked out of its networks means lots—lost of time, lost money, and, in some cases, can also threaten the public's health and safety.

In fact, I have visited Riverside County's Information Technology Center in my district to see what local governments are doing to combat cyber threats, and I have worked with California State University of San Bernardino to strengthen their cyber workforce teaching programs, and for improved pipeline workforce for our Nation.

I would like to know more about what happens when a company suddenly finds its employees locked out of their computers due to ransomware, who they can turn to, and what more the government can do to help. So, Mr. Carmakal, I understand you are involved in incidence response at Mandiant. What do companies struggle with the most, or what are their barriers when faced with a ransomware attack?

Mr. CARMAKAL. Thank you for the question, sir. So there is a lot of confusion in the early days of an incident.

First of all, people don't actually know what actually occurred. Sometimes you can figure out that you are a victim of a cyber attack, because they see a ransom note that is deployed across all systems. When they see that note, a lot of times those—the victim organization may call a legal team to help them assess what to do next. They might call an incident response organization to help them investigate the intrusion. They may call their cybersecurity insurance provider to see whether or not the other third parties that they are engaging can be reimbursed. They may reach out to law enforcement.

But within the first few days there is usually a lot of confusion, and everybody wants to get things back online as quickly as possible. They also want to assess what is the actual true impact of the incident. They want to understand whether or not data was stolen from the environment, and will that information show up on the internet down the road?

And unfortunately, it is a very complex situation that often takes several days or several weeks to be able to investigate and to be able to recover the environment. Most organizations that deal with some kind of disruption, best-case scenario, they will be back online within a few days. Realistic scenario, it is going to take them a few weeks, possibly even months, to fully recover every system across the environment. Every situation is different, and there is usually a team of experts that victim organizations call in and ask for help.

Mr. RUIZ. Thank you. Thank you.

Mr. Reiner, as we have heard today, one of the most challenging decisions a company faces is whether or not to pay the ransom. In fact, whether or not to prohibit payments of ransom was the one key issue on which your Ransomware Task Force could not reach

consensus. So can you please walk us through the considerations here?

And what are the most important recommendations the task force made when it comes to prohibiting ransom payments, and how did you arrive at those priorities?

Mr. REINER. Thank you for the question. Yes, it was definitely a contentious discussion around this issue within the task force. And, as we laid down in the report, what we believe is probably the most appropriate way or the most effective way of approaching this is to have a set of steps that need to be taken in order to move in that direction, if that is what is chosen to be done, from a policy perspective.

I think the conclusion of the task force was that, at this point, if you were to mandate the prohibition of payment, that it was just bad policy and that, again, a number of steps really need to be taken in order to move in that direction, one of which is to shore up defenses and get resources to companies and entities, municipalities, what have you, so that they can better defend themselves; take the fight to these ransomware actors in ways that we currently have not been doing, so they don't get to operate with such impunity; shoring up the cyber insurance market so that it actually is functioning in response to the level of threats that we are dealing with today.

There is really—there's a number of steps that we think need to be undertaken, concurrently——

Mr. RUIZ. Thank you.

Mr. REINER. Yes, sir.

Mr. RUIZ. Dr. Dameff, like you, I am a trained physician, and I know firsthand the heavy reliance hospitals have on digital records and network infrastructure. But people aren't going to stop having medical emergencies or procedures, or practice medicine when their technology is taken away. What kind of procedures do hospitals need in order to be able to effectively operate during ransomware attack?

For instance, should manual backup procedures exist for when electronic records and machines go down?

How can a hospital practice paper backup for preparedness?

And should those drills be included in accrediting bodies' criteria to be accredited?

Dr. DAMEFF. I strongly support the preparation for hospitals to operate under ransomware attack in a manual fashion to the—to restore those systems as quickly as possible, but not to rely on them to deliver emergent care to patients that are still going to come in the front door, like you mentioned, still going to come into the emergency department. Whether or not it should be a portion or a prerequisite or a condition of hospital accreditation is a complicated one, depending on what level of preparation you are going to require of a particular hospital.

What I can say is that there are current processes in place that are required of every hospital to be prepared for all hazards, things like earthquakes and hurricanes, for which cybersecurity disasters—truly, these could be disastrous consequences for hospitals—should be incorporated, and should be prioritized because, generally speaking, cybersecurity attacks—sorry, cybersecurity and

cyber attacks—can hit any hospital without geographic predilection or precondition.

What am I trying to say here is that every hospital needs to take this seriously. Every hospital should prepare for taking care of sick patients without the Electronic Health Record and other technical systems. Any preparation efforts for that should be supported, standardized, studied, and spread across the country.

Mr. RUIZ. Thank you very much.

Ms. DEGETTE. I thank the gentleman. The Chair now recognizes Mr. Joyce for 5 minutes.

Mr. JOYCE. Thank you, Chairwoman DeGette and Ranking Member Griffith, for holding today's hearing on the growing threat of ransomware.

All too often we see our Nation's critical infrastructure being attacked from nefarious actors, exposing our vulnerabilities and ultimately harming our citizens. As a doctor, I am aware of the growing importance of securing patients' personal identifiable information and medical records. This body must take a proactive approach to strengthen all critical infrastructure and ensure that all Americans' medical data is safe from those who choose to do harm.

Dr. Dameff, let's continue the discussion. In your experience, when a hospital or a healthcare system is the victim of a ransomware attack, how long are their systems down? Is it days? Is it weeks? Has it gone on for months?

Dr. DAMEFF. Great question. We have seen the entire gamut. And it doesn't necessarily always match with how prepared they were. It depends often on who the adversary is, what they particularly deployed.

But one thing I will say is that we need to study this because, looking at the latest headlines, it seems like cyber attacks are increasing in sophistication, frequency, and, potentially, increasing downtimes. I see more a trend towards weeks to months than I do days, insofar as these devastating attacks are more impactful and would result in a longer downtime.

Mr. JOYCE. So in this recovery response timeline after a cyber attack, does the healthcare system revert to manual patient care systems?

You said something that is somewhat frightening to me. You said you are a generation of doctors who have never used paper charts or have never written a prescription. As one of the five physicians on this committee here today talking to you, that is frightening to me. How do we respond?

Dr. DAMEFF. I think that it is key that we incorporate cybersecurity training and preparation into the next generation of medical education.

Mr. JOYCE. Would that include paper?

Dr. DAMEFF. I do. I do think that physicians should be trained to operate in conditions that do not have technology, or to rely on less connected technological backups as a stopgap measure for patient care.

Mr. JOYCE. When talking about ways to prevent or mitigate the effects of a cyber attack on healthcare systems, some individuals talk about the cloud or having a system backed up. Are these ultimately foolproof ways to ensure that a hospital system or a

healthcare provider does not have to pay the ransom, or the ransomware attack, or that patients are less impacted?

Dr. DAMEFF. I think that this trend towards centralization of medical device management, for example, or electronic health records into the cloud is a trend we are not going to see change.

I would defer to the specific security protections offered by such cloud architecture to other members of the panel, as it is not my expertise. But I will say that it is a two-edged sword, if you will. The centralization of these into the cloud means that a single attack on a cloud provider offering services to many hospitals across the country, if attacked, could impact all of them at once.

So that being said, many hospitals are not well equipped to defend their systems, as it is. So do you offer increased protections from the cloud more so than you would at individual hospitals, taking the risk that, if that particular cloud provider went down, you know, hundreds of hospitals could be hit?

This is something we are going to have to figure out, and, quite frankly, we do not have the data to make that decision currently.

Mr. JOYCE. Dr. Dameff, I would be remiss if I did not reach out and thank emergency physicians, emergency nurses, emergency technicians as we have faced a pandemic and as you continue to face the ransomware attacks that are occurring in the medical community. As someone who previously worked at Johns Hopkins Bayview Emergency Department, I have great respect for the work that you continue in the face of this pandemic, and I think I acknowledge that today and thank you.

Madam Chair, I remain—I yield my remaining few seconds.

Ms. DEGETTE. Thank you, Mr. Joyce. And I think that the entire panel and the entire Congress would echo your sentiments, thanking——

Mr. JOYCE. Thank you, Chair DeGette.

Ms. DEGETTE [continuing]. Emergency room personnel. Thank you.

The Chair now is pleased to recognize Mr. Peters for 5 minutes.

Mr. PETERS. Thank you, Madam Chair. Thanks to the witnesses for being here.

Dr. Dameff, you have got all the questions, but you are from San Diego, so I just have to ask you a couple.

First of all, thanks for your great work.

And just down the street from you, a major hospital system suffered this very attack, and I assume will—as they ease out of that, or as they climb out of that, we will learn more about what protocols could be.

I have heard you talk about making sure that, in the aftermath of an attack, that hospitals are prepared to operate without their technology, also to define protocols that hospitals might be able to rely on to prepare to defend themselves against these hacks.

One question I just haven't had—you haven't—heard you answer, and forgive me if I missed it, but should we be disconnected a little bit more?

I have often wondered if there is a way to take a unit like a hospital and to have some sort of way to fence it off so that they can operate internally in a connected way without being so exposed.

And that may be a question for you or for some of the people on the panel, but I am curious about that.

Dr. DAMEFF. I do believe we should invest in technology that limits the exposure of hospitals. Traditionally speaking, as I mentioned previously, hospitals are soft targets. They generally have flat networks, meaning that they are often employing the best practices for network segmentation. And as a consequence, they are more at risk for rapid spread of ransomware, for example.

So this concept of isolating critical sections of the hospital and being able to rely on those systems without risk of ransomware would require a lot of those technological solutions. They are costly and, as mentioned previously, there are a lot of healthcare systems that will not have the ability to deploy such technology without resources and additional guidance.

And so, for that, I would encourage that type of isolation. But I fear we are not going to get to it. Instead, I think we are, unfortunately, going to have to rely on just preparing for an inevitable attack and limiting the damage to patient care while we wait for system restoration.

Mr. PETERS. And also deploying defined protocols or best practices, I guess, as it would be—maybe we could help define.

You know, I appreciate that. And I also wanted to follow up on comments from questions from the Chair and from Ms. Schakowsky about what the duty is of private organizations to take care of their stuff.

You know, I thought a lot about Equifax—not to pick on any particular company—but there is a company that is performing a public function with a lot of private data. And it seemed to me that the loss of that data to the malefactors really didn't hit their bottom line. And so I have often wondered if the companies that do this kind of work—sort of like, in a way, providing a public service—are appropriately incentivized to take care of that data.

Maybe, Ms. Walden, I would direct this to you. Your testimony said that we should make sure that companies make it harder to get in, limit the scope of damage, and prepare for the worst. I guess—do you believe that companies are appropriately—to incentivize on—from the bottom line to take care of individuals' data, or is that something that the government has to define better?

Ms. WALDEN. First, as a victim of the OPM breach years ago——

Mr. PETERS. OPM, and the DNC, but I changed my cell phone number. That is a different situation——

Ms. WALDEN. Those are different situations. But I do think that companies need to be held to a standard to protect private data. But these cyber attacks are more than just about data leakage, right? They are interrupting business operations.

Mr. PETERS. Right.

Ms. WALDEN. And I do think that there is a role for the private sector in making sure that they prevent these criminal actors from getting into their systems in the first place. There are some very simple things that can take place that we described here: multifactor authentication, patching your software, et cetera.

But all that is to say is—I think we need to raise the collective security of critical infrastructure owners and operators, and we—

we need to put the onus on both the government, to protect the critical infrastructure, and the private sector that owns and operates the critical infrastructure——

Mr. PETERS. Don't get me wrong. I actually, really, am a believer that the private sector has the—is the appropriate place for these solutions to be investigated and developed. What I don't—what I am—just to make sure that I am clear, is that I am not sure that companies are incentivized in a way that would make them deploy the best practices.

So, even if we knew what those best practices were, even if we defined them from sector to sector, what is going to make the next company who has got private information invest in that, knowing that maybe the loss of that information doesn't directly affect their bottom line?

Ms. WALDEN. I would agree. I think many companies aren't properly incentivized to protect their data.

Mr. PETERS. I am out of my—I am out of time. I would just suggest that we might want to think about defining a duty of care in a piece of legislation that would just make sure that everyone is properly noticed that they have to do the right thing.

And Madam Chair, with that I yield back.

Ms. DEGETTE. I thank the gentleman. The Chair now recognizes Ms. Schrier for 5 minutes.

Ms. SCHRIER. Thank you, Madam Chair, and thank you to our witnesses.

When we hear the term "ransomware," we often think of high-dollar ransoms and large companies. But, as all of you pointed out, individuals and communities are also affected by these attacks when they can't get gas to go to work, when their school or local hospital is impacted by an attack, or when their own data is compromised.

I have heard from local hospitals about the immense cost and manpower it takes to try to harden a whole system to prevent a cyber attack—with my hospital, who is training up a workforce to not fall prey to phishing, and then to recruit and hire the best and brightest in cybersecurity, as you mentioned.

Dr. Dameff, I can tell you, from common experience, that just a few hours of power outage completely handicapped my ability to take care of patients, so I can only imagine how this sort of thing would impact a hospital, especially for days on end. And you already described for my colleague, Mr. Griffith, how those impacts on patient care may be felt more acutely in lesser-resourced and rural hospitals. Could you be a little bit more specific about how sister hospitals, if there even are sister hospitals, local entities, private-sector actors, and the Federal Government could better support specifically those healthcare systems, so that they have the resources they need?

Dr. DAMEFF. Thank you so much for that question.

I think the first and most important thing is the preparatory efforts to prevent and then mitigate the impacts of those attacks. So, looking at your particular geographic area, and understanding where are the linchpin hospitals, right? Which ones are providing trauma services? Which ones are stroke centers?

These types of specialized hospitals, who take care of hyper acute patient care, should be identified early and prioritized for that type of preparation, as well as resources to ensure that, when they do go down or when they are attacked, they are able to fail gracefully as much as possible, while still taking care of patients. So there is a preparatory step in that.

Second, in the response phase of this, I think it is common for a hospital to reach out to law enforcement early. I think that has been a pretty common theme, in that they will reach out to the FBI to help with investigatory efforts and response. But whether or not that type of communication transcends to other government agencies such as CISA or the FDA, even if medical devices are involved, can sometimes be—not happen.

And so I think that is partly the responsibility of a particular hospital but also of the bodies that accredit hospitals as well as local public health authorities in being able to quickly propagate meaningful metrics of patient care to authorities that can help, who can bring resources in the hour of need to help hospitals still take care of patients while addressing that.

Ms. SCHRIER. That is——

Dr. DAMEFF. So that type of interagency communication is lacking.

Ms. SCHRIER. That is really helpful. And I know, in Washington State, our Washington State Hospital Association does these kinds of drills with hospitals to help them prepare.

And then, speaking of incentives, I know a hospital's reputation is really integral to its ability to serve the public. It seems like one of the things we need to communicate to the public is that, even with the best preparation, these attacks are so common that you can still be hit. Do you think that is a role for public—you know, for the government, for the private sector, to kind of communicate this to the public?

Dr. DAMEFF. The communication—oh, thank you very much—the communication of that is rather difficult.

I have always said that there should be no competitive advantage in healthcare cybersecurity, right? There should never be billboards saying, "Come to our hospital, we didn't have this happen," because, quite frankly, I would agree with you that, because of increased—the sophistication of these types of attacks, no one is immune from this. No healthcare organization is immune, regardless of their cybersecurity budget.

So at the end of the day, I think communicating that it is an unfortunate consequence of the hyperconnectivity of healthcare, that there are steps being done and resources provided to hospitals to prepare and mitigate that is key, while still trying to restore trust in consumers and how they approach a particular hospital for healthcare.

Ms. SCHRIER. Thank you.

Dr. DAMEFF. That is key. That is really important.

Ms. SCHRIER. I have one last question for Mr. Reiner.

Now, I appreciate your comments about our country not really being quite at the right place to be able to prohibit payment of ransoms, even though that might slow or stop these cyber attacks. So, for now, what can companies do, for example, to have duplicate

systems, a wall between them so that they could recover afterwards, maybe without paying the ransom?

Mr. REINER. So one of the pieces that we haven't really discussed here today, outside of some of the elements of what companies can be doing to prepare, is to actually—what we discovered through our process is that a lot of companies actually don't have a plan. They actually haven't vetted out, at the executive level, what to do, whether or not to pay. And they have companies that they can turn to that can help them through that process, whether it is their insurance company, or a forensics company, or some of the folks on the panel here with me today.

But actually having that in place ahead of time, companies do tabletop this. They do exercise against it, but not all of them. And I think that is a resource that everyone should have in hand, to have a checklist, to have an actual plan to help make you make that decision if you do get hit.

Ms. SCHRIER. Thank you very much. I yield back.

Ms. DEGETTE. I thank the gentlelady. The Chair now recognizes Mrs. Trahan for 5 minutes.

Mrs. TRAHAN. Well, thank you, Chairwoman DeGette, for this important, certainly informative, and timely hearing.

The threat that hackers pose to businesses and institutions is so real, and the increasing frequency and severity of the attacks is deeply disturbing. You know, like so many of my colleagues and the panelists testifying today, I am concerned that cyber attacks are becoming especially commonplace within critical public service sectors, ranging from healthcare to education. In fact, a public university in my district was recently hit by a cyber attack that shut down operations for a week.

Ransomware has become one of the most attractive tools for criminals because of how lucrative it can be, often without much effort. And hackers find vulnerable caches of critical data being stored by organizations like hospitals, schools, and sometimes even local governments and then use ransomware to effectively lock the organization out of their own data until they agree to pay up.

Now, what has become clear is that improving our cyber defenses is not enough to combat this threat. We need to, you know, find ways to disrupt the ability of criminals to demand and receive ransom payments without consequence.

The Internet has allowed for ransoms to be paid remotely through digital gift cards and, of course, cryptocurrency such as Bitcoin. So, Ms. Walden, could you just explain what it is about cryptocurrencies that make them the chosen method of payment for ransoms in this type of cyber crime?

Ms. WALDEN. Yes, and thank you for that question.

So cryptocurrency, the technology underlying cryptocurrency, blockchain technology, allows for a transparent payment system that is decentralized and distributed, and it allows for, at the same time, pseudoanonymity. It is a complicated word to say for me, but that essentially means that, while you can track the transaction and you can see exactly, you know, the hops of money from one wallet to another, the on-ramps and the off-ramps, you can't necessarily see the persons behind the transaction. You can't see the person that owns the wallet.

So that is one thing that makes it attractive. The other is that the transactional costs in the crypto economy are much lower than in the traditional fiat economy. So central banking systems are just more expensive.

Mrs. TRAHAN. Sure.

Ms. WALDEN. And then, finally, the third thing is that it is difficult to trace—not impossible, but it is difficult to trace. So—but it is—and it is borderless. So you can have money move quickly and effectively across borders. There is no central banking authority that sort of maps it out. And the use of Bitcoin, in particular, is prevalent because it is the most widely used currency, virtual currency. It is easy to get, it is liquid——

Mrs. TRAHAN. Yes.

Ms. WALDEN. And victims can—can easily put that into the system.

Mrs. TRAHAN. Yes. And you——

Ms. WALDEN. I hope that answered your question.

Mrs. TRAHAN. Yes, it definitely did, and it is great to have that thorough answer on the record, because an oft-cited rationale for the use of cryptocurrency is the lack of visibility into parties conducting transactions and a lack of clarity regarding government relations.

And so, Mr. Reiner, I am wondering, you know, if you could answer this question. You know, cryptocurrency exchanges operate in the United States. They are subject to certain regulations. But, clearly, there are opportunities to expand the applicability and/or enforcement of those regulations. And if so, if you agree with that statement, you know, what specifically do you recommend?

Mr. REINER. I would agree with that, and thank you for the question.

I think the task force, as it came together, recommended a number of steps that could be taken to—and I think it is important to note here that the task force's position on this wasn't necessarily that cryptocurrency is the problem, right? Cryptocurrency is something that I think can add value to—in a number of different ways, but that, in this instance, it is something that is being abused.

There are a number of steps that could be taken to pull elements of the cryptocurrency ecosystem into existing regulatory regimes, whether that is expanding the application of know-your-customer rules, the anti-money-laundering rules that are already available.

I think, to your—to the nature of your question, though, something that is incredibly important here is some of this is outside of U.S. jurisdiction, and so there—and we need to be working very closely with international partners so that they can be taking these steps with actors in their spaces to do the same thing.

I think a number of the actors that we engaged with through the Ransomware Task Force process made it very clear that that is a conversation they want to be a part of, to positively contribute in that direction. I think there is real opportunity there.

Mrs. TRAHAN. Great. Well, thank you. I am out of time. I will submit the rest of my questions for the record.

Thank you, Madam Chair.

Ms. DEGETTE. I thank the gentlelady. The Chair now recognizes Mr. O'Halleran for 5 minutes.

Mr. O'HALLERAN. Thank you, Madam Chair and the ranking member, for today's hearing.

You know, securing the infrastructure for America is critical. We are all in agreement with that. I haven't seen anything today that would tell me that we aren't. Issues like Colonial Pipeline, how many more times do we have to see this occur and not get serious about this? Year after year after year, something comes up, where this becomes an issue. And now it is a critical issue, in my mind, for—and I know the doctors' minds—for the health and welfare of the people of America.

Big companies have tons of cyberspace security, and even they are attacked frequently. Should we hope and pray that we won't be targeted, or should we do something about this?

In Arizona we are facing record heat and droughts every year. I am concerned what would happen to vulnerable populations, especially older Americans, if our power, water utilities, and others went down. Our families could be left without running water or power for days, weeks, who knows, as new developments and technologies occur. I hope we can learn from today that this has to be a priority for our businesses in America and our government.

Ms. Walden, I am sure you agree that we need to do more to disrupt ransomware. You said in your testimony that Microsoft is working to make ransomware less profitable and more difficult to employ. What does that mean? What are you doing?

Ms. WALDEN. Thank you for the question. As you aptly pointed out, there is an imbalance, right, that allows ransomware to proliferate: one, it is a highly profitable crime; second, there is—there are few barriers to entry. I could get into the crime of ransomware, and I haven't coded since 1985. So it is just off balance.

And so our opportunity at Microsoft is to disrupt its scale. And what does that mean? That means that we go after the infrastructure. So we go after payment systems that support the profitability, and we disrupt that. But we also make it harder for our products and services to be used to proliferate ransomware. And we make the entry of the criminal to—more difficult, right?

So that means tearing down payment systems where we can, or the ability for ransomware actors to receive payment. And that means tearing down negotiation opportunities between the ransomware criminal gang and the victim. That means disrupting their ability to easily commit this crime. And that also means, from a threat actor perspective, working closely with our law enforcement partners to bring justice to these criminals that propagate the crime.

Mr. O'HALLERAN. Thank you very much for that answer.

Mr. Carmakal, what type of information sharing is there between private sector and the U.S. Government when it comes to attacks on businesses?

And how do we recommend—or you recommend—we can improve this?

It is obvious from today that there's a lot of areas where information sharing does not go on. And I don't know how this whole system works if we don't share that information. Mr. Carmakal, please.

Mr. CARMAKAL. Yes, thank you, sir. I think there is an opportunity for us to do a better job of sharing information between victim organizations and the rest of the world. But they need to do it in a way where they don't feel like they are going to be penalized for having a data security incident.

There is a common trend of victims becoming a second victim because of public shaming by other organizations, by the general public when there is a cybersecurity incident. So we need to create an opportunity and facilitate a way for victim organizations to be able to share information about active attacks, about compromises with some central governing body or some agency that is able to disseminate that information in a quick and actionable way.

A lot of times when we see threat actors operate, they conduct intrusions at dozens of organizations at the same time. And if we are able to take information from one victim organization and share it with the community, it helps us disrupt threat actors, helps us increase the cost of threat actor operations, and I think that is one of the many ways in which we could all take collective actions to curb this problem.

Mr. O'HALLERAN. I thank you.

And Madam Chair, I just don't believe that we are going to get the type of process moving forward that we truly need as a nation without clearly identifying how we are going to communicate with one another in this area, whatever privacy laws have to be placed or whatever has to be done to allow people to be able to talk to one another.

So with that, I yield.

Ms. DEGETTE. Thank you. I thank the gentleman.

The committee has a storied tradition of allowing members of the full committee to question. And that is particularly useful today because we have our resident technology expert with us, Mr. McNerney. So I am pleased to recognize him for 5 minutes.

Mr. MCNERNEY. Well, I thank the Chair for the hearing and the witnesses for your testimony. I thank the Chair and the ranking member for allowing me to waive on this morning—or this afternoon now.

Cybersecurity defenses are primarily intended to safeguard organizations' IT systems, but many critical sectors are relying on OT systems such as SCADA systems and PLCs to operate machinery or industrial controls.

OT system attacks are increasing in severity and frequency. For instance, the case of Colonial Pipeline attack, the company proactively shut down its OT systems in response to ransomware attacks on its IT system. Mr. Lee, how serious and widespread is the ransomware threat on OT systems?

Mr. LEE. Thank you for that question. It is significantly more frequent than people would realize. There's, you know, some weeks that we go where we might have five different incident response cases on just OT systems that never go public.

And so I think, you know, I agree with a lot of the recommendations around removing the stigma around this. But also, we have to make sure that there is value back to those organizations. So there is a lot of desire of you must communicate to the government.

But if there is no value back to those organizations in doing that, it is just not a top priority.

Mr. MCNERNEY. Well, is there any government support for companies in dealing with live OT threats?

Mr. LEE. I think that, while there are many great Members in the government and there is some expertise there, I would say that the OT cybersecurity expertise is very much more in the private sector than in government, and it is very nascent in the government to be able to handle that.

I would say, from a policy position, we should probably more proactively partner with those folks doing that work and make sure that we remove those barriers to get things like visibility in those systems. I think it was mentioned previously that you almost benefit when you have ransomware by the fact that you know it. There's a lot of these cases that people just simply don't know that they are getting compromised.

Mr. MCNERNEY. Thank you.

Mr. Carmakal, over the years in your career you have helped organizations across the globe respond to some of the most catastrophic cybersecurity attacks and insurance instances. Based on your experience, what risks will ransomware attacks on OT systems pose?

And how can the potential victim organizations best protect themselves?

Mr. CARMAKAL. Yes, and thank you for the question, sir. Ransomware attacks against operational technology systems have the potential to be incredibly devastating. We had the potential to see true kinetic responses and impacts that everyday people may be able to observe. And so there is certainly a risk and a threat there.

Generally speaking, a lot of organizations, they struggle to think about security from an operational technology perspective. Part of that challenge is with governance. A lot of times the person that is responsible for cybersecurity doesn't always have the governance and authority to be able to apply cybersecurity protocols and policies on operational technology environments. A lot of times it is the business owner or the asset owner that is responsible for cybersecurity. And a lot of times those asset owners don't actually have cybersecurity experience. And so there's some fundamental challenges that are out there.

I think we need to continue to focus on operational technology security. There is a lot of potential real-world impact that can occur there. And I think it is a natural evolution of the threat that we are seeing today.

Mr. MCNERNEY. Thank you.

And Mr. Lee, what role can the public-private partnerships that the administration announced in April play in shoring up some of these vulnerabilities in OT systems?

Mr. LEE. Yes, the very first thing is partnership with the sector, but more specifically in actually understanding what the sectors need.

A great example: There was many things recommended here today about patching and phishing, you know, training and similar, that are absolutely appropriate in the enterprise, and they would

make a top-10 list in operations technology security. There's a lot of enterprise security people that come into operations environments thinking that the playbook that they run in IT is what they should do in OT. And there have been more power outages in the United States to people patching systems than Russia, China, and Iran combined.

So when we look at OT, we need to make sure that the government partners understand: How do you operate a gas plant different than a nuclear power plant? What do you need to see in these standards, other than just what we think best practices are from a higher level?

Mr. MCNERNEY. Thank you.

Mr. Reiner, thank you for the recommendations from the IST. The discussion today has been entirely focused on attacks on institutions. I am a little curious about attacks on individuals. Are those attacks continuing to escalate, as they are?

Is there any resource in the government for people that need help in that situation?

Mr. Reiner, you want to answer that?

Mr. REINER. I think the preponderance of—I mean, this is a profit-driven enterprise, and so the attackers are looking for those—they do their research, they do their analysis to find those that are not only the most vulnerable but are going to be the most lucrative. And I don't really think that they necessarily discriminate, per se.

I personally am not as familiar with attacks that are targeted against individuals, as much as they are against organizations, which has the large attack surface that can be taken advantage of, et cetera, and that has the resources, actually, to pay these ransoms that these criminals are really looking for.

Mr. MCNERNEY. OK, thank you. I yield back.

Ms. DEGETTE. I thank the gentleman, and I really want to thank again all of our witnesses for participating in today's hearing. It was a really excellent—both the ranking member and I agreed, it was an excellent panel, gave us a lot of good information. And we will be following up with all of you on your recommendations.

I want to remind Members that, pursuant to committee rules, they have 10 business days to submit their additional questions for the record to be answered by the witnesses who have appeared. And I would ask the witnesses to please agree to respond promptly to any of those questions that you might receive, because they will be very helpful to us in developing further legislation and approaches.

Also, the ranking member and I would like to insert into the record by unanimous consent a report on cybersecurity by the E&C Republican staff dated December 7, 2018.

And without objection, it is ordered.

[The information appears at the conclusion of the hearing.]

Ms. DEGETTE. And with that, the subcommittee is adjourned.

[Whereupon, at 1:11 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

CYBERSECURITY STRATEGY REPORT

Prepared by the Energy and Commerce Committee, Majority Staff

Table of Contents

I. Introduction

A. The Subcommittee's Cybersecurity Concepts and Priorities

In today's connected world, where nearly all devices—from the phones in our pockets, to the refrigerators in our kitchens, to the multi-million-dollar equipment that runs our electric grid—are linked together through the Internet, cybersecurity has at once become a household term and one of the most complicated, difficult issues facing society. Once a topic seen mostly as a nuisance, requiring the occasional password reset or new credit card, cybersecurity now regularly makes headlines as the Internet and connected technologies have become not only economic, diplomatic, and military tools, but integral parts of our daily lives. However, even as the Internet has rapidly developed to become a vital part of modern society, it appears that the integration of effective cybersecurity has not kept pace.

Recognizing this reality, the Oversight and Investigations Subcommittee has spent the past several years analyzing certain cybersecurity issues with impacts across the Energy and Commerce Committee's broad jurisdiction. Several patterns have emerged from the Subcommittee's work. Regardless of industry, size, or sophistication, the cybersecurity challenges organizations face are largely the same. Further, traditional information technology (IT) strategies seem largely ineffective at stemming the growing tide of cybersecurity incidents—which now range from ransomware attacks that can hold an entire company hostage to hackers' exploitation of a security vulnerability in the latest cellphone model.

These observations raise two important questions for the Subcommittee:

(1) What are the common, root-cause origins of cybersecurity incidents?

(2) If traditional IT strategies have proven ineffective, what *can* organizations do to better strengthen their cybersecurity capabilities?

With regard to the first question, through dozens of briefings, hearings, letters, reports, and roundtables, the Subcommittee identified six interrelated, core cybersecurity concepts that contribute to cybersecurity incidents:

Concept 1: There will always be unknown unknowns.

Concept 2: You can't protect what you don't know you have.

Concept 3: Software is no longer written, but assembled.

Concept 4: There must be a common cybersecurity language.

Concept 5: Digital assets age faster and less predictably than physical ones.

Concept 6: Cybersecurity takes a "whole-of-society" approach.

The identification of these principles shaped the Subcommittee's approach to cybersecurity and guided subsequent work. As each of these concepts emerged, the Subcommittee began exploring and analyzing possible strategies for addressing them. This effort allowed the Subcommittee to answer the second question, and culminated in six priorities:

Priority 1: The widespread adoption of coordinated disclosure programs.

Priority 2: The implementation of software bills of materials across connected technologies.

Priority 3: The support and stability of the open-source software ecosystem.

Priority 4: The health of the Common Vulnerabilities and Exposures (CVE) program.

Priority 5: The implementation of supported lifetimes strategies for technologies.

Priority 6: The strengthening of the public-private partnership model.

Identifying these priorities was not enough; over the past several years, the Subcommittee has produced individual products related to each of these priorities that address each of their associated core cybersecurity concepts:

B. The Subcommittee's Cybersecurity Work

The Oversight and Investigations Subcommittee's work on these topics began in earnest in 2013, following two major IT-related incidents within the Energy and Commerce Committee's jurisdiction: the data breach at Target that compromised nearly 110 million user records and the launch of healthcare.gov.[1] These issues, along with several other massive data breaches and high-profile cybersecurity incidents across several sectors within the Committee's jurisdiction—including in the automotive, medical, and commercial sectors—raised several questions about the efficiency and efficacy of IT and cybersecurity practices.[2] At the same time, complex legal issues were arising at the intersection of technology and the justice system, to which the Committee responded by participating in the Joint Encryption Working Group with the Committee on the Judiciary.[3] As this work continued, the Subcommittee began to hone in on the common concepts and priorities identified above, and began producing work related to each.

---

[1] Brian Krebs, *The Target Breach, By the Numbers*, KREBS ON SECURITY (May 6, 2014), https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/; Sean Gallagher, *The seven deadly sins of HealthCare.gov*, ARS TECHNICA (OCT. 29, 2013), https://arstechnica.com/information-technology/2013/10/the-seven-deadly-sins-of-healthcare-gov/.

[2] Taylor Armerding, *The 17 biggest data breaches of the 21st century*, CSO (Jan. 26, 2018), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html; Dan Goodin, *Newly discovered flaw undermines HTTPS connections for almost 1,000 sites*, ARS TECHNICA (Feb. 9, 2017), https://arstechnica.com/information-technology/2017/02/newly-discovered-flaw-undermines-https-connections-for-almost-1000-sites/; Andy Greeberg, *Hackers Remotely Kill a Jeep on the Highway—With Me In It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; *Hospital drug pumps are hackable, experts warn*, BBC (June 9, 2015), https://www.bbc.com/news/technology-33063345.

[3] *Encryption Working Group Year-End Report*, H. COMM. ON ENERGY & COMMERCE, H. COMM. ON THE JUDICIARY (Dec. 20, 2016), https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf.

1. Subcommittee Work Related to Coordinated Disclosure

The Oversight and Investigations Subcommittee's work on coordinated disclosure was prompted by both progress and controversy in the public and private sectors on the topic, including guidance for industry released by the Food and Drug Administration released in October 2014 regarding management of cybersecurity in medical devices and media reports regarding vulnerabilities in medical devices and automobiles.[4] In November 2015, the Subcommittee held a staff-level roundtable attended by private sector stakeholders to examine coordinated disclosure and its challenges and opportunities.[5] Focused specifically on coordinated disclosure within safety critical sectors like automotive and medical devices, it brought together experts to discuss how standard coordinated disclosure practices can or should be evolved to better address these sectors' equities and risks. Following a high-profile, non-coordinated disclosure involving a medical device in 2016, the Subcommittee held a second roundtable in February 2017 to encourage further engagement with and development of the topic.[6]

In January 2018, the Energy and Commerce Committee sent letters to seven information technology companies—Amazon, AMD, Apple, ARM, Google, Intel, and Microsoft—involved with the largest known coordinated vulnerability disclosure to date: the discovery and disclosure of cybersecurity vulnerabilities Spectre and Meltdown, which could enable the unauthorized disclosure of sensitive information relying on modern chipsets.[7] The letters commended the stakeholders' embrace of coordinated disclosure while also highlighting potential concerns and the need for continuous evolution and improvement. For example, the Committee was concerned that the information embargo imposed by some letter recipients may have disadvantaged other affected companies that needed to respond to both vulnerabilities. In addition, the Committee was concerned that critical infrastructure equities may not have been fully considered during the letter recipients' decisions regarding disclosure timelines due to the fact that critical infrastructure owners and operators must often test patches for weeks or months before implementation, rather than the hours or days provided during the Spectre and Meltdown disclosure. Each recipient of the letter provided a written response and a briefing to Committee

---

[4] *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*, THE FOOD & DRUG ADMIN. (Oct. 2, 2014), https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf (FDA embrace of coordinated disclosure for medical devices); Charlie Osborne, *Hackers control medical pumps to administer fatal doses*, ZD NET (June 9, 2015), https://www.zdnet.com/article/hackers-can-control-medical-pumps-to-administer-fatal-doses/ (public disclosure of cybersecurity flaw after disagreement between researcher and company); Andy Greeberg, *Hackers Remotely Kill a Jeep on the Highway—With Me In It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; *Hospital drug pumps are hackable, experts warn*, BBC (June 9, 2015), https://www.bbc.com/news/technology-33063345 (hackers disable car engine driven by report on public highway).

[5] U.S. Committee on Energy & Commerce, Roundtable on Coordinated Disclosure, November 2015.

[6] Sean Gallagher, *Trading in stock of medical device paused after hackers team with short seller*, ARS TECHNICA (Aug. 26, 2016), https://arstechnica.com/information-technology/2016/08/trading-in-stock-of-medical-device-paused-after-hackers-team-with-short-seller/; U.S. Committee on Energy & Commerce, Roundtable on Coordinated Disclosure, February 2017.

[7] Letters from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. on Energy and Commerce, to Apple, Inc., Amazon, Advanced Micro Devices, Inc., ARM Holdings, PLC, Google, Inc., Intel Corp., and Microsoft Corp. (Jan. 24, 2018).

staff. The recipients acknowledged the Committee's concerns and provided additional insight and context into their decision-making processes, and pledged to continue working to improve coordinated vulnerability disclosure practices.

In July 2018, along with the Senate Committee on Commerce, Science, and Transportation, the Committee sent a letter to CERT Coordination Center following up on concerns raised about coordinated vulnerability disclosure (CVD) practices in the wake of Spectre and Meltdown.[8] The letter raised two potential gaps in the CVD process here based on the Committees' work involving this vulnerability: (1) whether the CVD process was adequately coordinated to ensure that companies, particularly those providing critical infrastructure, had enough time to test and implement patches prior to public disclosure of the vulnerabilities and that the U.S. government received timely notice of the CVD process; and (2) whether companies used precise terminology in describing the availability, not application, of patches. This latter distinction remains important with regard to patching issues, as a patch may be "available" without an affected user having "applied" it, which leaves the user unprotected. By using the two terms interchangeably, the Committees were concerned that organizations providing patches may have provided a false sense of security to users and the general public.

In October 2018, the Committee released a white paper entitled "The Criticality of Coordinated Disclosure in Modern Cybersecurity."[9] This white paper announced the Committee's support for coordinated vulnerability disclosure, explaining that such programs are a necessity for organizations in a society so heavily dependent on massively complex information systems and networks like the Internet and other connected technologies. It made two recommendations: that Congress clarify the legal environment in which coordinated vulnerability disclosures take place and that it find ways to support and encourage organizations to adopt such programs.

2. Subcommittee Work Related to Software Bill of Materials

In March 2017, an outbreak of the type of file-encrypting malware known as "ransomware" spread quickly across the globe, infecting hundreds of thousands of devices in dozens of countries in a matter of hours.[10] Dubbed "WannaCry," this strain of ransomware leveraged a powerful and widespread flaw in a popular computing operating system to spread quickly from device to device.[11] Most notably, the flaw was not a "zero-day," or unknown flaw, but one for which a patch had been available for months. However, many organizations were unaware of their exposure to the flaw due to the "black-box" nature of many medical technologies.

---

[8] Letter from the Hon. Greg Walden, H. Comm. on Energy & Commerce, and the Hon. John Thune, Sen. Comm. on Commerce, Science, & Transportation, to CERT/CC. (July 17, 2018).
[9] *The Criticality of Coordinated Disclosure in Modern Cybersecurity,* H. Comm. on Energy & Commerce (Oct 23, 2018), https://energycommerce.house.gov/wp-content/uploads/2018/10/10-23-18-CoDis-White-Paper.pdf.
[10] *See* Memorandum to Members, Subcommittee on Oversight and Investigations, Hearing on "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity," June 6, 2017, *available at* https://docs.house.gov/meetings/IF/IF02/20170608/106078/HHRG-115-IF02-20170608-SD011.pdf.
[11] *Id.*

WannaCry thus lent additional weight and urgency to a recommendation in a joint report from the public and private healthcare sectors, "Report on Improving Cybersecurity in the Health Care Industry", that was released in June 2017. The report made a series of recommendations for how the healthcare sector could better prepare for cybersecurity threats, including on software bill of materials, which directly addresses the type of challenge highlighted by WannaCry. The Task Force explained this recommendation, stating:

> Having a "bill of materials" is key for organizations to manage their assets because they must first understand what they have on their systems before determining whether these technologies are impacted by a given threat or vulnerability. Moreover, this transparency enables health care providers to assess the risk of medical devices on their networks, confirm components are assessed against the same cybersecurity baseline requirements as the medical device, and implement mitigation strategies when patches are not available.[12]

In response to the outbreak, report, and other related Subcommittee work, the Energy and Commerce Committee held a roundtable in August 2017 to discuss the opportunities and challenges presented by the recommendation to begin leveraging "bills of materials" in the healthcare sector.[13] Following that initial conversation, in November 2017, the Committee sent a letter to the Department of Health and Human Services (HHS) requesting that HHS convene an industry-wide process to find ways to develop, implement, and leverage software bill-of-materials (SBOM) across the health care sector.[14] In its response to the Committee, HHS set out their timetable to launch such a process:[15]

By July 30, 2018:	Announce the software BOM effort work stream to be conducted under the Healthcare Sector Coordinating Council (HSCC) MedTech Cyber Security Risk Management Task Group 1B.
By November 30, 2018:	Publish *Federal Register* notice for public meeting
By January 26, 2019:	Publish proposed agenda for public meeting
February 25, 2019:	Hold public meeting (draft deliverables will be vetted in a public setting)

[12] *Report on Improving Cybersecurity in the Health Care Industry*, HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, June 2017, https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf.
[13] U.S. Committee on Energy & Commerce, Roundtable on Software Bills of Materials, August 2017.
[14] Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to the Hon. Eric D. Hargan, Deputy Secretary, Dept. of Health & Human Services (Nov. 16, 2017), https://energycommerce.house.gov/wp-content/uploads/2017/11/20171116HHS.pdf.
[15] Letter from Matthew D. Bassett, Assistant Secretary for Legislation, Dept. of Health & Human Services, to the Hon. Greg Walden, Hon. Frank Pallone, Jr., and Hon. Diana DeGette, H. Comm. on Energy & Commerce (Sept. 18, 2018), https://energycommerce.house.gov/wp-content/uploads/2018/09/091718-HHS-Reply-to-Chairman-Walden.pdf.

By August 24, 2019:	Publish meeting summary to include responses to any recommendations made at the meeting or in the docket for the meeting

3. Subcommittee Work Related to Open-Source Software

As modern information systems and products have continued to grow in scale, sophistication, and complexity, the Subcommittee's work recognized the critical importance that open-source software (OSS) plays. The Energy and Commerce Committee sent a letter in April 2018 to the Linux Foundation, which leads an organization dedicated to the health and stability of OSS, requesting additional information on how OSS may be better supported.[16] The letter acknowledged that OSS has become "critical cyber infrastructure" and that, consequently, "the sustainability and stability of the OSS ecosystem is essential to the sustainability and stability of organizations' cybersecurity generally."[17]

The Linux Foundation responded on April 23, 2018, agreeing with the Committee's assessment and stating "it is the collective responsibility—and imperative—for business, industry, academic and technology leaders to work together to ensure that OSS is written, maintained and deployed as securely as possible" and "[i]t is essential that the corresponding OSS communities are supported and properly enabled to be proactive enough to manage future security challenges that will arise over time."[18]

4. Subcommittee Work Related to the Common Vulnerabilities and Exposures Program

While cybersecurity strategies, policies, and procedures remain largely individualized from organization to organization, there exist some foundational cornerstones that all such programs require. One of those cornerstones is the Common Vulnerabilities and Exposures (CVE) program, the standardized naming scheme for cybersecurity vulnerabilities the world over. In 2016, public reports emerged that the CVE program was struggling to fulfill its purpose and meet stakeholder needs.[19]

In response, beginning in March 2017 and culminating in August 2018, the Energy and Commerce Committee investigated the health and stability of the CVE program. In March 2017, the Committee requested documentation from the program's responsible organizations, DHS and

---

[16] Letter to Mr. Jim Zemlin, Executive Director, the Linux Foundation, from the Hon. Greg Walden and Hon. Gregg Harper, H. Comm. on Energy and Commerce (Apr. 2, 2018), https://energycommerce.house.gov/wp-content/uploads/2018/04/040218-Linux-Evaluation-of-OSS-Ecosystem.pdf.
[17] *Id.*
[18] *Id.*
[19] Catalin Cimpanu, *CVE System Sees Huge Backlog, Researchers Propose Alternative*, SOFTPEDIA, Mar. 12, 2016, http://news.softpedia.com/news/cve-system-sees-huge-backlog-researchers-propose-alternative-501665.shtml; Sean Sposito, *CVE, a key cybersecurity resource, is at risk inside and out*, SAN FRANCISCO CHRONICLE, Mar. 25, 2016, http://www.sfchronicle.com/business/article/CVE-a-key-cybersecurity-resource-is-at-risk-7107509.php; CSO, *Over 6,000 vulnerabilities went unassigned by MITRE's CVE project in 2015,* CSO ONLINE, Sep. 22, 2016, http://www.csoonline.com/article/3122460/techology-business/over-6000-vulnerabilities-went-unassigned-by-mitres-cve-project-in-2015.html.

MITRE, including all contracts associated with the CVE program and any timelines, analyses, or other relevant documentation detailing the oversight both organizations had performed throughout the program's lifetime.[20]

In August 2018, the Committee sent a second letter to DHS and MITRE summarizing the findings of the investigation, including that the contract vehicle for the CVE program was awarded or modified 30 times in nearly seven years, that funding for the program varied acutely, and that neither DHS nor MITRE conducted substantial oversight of the program.[21] The second letter made recommendations to both organizations based on the produced documentation, mainly that DHS should transition the CVE program to a dedicated Program, Project, or Activity funding model, and that DHS and MITRE should perform biennial reviews of the CVE program to ensure its effectiveness and stability.[22]

In September 2018, the Cyber Threat Alliance and the Cybersecurity Coalition, two groups comprised of cybersecurity companies and experts dedicated to advancing and improving robust cybersecurity practices and policies, expressed agreement with the recommendations made to DHS and MITRE. In a letter to the Committee, the groups wrote, "The Committee's August 27th letters noted the CVE program's importance, referring to it as 'critical cyber infrastructure.' We concur with the Committee's assessment."[23]

5. Subcommittee Work Related to Supported Lifetimes

The ransomware outbreak known as WannaCry, followed closely by an outbreak of an even more destructive strain of malware known as NotPetya, highlighted the cybersecurity risks that the use of old, outdated technologies pose. In recognition of both that fact, and that addressing such risks is a complex, multi-faceted problem, the Committee on Energy and Commerce in April 2018 released a Request for Information (RFI) seeking input on how to address legacy technology and related issues in the health care sector. The RFI stated that "[t]he challenges created by legacy technologies are, by definition, decades in the making. They implicate dozens of diverse stakeholders with different and at times competing equities, and they have no clear solutions . . . [t]o understand the full scope of the challenge and potential paths to

---

[20] Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to Mr. Jason Providakes, President and Chief Executive Officer, MITRE Corp. (March 31, 2017); Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to the Hon. General John F. Kelly, Sec'y, U.S. Dep't of Homeland Security (March 31, 2017).

[21] Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to Mr. Jason Providakes, President and Chief Executive Officer, MITRE Corp. (Aug. 27, 2018); Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to the Hon. Kristjen Nielsen, Sec'y, U.S. Dep't of Homeland Security (Aug. 27, 2018).

[22] *Id.*

[23] Letter from Cybersecurity Coalition and Cyber Threat Alliance to Hon. Greg Walden, Hon. Gregg Harper, Hon. Marsha Blackburn, and Hon. Robert E. Latta (Sept. 11, 2018), https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/Joint-Coalition-CTA-Letter-to-House-EC-on-CVE-9112018.pdf.

address it, [the Committee requires] insight from stakeholders of all sizes, from all parts of the health care sector."[24]

In response, the Committee received nearly 300 pages worth of comments. For example, many stakeholders agreed with two of the Committee's existing priorities, coordinated vulnerability disclosure and software bill of materials, while raising many additional complex issues to be considered. Following the RFI's release and the receipt of comments, the Committee continues to explore supported lifetimes challenges and opportunities, including a staff-level roundtable in October 2018 with members of the healthcare sector to discuss how to improve transparency and clarity with regards to legacy technology risks, roles and responsibilities, and strategies.[25]

6. Subcommittee Work Related to The Public-Private Partnership Model

While the nation is experienced at responding to threats to critical infrastructure from natural and man-made disasters, both the public and private sectors continue to explore and evolve their strategies for addressing cybersecurity threats. Throughout the first half of 2017, the Subcommittee on Oversight and Investigations held several events focused on the public-private partnership model established under current law that provides a framework for responding critical infrastructure threats caused by cybersecurity incidents.

At the first event, a roundtable discussion, Committee Members and representatives from public-private partnership organizations discussed current challenges and opportunities. On April 4, 2017, the Subcommittee held a hearing entitled "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships" at which members heard testimony from Denise Anderson, President, National Health Information Sharing and Analysis Center, Michael McNeil, Global Product Security and Services Officer, Phillips, and Terry Rice, Vice President, IT Risk Management and Chief Information Security Officer, Merck & Company, Inc. At that hearing, both Members and the witnesses focused on the fact that modern heath care cybersecurity is no longer just about protecting patient data or information, but that it has become a patient safety issue.[26]

On June 8, 2017, the Subcommittee held a hearing entitled "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity" at which members heard testimony from Emery Csulak, Chief Information Security Officer and Senior Privacy Official, Centers for Medicare and Medicaid Services and co-chair, Health Care Industry Cybersecurity Task Force, Steve Curren, Director, Division of Resilience, Office of Emergency Management, Office of the Assistant Secretary for Preparedness and Response, and Leo Scanlon, Deputy Chief Information Security Officer, U.S. Department of Health and Human Services. At

---

[24] *Supported Lifetimes Request for Information*, H. Comm. on Energy & Commerce (Apr. 20, 2018), https://energycommerce.house.gov/wp-content/uploads/2018/04/20180420Supported_Lifetimes_RFI.pdf.
[25] U.S. Committee on Energy & Commerce, Roundtable on Supported Lifetimes, October 2018.
[26] *Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships Before the Subcomm. On Oversight & Investigations*, 115th Cong. (Apr. 4, 2017), https://energycommerce.house.gov/hearings/cybersecurity-heath-care-sector-strengthening-public-private/.

this hearing, which took place only weeks after the WannaCry infection that crippled health care systems in the United Kingdom, members highlighted the criticality of the Department's role as a leader and partner in health care cybersecurity and pressed the witnesses to ensure that Department remained effective at both.[27]

* * *

This report seeks to combine the work described above into an overarching strategy detailing why the Subcommittee selected these core concepts, why these priorities represent the most effective strategies for addressing them, and, most importantly, why each concept and each priority is inextricably linked to its fellows.

Cybersecurity's importance grows in parallel to society's dependence on the Internet and connected technologies. Over the course of the last two decades, the Internet has exponentially expanded and society's dependence on connected technologies has exploded. If the growth during that period is to serve as a guide, cybersecurity is and will continue to be one of the premier issues facing governments, companies, and individuals globally. This report represents the culmination of the Subcommittee's initial efforts illuminate these issues for use by the full Committee on Energy and Commerce, and to assist with its various and ongoing legislative work addressing cybersecurity matters across its jurisdiction.

[27] *Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity Before the Subcomm. On Oversight & Investigations*, 115th Cong. (June 8, 2017), https://energycommerce.house.gov/hearings/cybersecurity-heath-care-sector-strengthening-public-private/.

II. Coordinated Disclosure: Because There Will Always Be Unknown Unknowns

A. Concept: There Will Always Be Unknown Unknowns

As the Subcommittee on Oversight and Investigations led Committee efforts to investigate the growing number of cybersecurity incidents over the past several years, a common trend emerged: organizations that suffer cybersecurity incidents often do not discover those incidents themselves. Federal agents notified 3,000 companies in 2013 that they had suffered data breaches.[28] Two independent security researchers discovered the infamous "Jeep hack" found to affect certain Chrysler vehicles.[29] Google, Intel, Johnson & Johnson, General Motors, and even the United States Department of Defense have each been informed of cybersecurity vulnerabilities in their systems by external parties.[30] At first glance, the fact that organizations are not discovering their own incidents may seem irresponsible. But in looking at the complexity of modern systems, it is clear why this is the case.

Modern information systems and networks contain hundreds to thousands of individual hardware and software components, each of which typically contain dozens of software libraries and thousands of lines of code, which in turn may be vulnerable to various cybersecurity flaws or risks. The exact combination of these components then varies from network to network, where organizational requirements or misconfigurations may introduce new sources of vulnerability. Exacerbating the situation, one organization's network is then connected to additional networks, and in doing so inherits the complexity and vulnerabilities of each system to which it is attached. As frustrating as it seems, in cybersecurity, there will always be "unknown unknowns."

The recognition of this fact gives rise to a daunting question—what can an organization do about it? It is unacceptable to take no action, since the frequency and severity of cybersecurity incidents has been increasing steadily and shows no signs of slowing. Expecting organizations to identify all their unknown unknowns, however, would be impractical and counterproductive. One way to solve this problem, which has been implemented in many modern cybersecurity incidents, is third-party disclosure. To put it simply, even if an organization doesn't know what it doesn't know, someone else might. And better yet—that entity might be willing to work with the affected organization to fix it.

---

[28] Ellen Nakashima, *U.S. notified 3,000 companies in 2013 about cyberattacks*, WASH. POST (Mar. 24, 2014), https://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html?utm_term=.e8e60d8f5dd1.

[29] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me In It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[30] Lisa Ferdinando, *Carter Announces 'Hack the Pentagon' Program Results*, U.S. DEPT. OF DEFENSE (June 17, 2016), https://www.defense.gov/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results/; Tod Beardsley, *R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump*, RAPID7 (Oct. 4, 2016), https://blog.rapid7.com/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/; Peter Bright, *Meltdown and Spectre: Here's what Intel, Apple, Microsoft, others are doing about it,* ARS TECHNICA (Jan. 5, 2018), https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/; Kate Conger, *General Motors is Expanding Its Bug Bounty Program*, GIZMODO (Mar. 15, 2018), https://gizmodo.com/general-motors-is-expanding-its-bug-bounty-program-1823809720.

B. Priority: Coordinated Disclosure

Coordinated disclosure is a collaborative vulnerability identification and remediation process. A coordinated disclosure occurs when a "finder," whose identity can range from an independent individual to a large, multi-billion-dollar company, discovers a cybersecurity vulnerability or incident and then notifies the "owner" of the affected product or network about the issue. These parties then typically work together behind the scenes to validate the findings, develop a patch or mitigation, and then publicly announce both the flaw and the fix at an agreed-upon time. While coordinated disclosures can and do occur on an ad-hoc basis, the most successful coordinated disclosures generally take place within official coordinated disclosure programs adopted by organizations.

An organization's adoption of a coordinated disclosure program produces numerous benefits. It allows an owner to invite the aid and expertise of outside parties in identifying an organization's unknown unknowns, potentially avoiding a cybersecurity incident later, while setting "ground rules" for third-party investigations of its data and networks. This scoping helps to avoid unintended consequences such as outages or data destruction, and allows an owner to simultaneously protect its assets and customers while receiving the full benefits of coordinated disclosure. Finders in turn benefit through the ability to perform cybersecurity research without fear of civil or criminal penalties, incentivizing them to ferret out otherwise invisible bugs and report them to the affected owner. By enabling both behaviors, coordinated disclosure programs facilitate the protection of society at large by providing robust mechanisms through which cybersecurity vulnerabilities may be found and fixed before they become a widespread threat.

The existence of coordinated disclosure recognizes the reality that all organizations will always have cybersecurity unknown unknowns. But organizations' accelerating adoption of coordinated disclosure programs serves as an acknowledgement that one of the most effective ways to address those unknowns is to invite collaboration and cooperation. Such programs greatly increase the chance that an organization will be made aware of potential vulnerabilities before they lead to a cybersecurity incident that negatively impacts the organization, its partners, and users. Coordinated disclosure is, however, only the first step in addressing the myriad cybersecurity threats facing organizations and society. The next step is to minimize as many of those unknown unknowns as possible.

Committee Products: Roundtables and Spectre and Meltdown Investigation

In November 2015 and February 2017, the Energy and Commerce Committee held staff-level roundtables with private sector stakeholders to examine coordinated disclosure and its challenges and opportunities.

In January 2018, the Energy and Commerce Committee sent letters to stakeholders responsible for the largest known coordinated vulnerability disclosure to date.

In July 2018, the Energy and Commerce Committee and the Senate Committee on Commerce, Science, and Transportation sent a follow-up letter to CERT/CC asking them to incorporating lessons learned from recent coordinated disclosures.

In October 2018, the Energy and Commerce Committee released a white paper, "The Criticality of Coordinated Disclosure in Modern Cybersecurity."

III. Software Bill of Materials: Because You Can't Protect What You Don't Know You Have

A. Concept: You Can't Protect What You Don't Know You Have

Two major incidents in recent years have underscored the stark truth that, in cybersecurity, you can't protect what you don't know you have: the discovery of the critical vulnerability known as Heartbleed and the outbreak of the widely infectious ransomware known as WannaCry. Amid both incidents, organizations looking to protect themselves scrambled to find out if they were vulnerable. This arguably straightforward inquiry turned into a Pandora's box, however, as organizations quickly realized that, due to incomplete asset and inventory lists of the technologies in their environments, they didn't know if their systems and networks were exposed to either threat. This in turn led to an even more problematic realization: even if they *had* perfect inventory lists, the black-box nature of many technologies would stymie their efforts.

Heartbleed and WannaCry took place three years apart, the former in 2014 and the latter in 2017. Regardless, organizations found themselves facing the same challenge. Due to the black-box nature of most technologies, organizations did not know, and had no straightforward way to discover, what hardware or software they were running. This lack of visibility—which still exists today, across all sectors and many technologies—forces organizations to try to mitigate cybersecurity vulnerabilities blindly, relying on sporadic and usually opaque vendor guidance when it's provided, or on broad-stroke best practices when it's not. By demonstrating the consequences that can arise when organizations lack visibility into the technologies in their environments, Heartbleed and WannaCry provided two painful examples of the following concept—you can't protect what you don't know you have.

As *some* unknown unknowns are inevitable, the most effective method for organizations to address this reality is to maximize what they know. As illustrated by Heartbleed and WannaCry, organizations need to dramatically improve their asset and inventory strategies to ensure that these lists are comprehensive and up-to-date. As Heartbleed and WannaCry also revealed, however, this is not enough. Organizations must find some way to crack open the current technology black boxes that they are connecting to their systems so that they may fully assess their risks and, as a result, more completely understand their organization's cybersecurity exposure.

B. Priority: Software Bill of Materials

One way for an organization to be better prepared to respond to vulnerabilities is to have a software bill of materials (SBOM) that details the components that form the technology it uses. The concept has existed for many years in various forms, but a 2017 report included the practice as an official recommendation for government agencies.[31] In short, SBOM becomes an ingredients list for a given piece of technology, listing the hardware, software, and other relevant components that it contains or relies upon. This creates two primary benefits. First, it permits organizations to make informed risk decisions about which technologies to purchase and use based on known

[31] *Report on Improving Cybersecurity in the Health Care Industry*, HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, June 2017, https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf.

vulnerability information. Second, when new vulnerabilities are discovered, it allows organizations to quickly identify their exposure and to take appropriate steps in response.

The problem highlighted by Heartbleed and WannaCry was not that organizations did not know which software was vulnerable—that information was made publicly available from the outset—it was that they did not know which pieces of technology that *they depended on* included it. SBOM addresses this issue by cracking open otherwise black box technologies. In doing so, it helps minimize the number of unknown unknowns with which organizations must contend, and greatly increases their ability to protect themselves, their users, and ultimately society, by giving them much-needed cybersecurity data to which they can respond.

Much like coordinated disclosure, however, SBOM is not an end in and of itself. Once organizations have access to and have developed methods to leverage SBOM and minimize their unknown unknowns, these ingredient lists by their nature will reveal additional factors. One of the primary factors that any SBOM will quickly make clear is that, in addition to the proprietary technologies that organizations know that they are acquiring when they purchase IT, organizations will see the pervasiveness of open-source software—which they often do not know they're acquiring.

Committee Product: **Software Bill of Materials Letter**

In August 2017, the Energy and Commerce Committee convened a staff-level roundtable with members of the healthcare sector to discuss the opportunities and challenges associated with SBOM design and deployment.

Following that initial discussion, in November 2017, the Energy and Commerce Committee sent a letter to the Department of Health and Human Services (HHS) requesting that HHS convene an industry-wide process to find ways to develop, implement, and leverage SBOM across the health care sector. In response, HHS launched this process in 2018, which will conclude in 2019.

IV. Supporting Open-Source Software: Because Software Is No Longer Written, But Assembled

A. Concept: Software is No Longer Written, But Assembled

Walk into nearly any office in today's connected world, and it is likely that the desks will be topped by computers running Microsoft's Windows or Apple's macOS. Their screens might show websites open in Google's Chrome or Microsoft's Edge, and smartphones running Apple's iOS or Google's Android will likely be sitting next to keyboards. The ubiquity of such proprietary technologies is so well-known that it is taken for granted. What remains less well-understood are the technologies and software running under the hood of each of those products. The Windows operating system is not constructed solely of Microsoft-developed code.[32] Android phones and iPhones contain more than Google- or Apple-designed software.[33] Today, an organization's technology rarely consists solely of that organization's code.

For the same reasons that physical manufacturing moved away from bespoke craftmanship to assembly-line-based manufacturing, software development has moved from an artisanal, soup-to-nuts process to one more akin to bricklaying. The bricks are supplied by open-source software (OSS), which provides free, customizable code packages that typically perform one programming task—such as data encryption or storage—reliably and efficiently. Like screws, nuts, or washers, whose standardized characteristics allow their use across an array of physical products and whose availability eliminates the need for companies to develop custom tools, OSS may be built into larger pieces of software to take care of common programming staples. The benefits of doing so are so remarkable, in fact, that one study estimates that 78 percent of companies "run on OSS."[34] Consequently, software is no longer written, but assembled.

With that concept comes a corollary; in such a world, the quality of the bricks used to assemble software becomes critically important. If 78 percent of companies rely on OSS, then OSS vulnerabilities—reliability, cybersecurity, or otherwise—can pose an immediate and widespread threat to a significant portion of modern organizations. Considering that many pieces of OSS are developed and maintained by globally-located volunteers, many of whom are unpaid and have unrelated full-time employment, it is no longer enough for organizations to prepare for Microsoft's infamous Patch Tuesdays, or for IT departments to ensure that their workforces are running the latest iOS on company iPhones. Now, these organizations must recognize the critical importance of OSS and behave accordingly.

---

[32] *Open Source at Microsoft*, MICROSOFT (last visited Apr. 11, 2018), https://opensource.microsoft.com/.
[33] *Open Source*, APPLE (last visited Apr. 11, 2018), https://developer.apple.com/opensource/; *Google Open Source*, GOOGLE (last visited Apr. 11, 2018), https://opensource.google.com/projects/list/featured.
[34] *2015 Future of Open Source Survey Results*, BLACK DUCK SOFTWARE (Apr. 15, 2015), https://www.slideshare.net/blackducksoftware/2015-future-of-open-source-survey-results/9-SECTION2CORPORATEUSE2XSINCE_2010USE_OF_OPEN_SOURCE.

B. Priority: Supporting Open-Source Software

Stakeholder support for OSS is neither a particularly new nor complicated policy proposition. The Heartbleed vulnerability—before it became a key exhibit in the argument for better technology transparency and SBOM—led many organizations to recognize their status as OSS-reliant stakeholders, and prompted the very behavior changes the pervasiveness of OSS requires. While examples like the Core Infrastructure Initiative remain the clearest manifestations of these changes, as the Initiative's members include some of the largest technology companies in the world and it provides funding and other support for the OSS ecosystem, it is not the only example.[35] Some organizations now allow and encourage their programmers to contribute to OSS as part of their duties, and others have "open-sourced" some of their own code to better promote software quality across the connected ecosystem.[36]

Each of these contributions, whether on the global scale of the Initiative or the smaller scale of individual company efforts, helps improve the overall health of the OSS ecosystem. They recognize that OSS is not just another shared resource; OSS components form such a substantial part of the Internet's foundation that to strengthen one is to strengthen the other. As a result, such contributions enable some of the highest return-on-investment for companies looking to improve cybersecurity for a relatively low cost. After all, if 78 percent of companies run on OSS, then any improvement in the quality of OSS bricks will create immediate, widespread, and effective increases in the overall quality of the cybersecurity capabilities of the organizations using them.

OSS support, together with coordinated disclosure and SBOM, recognize and address some of the most critical facets of organizations' modern cybersecurity challenges. The combination of these three priorities allows organizations to simultaneously accept their unknown unknowns, minimize as many of them as possible, and support the quality of the shared software resources upon which they, their partners, and their customers rely. At some point, however, organizations need to look outside of themselves to truly understand their cybersecurity exposure and manage their cybersecurity risks. When that occurs, organizations need a common cybersecurity language.

Committee Product: Open-Source Software Letter

In April 2018, the Energy and Commerce Committee sent a letter to the Linux Foundation, which leads the Core Infrastructure Initiative, requesting additional information on how OSS may be better supported. The Committee continues to analyze the response and explore ways to ensure the stability and effectiveness of the OSS ecosystem.

[35] *FAQ – What is the Core Infrastructure Initiative?*, CORE INFRASTRUCTURE INITIATIVE (last visited Jan. 17, 2018), https://www.coreinfrastructure.org/faq.
[36] Cynthia Harvey, *35 Top Open Source Companies*, DATAMATION (Sep. 21, 2017), https://www.datamation.com/open-source/35-top-open-source-companies-1.html.

V. The CVE Program: Because There Must Be a Common Cybersecurity Language

A. Concept: There Must Be a Common Cybersecurity Language

Setting aside clever marketing names like Meltdown, FREAK, or Heartbleed, when cybersecurity vulnerabilities are found today, they are not identified by a description of the vulnerability itself—which may be, in strict terms, several flaws chained together—but by a Common Vulnerabilities and Exposures Identifier or CVE ID. Overseen by the Department of Homeland Security (DHS) and maintained by federal contractor MITRE, the CVE program has provided unique identifiers for over 100,000 vulnerabilities during its two decades in existence.[37] In a world where cybersecurity incidents can occur in a fraction of a second, with flaws that range from straightforward to outright labyrinthine, the ability enabled by the CVE program to instantaneously identify a vulnerability is critical to modern cybersecurity professionals, products, and practices.

This fact was made abundantly clear in the spring of 2016, when multiple media outlets reported that the CVE program was struggling to keep up with the number of vulnerabilities reported.[38] As the program administrators later publicly admitted, the explosive growth of connected technologies had caught the program off-guard.[39] Consequently, ID assignments were delayed for weeks or sometimes months, and some vulnerabilities were deemed "out of scope" for the program and rejected outright.[40] As outlined in the press reports, these issues had immediate, noticeable impacts on the cybersecurity industry.[41] It was during this period, as stakeholders caught a glimpse of what a world without CVE might look like, that the following concept became clear: there must be a common cybersecurity language.

What also became exceedingly clear is that the CVE program already is that common language. Over its two decades, the CVE program has become more than just another convenient government service; it is the cornerstone on top of which modern cybersecurity is constructed. It took the 2016 press reports to shine a light on not just this truth, but on the far more uncomfortable truth that CVE stakeholders, both in the public and private sector, had taken the program for granted. To protect the CVE program, the root-causes of problems affecting the program needed identification and remediation.

---

[37] *About CVE*, THE MITRE CORPORATION (last visited Nov. 30, 2018), https://cve.mitre.org/about/.
[38] Catalin Cimpanu, *CVE System Sees Huge Backlog, Researchers Propose Alternative*, SOFTPEDIA, Mar. 12, 2016, http://news.softpedia.com/news/cve-system-sees-huge-backlog-researchers-propose-alternative-501665.shtml; Sean Sposito, *CVE, a key cybersecurity resource, is at risk inside and out*, SAN FRANCISCO CHRONICLE, Mar. 25, 2016, http://www.sfchronicle.com/business/article/CVE-a-key-cybersecurity-resource-is-at-risk-7107509.php; CSO, *Over 6,000 vulnerabilities went unassigned by MITRE's CVE project in 2015,* CSO ONLINE, Sep. 22, 2016, http://www.csoonline.com/article/3122460/techology-business/over-6000-vulnerabilities-went-unassigned-by-mitres-cve-project-in-2015.html.
[39] *News & Events – FOCUS ON: CVE Program Status*, THE MITRE CORPORATION, Mar. 21, 2016, https://cve.mitre.org/news/archives/2016/news.html#march212016_FOCUS_ON_CVE_Program_Status_Update.
[40] *See supra* note 11.
[41] *See supra* note 11.

B. Priority: The CVE Program

The Committee on Energy and Commerce opened an investigation into the CVE program in March 2017.[42] That investigation acknowledged that while steps had been taken to improve the program's effectiveness and stability following the 2016 press reports, neither DHS nor MITRE had provided an explanation as to *how* the program had become so unprepared. To answer that question and ensure that the same or similar issues would not reoccur, the Committee requested and reviewed contract and management documentation related to the CVE program. That review found that instability in the program's funding and management mechanisms were primarily at fault, and resulted in two recommendations: that DHS move the CVE program from a contract-based funding model to a dedicated Program, Project, or Activity and that both DHS and MITRE should perform biennial reviews of the program. The Committee believed these recommendations would strengthen the program and minimize the likelihood of serious problems once again interfering with its operation.

Both the Committee's investigation and its recommendations acknowledge that the CVE program is the foundation upon which modern cybersecurity practices are built and the common language that modern cybersecurity practitioners speak. By exercising its authority to analyze the historical factors that had allowed the CVE program's problems to manifest and grow entrenched, and then shaping the resulting conclusions into actionable recommendations, the Committee sought to ensure that a critical cybersecurity resource did not collapse. More than that, the recommendations were targeted at creating an environment in which the CVE program would be able to grow and evolve in parallel to the very stakeholders it is meant to serve.

The CVE program, like coordinated disclosure, SBOM, and OSS support, remains another critical cybersecurity building block. To be truly effective, organizations must continue building atop it, and leverage the common cybersecurity language it creates to better understand and analyze their IT and cybersecurity posture. In doing so, organizations using the program and its vocabulary of CVE IDs will quickly be confronted with the fact that all digital technologies are vulnerable and the older a technology is, the more vulnerable it becomes.

Committee Products: Oversight Letters on the CVE Program (March 2017, August 2018)

Beginning in March 2017 and culminating in August 2018, the Energy and Commerce Committee investigated the health and stability of the CVE program. The first letter requested documentation from the program's responsible organizations, DHS and MITRE, while the second made recommendations to both organizations based on the produced documentation.

[42] Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to Mr. Jason Providakes, President and Chief Executive Officer, MITRE Corp. (March 31, 2017); Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to the Hon. General John F. Kelly, Sec'y, U.S. Dep't of Homeland Security (March 31, 2017).

VI. Supported Lifetimes: Because Digital Assets Age Faster and Less Predictably Than Physical Ones

A. Concept: Digital Assets Age Faster and Less Predictably Than Physical Ones

While recent newsworthy cybersecurity incidents have targeted a wide variety of victims and varied wildly in sophistication, effectiveness, and consequences, many share a common factor: the exploitation of old or legacy technologies. The infamous WannaCry outbreak that ravaged the healthcare sector exploited a 30-year-old protocol.[43] Triton, a strain of malware designed to target industrial control systems within the energy sector, relied upon a vulnerability in a legacy version of a manufacturer's firmware.[44] More generally, many malware authors leverage "exploit kits," which combine multiple known vulnerabilities into a single package that, upon execution by unsuspecting victims, attempt to exploit any unpatched, legacy software or firmware on a victim's device.[45]

This trend is borne out in more than just anecdotal data; a cursory examination of any technology's CVE IDs shows that the number of associated discovered vulnerabilities increases over time. Like physical products later found to have some flaw under certain circumstances, the very process of putting digital technologies into use will stress them and reveal both reliability and cybersecurity issues. Further exacerbating this is the pace of technological innovation; organizations are constantly developing or searching for new, more advanced technologies to better carry out their missions. As a result, legacy technologies receive less support and attention as time goes on. This confluence of factors leads to the following concept; digital assets age faster and less predictably than physical ones.

When faced with the potentially severe consequences created by this concept, a seemingly ideal and obvious solution presents itself; decommission the technologies. After all, doing so would completely eliminate the threat of their exploitation, and often whatever new technologies replace older versions will include additional advanced features that benefit the organization in addition to reducing risk. But that recommendation ignores the complicated and controversial context in which legacy technologies exist. The problems created by legacy technologies are, by definition, decades in the making. Their solutions are unlikely to be less so.

B. Priority: Supported Lifetimes

The first step in examining the legacy technologies problem is to realize that the issue extends far beyond the technologies themselves. The risks associated with the use of legacy technologies raise numerous questions. How long should organizations that develop or maintain technologies be required to support them? How long should organizations that use those

[43] Lily Hay Newman, *The Ransomware Meltdown Experts Warned About is Here*, WIRED, Mar. 12, 2017, https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.
[44] *Important Security Notification – Malware Discovered Affecting Triconex Safety Controllers V2.0*, SCHNEIDER ELECTRIC (Jan. 18, 2018), https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Id=9555022209&p_File_Name=SEVD-2017-347-01+Triconex+V2.pdf&p_Reference=SEVD-2017-347-01.
[45] Joshua Cannell, *Tools of the Trade: Exploit Kits*, MALWAREBYTES (Oct. 17, 2016), https://blog.malwarebytes.com/cybercrime/2013/02/tools-of-the-trade-exploit-kits/.

technologies be permitted to reasonably rely on them? Some technologies continue to exhibit perfectly acceptable physical function long after their digital components age—must they still be replaced in their entirety? With this context, referring to these issues as the "legacy technology problem" is reductive and misleading. Instead, the Committee groups these issues under the heading "Supported Lifetimes" and examines them holistically.

If legacy technologies and their associated, intractable Supported Lifetimes questions are to be addressed, the solutions will require creativity, cooperation, and compromise. Technology developers will likely need to provide some guaranteed minimum support lifetime to the products they sell. Users will have to accept and plan for the phasing out of technologies as they get older, whether or not their physical performance is optimal. Beyond that, technology development strategies will likely need to be carefully reexamined. Is it possible, for example, to decouple physical assets from digital ones, so that the obsolescence of one does not necessarily force the obsolescence of the other? Should organizations move to a technology-leasing model, rather than a purchasing model, so that manufacturers may swap old, vulnerable technologies with new, more secure ones with greater ease? These types of Supported Lifetimes questions and more require careful but prompt consideration.

A common thread running through each of the five concepts already discussed is that all require collaboration between diverse and at times competing stakeholders whose technologies and networks are all inextricably linked. An organization on its own may be able to protect a single computer running isolated code, unplugged from the Internet or any other devices, but that computer is unlikely to be particularly useful. The power of connected technologies is just that – connection. By necessity, then, protecting these technologies requires protecting each end of the connection. And that will require partnership.

Committee Product: Supported Lifetimes Request for Information

In April 2018, the Committee on Energy and Commerce released a Request for Information seeking input on how to address legacy technology and related issues in the health care sector. The Committee continues to review the received responses and plans to pursue initiatives based on stakeholder perspectives and feedback.

As part of the Committee's review and continued exploration of RFI responses, the Committee held a staff-level roundtable in October 2018 with stakeholders to discuss how to improve transparency and clarity with regards to legacy technology risks, roles and responsibilities, and strategies.

VII. The Public-Private Partnership Model: Because Cybersecurity Requires a "Whole-of-Society" Approach

A. Concept: Cybersecurity Requires a "Whole-of-Society" Approach

With news of cybersecurity incidents dominating headlines on a regular basis, government agencies, private companies, and individual users have become aware of the cyber threat. Government agencies are required by law to meet certain cybersecurity standards. Organizations are constantly seeking new, innovative solutions to protect their systems and secrets from prying digital eyes. Even consumers now seek out cybersecurity guides for advice on how best to protect themselves from identity thieves, ransomware, fake apps, and more. Too often, though, each of these groups try to manage cybersecurity risks and protect themselves from cyber threats on their own. This is a strategy doomed to fail. True cybersecurity, in this case, takes at least two. And on the Internet, it takes a great many more than that.

Cybersecurity is a shared problem, and not just abstractly. The Internet by its technical design requires at least two devices, connected through wires or spectrum, communicating through standardized networking protocols. Consequently, even if one end of a connection is secure, the other might not be, and that puts both at risk. Multiplied by the millions upon millions of individual connections that make up the Internet, the end result is that the only feasible way to provide any appreciable level of cybersecurity is cooperation. More so than nearly any other shared resource, cybersecurity requires a "whole-of-society" approach, in which individuals and organizations across both the public and private sectors play vital, integral roles.

This reality becomes even more complicated when the composition of the modern Internet is taken into full consideration. At its inception, the Internet was made up primarily of consumer devices like personal computers, servers, and other business-centric devices. Now, it includes smart grid equipment, medical devices, connected cars, critical manufacturing equipment, and much more. Today, diplomatic and military secrets transit the same networks as social media posts and viral videos. Exacerbating the situation further, many of these connected critical infrastructure components are owned and operated by the private sector, which makes public-private partnership in cybersecurity more than just a catchphrase, but essential; without it, many cybersecurity strategies fail altogether.

B. Priority: The Public-Private Partnership Model

In the United States, a Public-Private Partnership model has been established for designated critical infrastructure through Presidential Policy Directive 21 ("PPD-21") and its predecessors.[46] These policies divide critical infrastructure into 16 sectors and assign several roles and responsibilities to public and private sector representatives within each. Three of the most critical roles designated in PPD-21 are: Sector-Specific Agencies (SSAs), responsible for overseeing and guiding their sectors; Sector Coordinating Councils (SCCs), voluntary groups consisting of private sector representatives who work with and represent industry equities to their SSAs; and

[46] *Presidential Policy Directive – Critical Infrastructure Security and Resilience*, THE WHITE HOUSE (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Information Sharing and Analysis Centers (ISACs), official public-private forums for the sharing of information between sector members.

While these roles and acronyms may seem academic, their criticality—especially in cybersecurity—is undeniable. The hybrid nature of the Internet, where data and information critical to national and economic security flow over and through cables, networks, and devices owned and operated by the private sector, requires cooperation on a level that would likely be impossible to achieve without a framework like the one created by PPD-21. Further, while the sophistication of the different sectors varies significantly, the sectors with the strongest SSAs, SCCs, and ISACs are almost universally considered to be the gold standard with regards to cybersecurity capabilities and readiness. Considering that critical infrastructure sectors include those like energy, telecommunications, and information technology—the sectors, in other words, the make the Internet possible—the strengthening of these 16 sectors and the PPD-21 public-private partnership model strengthens the Internet as a whole.

The public-private partnership model is the sixth and final priority identified by the Subcommittee through its cybersecurity work. It builds on and incorporates each of the priorities examined before it, as, after all, the information shared through this model no doubt includes vulnerabilities discovered through coordinated disclosure, context derived from SBOM, details around OSS usage, and supported lifetimes risks and strategies, all shared through the standardized CVE language. It enables connected ecosystem stakeholders to recognize their shared risks and collaborate to protect their shared resources. Most critically, it creates a positive feedback-loop among and between the Subcommittee's six interdependent priorities, and in doing so, increases desperately needed cybersecurity capabilities across society as a whole.

Committee Products: ISAC Roundtable and Public-Private Partnership Hearings (April 2017, June 2017)

Throughout the first half of 2017, the Subcommittee on Oversight and Investigations held several events focused on the public-private partnership model established under PPD-21. In the first, Committee Members and ISAC representatives discussed current ISAC challenges and opportunities. In the subsequent hearings, Members heard testimony from public and private sector representatives from the health care sector to examine how the sector can be made more effective and prepared for modern cyber threats.

VIII. Conclusion

This report represents the culmination of the Subcommittee on Oversight and Investigations' initial efforts to understand, explore, and ultimately address the cybersecurity challenges facing modern society. It recognizes that society today is so heavily dependent and so inextricably intertwined with the Internet and connected technologies that threats to the latter become immediate, serious threats to the former. Not only that, this report recognizes that there is no one "solution" to cybersecurity, but instead discrete yet interdependent policies that together create a holistic and effective strategy for dealing with the realities of modern cyber threats and opportunities.

Each of the concepts and priorities detailed here represent a piece of the broader cybersecurity challenge. Pursuing any one concept-priority pair in isolation will undoubtedly improve society's overall cybersecurity to some degree, but the Subcommittee's work over the past several years has shown that each concept-priority pair feeds off and builds upon its fellows. Further, as highlighted throughout this report, the Subcommittee has not simply identified important, high-level areas for future action, but has already begun to act. The work products associated with each concept and priority represent the Subcommittee's first steps towards implementing the policies it has identified.

More work remains to be done. The Subcommittee remains committed to strengthening the cybersecurity of the stakeholders under its jurisdiction, and will continue to pursue cybersecurity strategies and policies to enable the continued improvement of cybersecurity across society as a whole.

Attachment—Additional Questions for the Record

Subcommittee on Oversight and Investigations
Hearing on
"Stopping Digital Thieves: The Growing Threat of Ransomware"
July 20, 2021

Ms. Kemba Walden, Assistant General Counsel, Microsoft Corporation

The Honorable Frank Pallone, Jr. (D-NJ)

1. The Department of Homeland Security, FBI, and other law enforcement assist with incident response, but I would like to understand whether we are providing victims the variety of resources needed beyond traditional law enforcement, such as technical expertise, recovery strategies, best practices on how to deal with the malicious actors, and other resources that may be required in order to ensure continuity of operations.

    a. What more do you think the U.S. government can and should be providing to victims of ransomware attacks?

Microsoft applauds the U.S. Government's efforts to assist victims of ransomware by providing a "one-stop" whole-of-government resource in the recently launched website: www.stopransomware.gov. This website not only provides helpful information and resources to prevent ransomware attacks and to effectively respond, but it also provides an easy method to report a ransomware attack to the FBI and to CISA. We also appreciate CISA's new assessment tool – Cyber Security Evaluation Tool (CSET): the Ransomware Readiness Assessment (RRA) – which is provided free to the public. Finally, Microsoft applauds NISTs current efforts to establish a guide for managing the risks of ransomware.

The U.S. Government could help the security community better prepare victims to defend against a ransomware attack or recover from a ransomware attack by providing access to reliable, timely, and actionable data and assistance with recovery such as decryption tools.

    b. Do you have any recommendations for actions Congress may take in order to assist in those efforts?

As articulated in the IST Ransomware Task Force Report as Action 4.1.2, a primary opportunity for Congress to assist victims with prevention, remediation, and recovery from a ransomware attack is to create a ransomware response fund to support victims who may refuse to pay ransoms. Without becoming overly prescriptive, Congress may also consider codifying the baseline security measures recommended by NIST or otherwise require local governments and management service providers to adopt limited baseline measures as outlined in Action 3.3 of the Report. Finally, assisting victims with preventing or responding to ransomware attacks depends

on access to baseline data. Microsoft encourages Congress to continue its legislative efforts to require cybersecurity incident reporting. In addition to requiring reporting, that legislation should also (1) require timely and actionable, information sharing with the private sector (2) require the cognizant Department or Agency to explicitly consult with the private sector when developing rules and (3) require CISA to maintain the collected information in a secure manner because such a repository will be a target of exploitation for adversaries.

The Honorable Diana DeGette (D-CO)

1. I am encouraged by the actions the Biden Administration has taken thus far, including the announcement of forthcoming cybersecurity performance goals for critical infrastructure and the formalization of the Industrial Control System Cybersecurity Initiative. Given the critical role the private sector plays in both the operation and security of our critical infrastructure, I would like to hear your take on its response to these threats and to the initiatives and requirements being announced by DHS and other agencies. How do you rate private industry's response thus far and is there anything Congress can be doing to further incentivize the private sector to take these threats seriously?

Microsoft believes a whole-of-nation effort is necessary to secure our cyber ecosystem given that the government and private sector have unique but equally important roles. The President's National Security Memorandum (NSM) on Improving Cybersecurity for Critical Infrastructure Control Systems directing CISA and NIST to develop performance goals is certainly a step in the right direction. Microsoft is eager to learn about those performance goals and would welcome an opportunity to collaborate with CISA in developing those goals.

The IST Ransomware Task Force report outlines at least two potential legislative actions to incentivize the private sector to take ransomware threats seriously. First, as articulated in Action 3.4.4 of the Report, Congress could require regulatory Agencies to consider the private sector's adherence to a risk management framework for ransomware prevention to mitigate an enforcement action. Second, as articulated in Action 3.4.5 of the Report, Congress could offer financial incentives to businesses, including small and medium businesses, that meet certain baseline standards for ransomware preparedness.

The Honorable H. Morgan Griffith (R-VA)

1. The first ransomware attack occurred in 1989, it is not a new threat, but a longstanding cybercrime. The new aspect of ransomware is the use of cryptocurrencies for ransom payments. Can you explain how the role of cryptocurrencies has changed the nature of ransomware attacks?

Ransomware existed before the development of blockchain technology or cryptocurrencies; however, the pseudonymous nature of cryptocurrency as well as its increasing stability and liquidity have allowed ransomware demands to scale. Cybercriminals, in turn, have taken advantage of cryptocurrency's non-traditional financial attributes in a variety of criminal

campaigns, including ransomware attacks. For example, cryptocurrencies allow for the unbanked to perform financial transactions and the decentralized nature of the flow of cryptocurrency results in low administrative costs. Thus, cybercriminals do not need a "bank account" controlled by a central banking system, and the administrative costs associated with receiving large sums of money are far less than if that same volume flowed through a central banking system.

Regardless of where ransomware is deployed, typically the threat actors will demand payment via cryptocurrency through crypto wallets. Although the underlying blockchain technology facilitates transparent cryptocurrency flows, the owners of wallets remain pseudonymous. Nonetheless, the cybercriminal still needs to find on- and off-ramps into the crypto ecosystem. At its core, the criminal actor needs to append the blockchain with a transaction and ultimately find a way to cash out. There are several stakeholders within the cryptocurrency ecosystem that facilitate ransom-related transactions and payments. These intermediaries often exist in jurisdictions with governments that are historically unwilling to cooperate with the United States and others. It's these intermediaries that facilitate the flow of ill-gotten earnings from ransomware. The private sector through civil litigation, and the government through prosecution, regulatory enforcement, and international collaboration, can take coordinated action against intermediaries to disrupt the payment process. Appendix B of the IST Ransomware Task Force report provides a detailed explanation of the cryptocurrency payment process.

The Honorable Gary Palmer (R-AL)

1. Unfortunately, many of these attacks abuse the fact that corporate networks run on Microsoft software. Every ransomware actor seeks to gain "Domain Admin" level control as the first step to being able to adjust "Global Policies" in the Windows Registry to enable the encryption and exfiltration of the entire network. Is there more that Microsoft could be doing to detect and stop unauthorized Powershell commands or changes to Global Policies on a Windows Domain?

The attacks are well-understood by the security community and the mitigations for them have been well documented for many years (https://aka.ms/SPA). The security community keeps up to date on best practices and Microsoft has developed tooling to help customers combat ransomware, several of which are free of charge (https://aka.ms/LAPS). Nonetheless, Microsoft has observed two challenges to organizations adopting these best practices.

(1) *Security is overwhelmed* - Microsoft recognizes that many security teams are overwhelmed, which drives a reactive approach to security, rather than proactively seeking out and protecting against future threats. This challenge is exacerbated by a common leadership misperception that cybersecurity is a technical problem to be solved, which creates pressure to quickly and cheaply "solve" these problems rather than seeing it as an investment in managing an ongoing and evolving risk driven by human intelligence.

(2) *Security does what they know* – Security teams often prioritize and focus on what they know and are familiar with, which is often network technologies and not identity technology (each of which are complex specialized topics in their own right).[1]

This combination leads many organizations to have a fairly poor security posture, particularly around identity technology that may be unfamiliar to many security professionals. Microsoft observed that many organizations do not focus on systems that create, issue, use, and terminate electronic identities proactively, they only address these after they have been specifically targeted and attacked with these techniques.

Microsoft hopes for an increasing culture shift in organizations to bring security into normal business planning and assign security risk where it belongs with other risks (frequently business asset owners). Folding security into the normalized business risk assessment will help ensure that security is considered part of an organization's culture and processes, will allow for adequate resources, and bring in a multi-faceted team, including the security team, to work on this problem at once. Microsoft's guidance (https://aka.ms/cafsecure) and our work with organizations like NIST, The Open Group, and CIS reflect this push.

[1] An Identity Management System is any system that creates, issues, uses, and terminates electronic identities. In other words, an Identity Management System provides lifecycle management for the digital credential sets that represent electronic identities.

Attachment—Additional Questions for the Record

Subcommittee on Oversight and Investigations
Hearing on
"Stopping Digital Thieves: The Growing Threat of Ransomware"
July 20, 2021

Mr. Robert M. Lee, Chief Executive Officer, Dragos

The Honorable Frank Pallone, Jr. (D-NJ)

1. The Department of Homeland Security, FBI, and other law enforcement assist with incident response, but I would like to understand whether we are providing victims the variety of resources needed beyond traditional law enforcement, such as technical expertise, recovery strategies, best practices on how to deal with the malicious actors, and other resources that may be required in order to ensure continuity of operations.

    a. What more do you think the U.S. government can and should be providing to victims of ransomware attacks?
        i. The U.S. government provides valuable expertise in many areas and is especially useful when they provide the community insights on what is important to accomplish and why it is important to accomplish it. Continuing to provide best practice guidance as CISA has done is important government work. However, the technical expertise and the "how" of accomplishing that work already exists in the private sector in larger quantities and deeper expertise than is present in the government, largely because of the government's investments over the years in the community. Additionally, with respect to critical infrastructure, most of it is owned and operated by the private sector, and the responsibility should be on that entity to ensure they are remediated and protected. Incident response, recovery strategies and help, and insights to malicious actors are widely abundant in the private sector. U.S. government resources would best be leveraged in helping Federal and State, Local, and Tribal governments with their systems. Private sector help should be strategic and focused on those that do not have the capability to understand their environment, share with the government, and have a critical impact if they were not functioning (such as in the case of water systems), not tactical security level efforts, such as providing one time assessments and other services that in essence compete with the private sector. The reason being 2 fold:

            1) Tying GDP to incident response is a dangerous endeavor as the scale of the problem often grows quickly beyond one entity being penetrated. In

the case of many cyber attacks, the perpetrator is also attacking multiple other sites.
2) The private sector needs to immediately solve visibility challenges and direct support enabling them to bring on managed services providers is the fastest way to do so, with an eye to organizations critical to the functioning of the US economy or loss or life or both.

b. Do you have any recommendations for actions Congress may take in order to assist in those efforts?
   i. Congress should seek to harmonize the roles and responsibilities between the government and private sector providers. Government agencies should not look to recreate services and offerings that are already available in the private sector but instead look to partner with them to help speed and scale especially where national security priorities exist. As an example, the Department of Energy maintains the Defense Critical Energy Infrastructure list and the Department of Homeland Security maintains the Section 9 critical infrastructure list. Those are the companies that are the most critical to national security and deserve an extra level of support. There is little debate about who is on the list or what needs to be done but finding resources, or "who funds it", is the preeminent debate for any efforts that need performed. Government does not need to provide services and products to those infrastructure members but instead could seek to provide resources to those companies so that they can make the best choices for them in concert with the government to include working with cybersecurity providers who in turn would be able to later take on the responsibility themselves, thus raising the level of information sharing the government and others receive while at the same time immediately remediating threats and vulnerabilities in their environments.

The Honorable Diana DeGette (D-CO)

1. I am encouraged by the actions the Biden Administration has taken thus far, including the announcement of forthcoming cybersecurity performance goals for critical infrastructure and the formalization of the Industrial Control System Cybersecurity Initiative. Given the critical role the private sector plays in both the operation and security of our critical infrastructure, I would like to hear your take on its response to these threats and to the initiatives and requirements being announced by DHS and other agencies. How do you rate private industry's response thus far and is there anything Congress can be doing to further incentivize the private sector to take these threats seriously?

   a. The Biden Administration's efforts with the Industrial Control System Cybersecurity Initiative have so far been very positively seen across the community. The 100 day action plan for the electric sector is one component of that plan that should be used as a blueprint for future efforts. The White House, Department of Energy, and Department of Homeland Security worked together to

determine the "why" and "what" but left the "how" to the electric sector, which resulted in them adding key cybersecurity capability in a rapid fashion to where more than 70 percent of the electric sector now remains protected. It is a feat that should be highlighted as a huge accomplishment given the scale and magnitude of the improvement in such a short period of time. The White House's efforts noted why industrial control system cybersecurity was so important and noted what it wanted the sector to achieve including enhanced threat detection capabilities in industrial control system networks with information sharing being made available to the government. It did not dictate how that would be accomplished though. They instead treated the electric sector as partners and as experts on their infrastructure, which they are. Due to this, through an entirely voluntary effort, the electric sector had over 155 utilities opt into participating by selecting private sector technologies and banding together to provide visibility on the threats and vulnerabilities in these key infrastructure networks to the government. As noted above, we as a community went from 0% monitoring of industrial networks shared to the government to 70% of the electric system being monitored in under 100 days. The private industry's response could not be rated higher. There has been no greater success in cybersecurity historically. When government agencies and regulators are too prescriptive it causes churn and barriers to success. When government agencies speak with one voice as to the "why" and "what" and leave the "how" to the private sector amazing efforts are achievable quickly. Congress can and should further incentivize these efforts by providing resources to those who could not take the efforts voluntarily, providing incentives for those who are obviously acting as good community members, and most importantly amplifying and celebrating the good work that took place. This is one of the most amazing efforts that has ever taken place in the cybersecurity community and yet it remains one of the most unknown as well. While the government did a great job of setting the goals it did not follow up with celebrating the successes or amplifying that there were answers that worked.

The Honorable H. Morgan Griffith (R-VA)

1. Recently, a ransomware attack occurred during the Fourth of July holiday weekend on the Florida information technology company Kaseya. President Biden commented on the impact of the ransomware attack that it inflicted only "minimal damage to U.S. business, but we're still gathering information."[1]

    a. To date, what information is known about the damage caused by this attack?
        i. The ransomware attack impacted managed service providers who provide services mostly to small and medium sized businesses. In many ways it was a very significant attack but because it did not impact many large businesses largely went underreported. Hundreds of companies around the

[1] *Biden says ransomware attack caused 'minimal damage' to U.S. companies*, Reuters (July 6, 2021).

world, rumored to be in the thousands, had to perform incident response and recovery procedures. The highest profile impact was the European supermarket store Co-Op causing hundreds of their locations to have to close temporarily.

b. What type of damage is expected to result from ransomware attacks?
   i. Ransomware attacks on information technology networks deny availability to systems so employees and businesses can not operate and often leak sensitive information to include personal identifiable information. When those attacks occur on operational technology networks such as those found in hospitals, power plants, and gas pipelines they can result in key service disruptions and in extreme cases loss of life scenarios though only close calls have been observed on the topic of human life loss.

c. Kaseya stated that the attack never affected critical infrastructure. How does Kaseya define "critical infrastructure?" Does its definition include transportation networks, electrical power grids, health care facilities, governmental entities, etc.?
   i. It is not known how Kaseya defines critical infrastructure; that term is often abused and defined many ways by many groups. Even the Department of Homeland Security arguably defines that term too broadly over more than 16 sectors. The definition under any argument would include electrical power grids, transportation networks, health care facilities, and government entities. Kaseya only provided software to managed service providers who largely dealt with small and medium sized businesses though. Therefore, it is not likely that critical infrastructure was impacted. However, grocery stores, small and local power providers, and others that would not be deemed national critical infrastructure are still critical infrastructure to those local communities.

The Honorable Michael C. Burgess, M.D. (R-TX)

1. In May, a ransomware attack shut down the Colonial Pipeline company's operations for nearly a week. This act cut nearly half of the southeastern United States' transportation fuels.

   a. How can we make our critical infrastructure more resilient against ransomware attacks?

      i. The Biden Administration launched an Industrial Control System initiative that kicked off with a 100 day action plan across the electric sector. The plan called for companies to voluntarily deploy private sector technologies that provide visibility and detection of threats and vulnerabilities in industrial control system networks. These are the networks that make these critical infrastructure companies critical and are important for the

services and goods they provide as well as protection of human life and the environment. This effort is exactly what right looks like. The plan gave the "why" and the "what" but did not dictate the "how." The electric sector went to 70 percent coverage in OT visibility amongst the industry within that 100 days. It was not prescriptive and left the sector to innovate and choose the best technologies and offerings for them. As the government communicates with a single voice on what is important and why and provides resources for companies to make the right choices including private sector technologies and services we will see a significant increase in resiliency against ransomware attacks and other forms of cyber risk.

b. Is it possible to compartmentalize critical infrastructure so that attacks have smaller impacts?

    i. It is possible. It's always a question of cost. Every critical infrastructure provider knows how to be more resilient, but not how to resource it in a scalable way. It is important to identify what we want the community to be resilient against and then provide mechanisms for those companies to recover the costs that have societal value. In that vein another key area that is foundational to reducing the impact of large scale cyber attacks is visibility with an emphasis on organizations that have Industrial Controls and Operational Technologies.

c. Should infrastructure have physical fail-safes to ensure continued operations during a cyber-attack?

    i. Physical fail-safes are one type of risk reduction method and in many cases can be effective. They are not very scalable though and can be incredibly cost intensive especially in comparison to digital transformation initiatives the companies need to take to modernize their infrastructure to stay competitive in the global economy. Physical fail-safes need to be one tool in the toolbox but as with all the tools cannot be stressed above others without understanding the problem we are trying to solve for.

d. What can individuals do to better protect themselves and their employers from ransomware?

    i. Companies need to implement technology in such a way that individuals that are made to be victims by criminals and state actors do not cripple the company. It is an unrealistic expectation to have employees never click on malicious emails or links. But it is a realistic expectation to design networks and systems in such a way that when adversaries gain access to

networks through such means that defenders can mitigate, detect, and respond to them quickly. As of now, the fastest most efficient way to do this at scale is through working with private sector technologies especially in the Operational Technology layer where the greatest impacts and risks from cyber disruption exist.

The Honorable Gary Palmer (R-AL)

1. Should we be asking the military to do more in these situations? Taking "acts of war" off the table for the moment, how would you advise us to direct our military to bring their awesome powers to bear on the problem of attribution of these hackers and those who control them?

a. The military is in an incredible position to attribute attacks and put additional costs on foreign criminals including taking down their infrastructure overseas. This alone will not be significantly impactful but in concert with an overall strategy from the government including the Department of Justice, can be an effective method of shaping adversary behavior through more directly pursuing the adversary. Given the nature of the threat and the difficulty in accounting for all possibilities, it is not always possible to deter adversary behavior and such actions do not always have immediate benefit for defenders at the victim companies. The number one thing that must be done is to raise visibility and defense of the critical infrastructure of the nation, which in turn will better help the DOD and federal partners to have the information they need to root out the actors responsible. Government resources in this area are an instrument that should be leveraged, but more immediately post Solarwinds and Kaseya and other supply chain related incidents, we should do more with more urgency to resource companies to defend themselves.

2. In your testimony, you mention that most Critical Infrastructure companies are underfunded in the area of Operational Technology and the ability to monitor and detect attacks there. Do you believe that a mid-sized energy company can reach a level of cybersecurity where they can defend themselves from a motivated state-sponsored attacker? Is that even possible?

a. It is possible and we have experience seeing mid-sized energy companies defend themselves against such attacks. It requires investment and often times Operational Technology gets $1/20^{th}$ or less of the resourcing that Information Technology budgets get and those types of gaps will continue to be vulnerable to significant supply chain impacts. When you are not investing in defense, you will lose. But when you invest we have enough examples of what right looks like in the face of strategic adversaries to state that it is doable. Hence the aggressive push to provide small and mid size entities to obtain the resources and tools they need in order to have visibly into their

environments, remediate their active security logging and gaps, and instituting programs that allow them to take action to defend themselves through incident response and sharing information with government agencies (which require a certain level of skill and personnel to effectively do).

3. How much of what you would recommend is "companies doing a better job" and how much is "companies fully engaged in (what you called) collective defense" through information sharing? Should we be "doing better" at identifying and eliminating these attackers through whatever means necessary?

a. Information sharing is often reactive and measured in days or weeks. It is an important topic but lags in the face of targeted threats. Collective defense occurs in real time and ensures that any one company facing a threat can immediately share the appropriate defenses to other companies to be made aware of that threat to everyone. It massively increases the cost on adversaries to be successful. So far there are limited applications of this in practice but one success was the 100 day action plan for the electric sector where over 155 utilities deployed operational technology specific detection technologies and over 90 of them opted into collective defense sharing. This work done with Dragos and NERC's E-ISAC has provided considerable value based on the leadership of the involved government agencies and the voluntary effort and significant leadership shown by the electric companies.

(QFRs) Questions For the Record
for Dr. Christian Dameff MD

House Energy and Commerce Committee
Subcommittee on Oversight and Investigations
Hearing on “Stopping Digital Thieves:
The Growing Threat of Ransomware”

July 20th, 2021

The Honorable Frank Pallone, Jr. (D-NJ)

Question 1: The Department of Homeland Security, FBI, and other law enforcement assist with incident response, but I would like to understand whether we are providing victims the variety of resources needed beyond traditional law enforcement, such as technical expertise, recovery strategies, best practices on how to deal with the malicious actors, and other resources that may be required in order to ensure continuity of operations.

a. What more do you think the U.S. government can and should be providing to victims of ransomware attacks?

b. Do you have any recommendations for actions Congress may take in order to assist in those efforts?

Answer 1: Thank you for this important question. I believe there are numerous avenues to provide assistance to ransomware victims, many of which you have already identified in your question. Contextualizing those potential resources around healthcare ransomware attacks can both clarify the true impact to health systems as well as identify novel opportunities to assist.

Technical expertise - This is critically important as many hospitals and clinics have little or no cybersecurity experience or staff, as cited by the 2017 HHS Healthcare Cybersecurity Task Force report. Technical expertise during an attack can be very helpful in cases where a hospital does not have a previously contracted incident response company or can't handle recovery in house. Technical expertise prior to an attack to aid in identifying vulnerabilities and areas of critical risk can be very effective, and will likely be welcomed by many healthcare delivery organizations especially those with reduced resources such as Critical Access and rural hospitals.

Recovery Strategies - Recovery playbooks and best practices are helpful to organizations that are not already internally preparing for such attacks. Although no data exists on the proportion of hospitals adequately preparing, it is likely that most hospitals in the US do not have any meaningful recovery preparations. Congress can encourage and provide resources to The Office of the Assistant Secretary for Preparedness and Response (ASPR) to improve/expand existing resources and build a more comprehensive set of healthcare specific recovery strategies at all levels of patient care.

Data collection - Without the collection and subsequent analysis of data pertaining to patient harms associated with cyberattacks, we as a nation will be unable to respond appropriately to healthcare ransomware attacks. Congress can support the creation of a National Cyber Harm Registry as a data repository of injury to life and limb resulting from cyberattacks on all sectors. Congress can support mandatory reporting of ransomware attacks, payment details, and impacts to human life for inclusion in this registry.

The Honorable Diana DeGette (D-CO)

Question 2: I am encouraged by the actions the Biden Administration has taken thus far, including the announcement of forthcoming cybersecurity performance goals for critical infrastructure and the formalization of the Industrial Control System Cybersecurity Initiative. Given the critical role the private sector plays in both the operation and security of our critical infrastructure, I would like to hear your take on its response to these threats and to the initiatives and requirements being announced by DHS and other agencies. How do you rate private industry's response thus far and is there anything Congress can be doing to further incentivize the private sector to take these threats seriously?

Answer 2: Thank you for this question. It is clear many hospitals in our nation lack the internal expertise and resources to adequately secure their infrastructure. Preexisting stressors in the healthcare markets and the pandemic response have left many healthcare delivery organizations without the means to protect hospitals, patient data, and clinical care from attack. Congress can take a similar approach to the 2009 HITECH Act signed by President Obama, wherein financial incentives (and delayed financial penalties) were provided to hospitals to catalyze the transition from paper to electronic health records. A similar legislative structure where funds (CMS reimbursement increases) can be earmarked to improve healthcare facility cybersecurity could greatly improve the cybersecurity of the entire healthcare sector. The key to effective change would be ensuring the funds are subject to appropriate oversight and spent on evidence based cybersecurity risk mitigation technologies and security personnel.

The Honorable Michael C. Burgess, M.D. (R-TX)

Question 3: We have witnessed an uptick in ransomware attacks on health systems, especially as our nation responded to the Coronavirus public health emergency. As you highlighted in your testimony, ransomware attacks on health systems are unique and particularly delicate as patients' private and sensitive health data is at risk, in addition to patient access to care.

a. If larger health systems are not equipped to protect against ransomware attacks, how can smaller hospitals and health systems ensure their patients are protected?

Answer 3: Thank you for this question. I am very pessimistic that smaller hospitals will be able to meaningfully improve their cybersecurity and ransomware resilience without a significant infusion of external financial resources. Smaller hospitals tend to be the only care facilities in many rural and underserved communities, and if ransomed would result in significant care disruptions. Many smaller hospitals do not have the budgets for even basic cybersecurity protections such as multi-factor authentication. Cybersecurity workforce shortages are a significant barrier for many large urban healthcare facilities and are exacerbated for rural communities that often are not able to offer competitive wages or living environments.

Please see **Answer 2** for possible Congressional legislative action based on the 2009 HITECH Act to improve healthcare sector cybersecurity protections from ransomware.

Question 4: Dr. Christian Dameff, during the hearing, we discussed that some organizations and hospitals may be fearful of reporting ransomware and other cyber-attacks because they do not want to lose the trust and confidence of their customers or patients.

a. What is the right balance to strike between requiring private entities to report ransomware or other cyber-attacks and maintaining public confidence in an affected entity's care or services?

i. Follow-up: Would a delayed public disclosure, required only after immediate response and recovery efforts, encourage entities to report attacks?

Answer 4: Thank you for this question. Ransomware attacks on hospitals frequently generate significant media and community attention shortly after the attacks occur. This is due in part to the public nature of hospital operations and the number of patients affected by increased wait times, cancelled appointments, and delayed surgeries. In other words, most communities around ransomed hospitals will already know about an attack before any mandatory reporting can be disseminated by government channels. In my opinion, mandatory reporting of ransomware attacks and payments are unlikely to change public perceptions and confidence in a healthcare delivery organization because it is already known and the confidence may already be shaken. Instead, I support the expansion of mandatory reporting elements to include patient care impacts such as morbidity and mortality resulting from a ransomware attack. Furthermore, delayed disclosure may worsen regional response to ransomware attacks due to infected hospitals not sharing critical attack details and attacker methods with other non-infected hospitals so they may search for indications of compromise on their own networks.

b. How can the federal government help better prepare health care organizations to prevent and respond to ransomware attacks?

Answer 5: Please see Answer 1 "Recovery Strategies"

The Honorable Gary Palmer (R-AL)

1. In your testimony you referenced the attack on five large hospitals in the San Diego area. Did anyone die as a result of that attack?

Answer 6: I am not aware of anyone dying as a result of the attack. I am aware of significant effects on my own hospital system as a result of the attack such as significantly increased Emergency Department wait times, patient census, and ambulance arrivals. Unfortunately there is no mandatory reporting of patient harms from cyber attacks such as ransomware. Furthermore most modern hospitals use the electronic health record system to measure care quality and patient safety metrics. These systems and processes are often impacted by the ransomware itself. In other words, ransomware attacks often result in hospitals "flying blind" when it comes to patient safety. This lack of centralized mandatory reporting as well as outages in systems designed to capture patient impacts, forms significant barriers to discovering patient harm.

2. I wanted to thank you for your discussion of the Software Bill of Materials (SBOM) concept. The idea, as I understand it, is that each software package a hospital installs may contain underlying vulnerabilities that the hospital is unaware of because they don't know that the vulnerable software is part of the system they purchased and installed. What could our committee, or the Congress as a whole, do to encourage the adoption of SBOM. Are you asking for Regulation? Or is this something that the FDA who has oversight over medical devices, or HHS who has oversight over compliance with HIPAA, should address through Guidance?

Answer 7: Thank you for this question. Software Bill of Materials (SBOM) is an important component of reducing ransomware risk by increasing the transparency of software components, aiding in identifying which systems may be more vulnerable to attack. SBOM is a great proactive step and, when operationalized, can help hospitals triage which systems to secure first. This committee's 2017 letter to the Department of Health and Human services in support of SBOM was a great first step and resulted in the FDA incorporating it into official guidance under the leadership of Dr. Suzanne Schwartz. To advance SBOM I would ask the committee to consider granting legislative authority to require SBOM instead of relying on voluntary cooperation as detailed in the 2018 Medical Device Safety Action Plan.

Attachment—Additional Questions for the Record

Subcommittee on Oversight and Investigations
Hearing on
"Stopping Digital Thieves: The Growing Threat of Ransomware"
July 20, 2021

Mr. Charles Carmakal, Senior Vice President and Chief Technology Officer, Mandiant

The Honorable Frank Pallone, Jr. (D-NJ)

The Department of Homeland Security, FBI, and other law enforcement assist with incident response, but I would like to understand whether we are providing victims the variety of resources needed beyond traditional law enforcement, such as technical expertise, recovery strategies, best practices on how to deal with the malicious actors, and other resources that may be required in order to ensure continuity of operations.

a. What more do you think the U.S. government can and should be providing to victims of ransomware attacks?

b. Do you have any recommendations for actions Congress may take in order to assist in those efforts?

In general, private sector organizations that require support with responding to cybersecurity incidents engage third-party security vendors. The third-party security vendors often help victim organizations with the following activities:

- Determining the initial attack vector used to access the victim environment
- Determining the scope of the compromise
- Determining what data was accessed or stolen
- Determining who conducted the intrusion
- Containing the incident and eradicating the threat actor
- Recovering and reconstituting the environment
- Providing recommendations to harden the environment to mitigate the risk of future attacks

Mandiant encourages our clients to engage with government entities like the FBI and CISA for support with cybersecurity incidents. Public and private sector collaboration is critical to combatting ransomware and multifaceted extortion operations.

Mandiant recommends the government consider the following actions to help organizations defend their networks and to respond and recover from cyber attacks:

1. Increase efforts to identify, indict, and arrest cyber criminals.
2. Actively share threat intelligence that will enable organizations to defend their networks more quickly and effectively.

3. Continue to provide critical vulnerability information for known and anticipated cyber attack vectors.
4. Continue to disrupt the infrastructure that threat actors use to conduct their intrusions, distribute malware, steal data, communicate with each other, and receive payments.
5. Provide early notifications to victim organizations into which the government becomes aware of intrusion or potential intrusion activity.
6. Continue to develop security best practices, hardening guidelines, and other guidance to inform and educate the private sector and critical infrastructure owners and operators.
7. Consider creating or expanding a panel or other certification process for cyber security vendors like the National Security Cyber Assistance Program previously sponsored by the National Security Agency. This would allow for a rapid response and surge support option to provide to victims who need immediate assistance.

The Honorable Diana DeGette (D-CO)

I am encouraged by the actions the Biden Administration has taken thus far, including the announcement of forthcoming cybersecurity performance goals for critical infrastructure and the formalization of the Industrial Control System Cybersecurity Initiative. Given the critical role the private sector plays in both the operation and security of our critical infrastructure, I would like to hear your take on its response to these threats and to the initiatives and requirements being announced by DHS and other agencies. How do you rate private industry's response thus far and is there anything Congress can be doing to further incentivize the private sector to take these threats seriously?

Mandiant is encouraged by the actions taken by the Biden administration and USG stakeholders. We acknowledge the strides DHS/CISA has made in recent years to encourage information sharing from the private sector and to develop capabilities that provide cyber threat hunting and incident response capabilities to government agencies and critical infrastructure partners. However, CISA's capacity is still limited compared to the relative demand, especially during periods of large-scale or widespread cyber-attacks.

It is too early for Mandiant to comment on private industry's response to the formalization of the Industrial Control System Cybersecurity Initiative. However, we are encouraged by the bipartisan support for the national breach disclosure reporting legislation which will provide incentives, protections and standards for private sector organizations to report significant cyber events to CISA. We believe this type of legislation will further strengthen the focus and priority of cyber defense investments and initiatives across critical infrastructure owners and operators.

The Honorable H. Morgan Griffith (R-VA)

1. Employees warned Kaseya's higher-ups for years about critical security flaws in its software but their concerns were brushed off, former workers told Bloomberg.[1] Several

[1] *Kaseya Failed to Address Security Before Hack, Ex-Employees Say*, Bloomberg (July 10, 2021).

staffers quit in frustration or were fired after repeatedly sounding the alarm about failings in the IT firm's cybersecurity practices. Between 2017 and 2020, employees reported "wide-ranging cybersecurity concerns" to their superiors, claiming that Kaseya used outdated code, implemented poor encryption, and didn't routinely patch its software and servers, Bloomberg reports.[2] Now, Kaseya is at the center of a massive ransomware attack that's ensnared more than 1,000 companies worldwide.[3]

a. Do organizations place more trust in notifications of system vulnerabilities from outside groups, like FireEye-Mandiant, over their own internal cybersecurity departments?

b. If organizations are more inclined to listen to warnings from outside groups, should we continue to outsource cybersecurity monitoring to ensure more companies incorporate their suggestions?

c. How do we encourage organizations from local governments to private companies to seriously consider the severity of cyber threats at the point when they are discovered on their systems, instead of at the time of a ransomware attack?

Mandiant is not in a position to comment on the Kaseya security event.

In general, some organizations prioritize security remediation actions based on concrete threat information provided by trusted third party security companies. For example, Mandiant often provides threat information to organizations, such as security vulnerabilities in their products or evidence of compromise of systems. When we communicate with organizations, we try to quantify the associated business and reputational risk, which enables the organization to quantify the risk and prioritize their response accordingly. Organizations often take action based on the threat information that we provide to them.

Mandiant often obtains evidence of compromise of organizations with which Mandiant has no existing relationship. We attempt to proactively reach out to the impacted organizations and provide them with specific and actionable threat information. Some organizations, especially smaller ones that have no knowledge of Mandiant, don't understand the significance of the information we have provided or don't have technical security personnel that can take action, which sometimes results in disruptive enterprise security incidents.

For many organizations, cyber security is still not a core business function or priority. Like Information Technology, many organizations either outsource their security operations and/or make a best effort to understand cyber risks and prioritize against other business and financial risks. Every cyber attack, like every accident or traditional crime, is predicated on a series of events that, if interrupted, could result in avoidance of the risk. The challenge most organizations

---

[2] *Kaseya's Staff Sounded the Alarm About Security Flaws for Years Before Ransomware Attack*, Gizmodo (July 11, 2021).

[3] REvil Gang Takes Credit for Massive Kaseya Attack and Asks for $70 Million Ransom, Gizmodo (July 5, 2021).

face related to cyber security is that even if they take all reasonable and appropriate measures to defend themselves, they may still experience cyber breach. This is a systemic risk that individual organizations can never fully protect against individually. A collective defense and collective response could be helpful.

2. In October 2020, the U.S. Department of Treasury's Office of Foreign Assets (OFAC) issued an advisory guidance to companies providing services to victims of ransomware attack payments.[4] The advisory warns against payments from U.S. persons with individuals or entities Specially Designated Nationals and Blocked Persons List (SDN List), and other blocked persons and those covered by comprehensive country or region embargoes. The advisory states that a violation by a non-U.S. person, which causes a U.S. person to violate any sanctions, or U.S. persons facilitating actions of a non-U.S. persons in an effort to avoid sanctions regulations, are also prohibited. The advisory states that OFAC may impose civil penalties based on strict liability. In summary, there are potential sanction risks associated with facilitating a ransomware payment. Do you think this OFAC guidance is helpful or hurtful to companies providing services to victims of ransomware attacks?

Mandiant does not advise victim organizations on whether to pay or not pay an extortion demand. Mandiant, however, does seek to help organizations think through a variety of considerations and facts to help make the business make the decision.

Some considerations include:

- Can the organization recover their business without a threat actor-provided decryptor?
- Will a decryptor accelerate the recovery process in addition to recovering through system backups?
- What's the business impact of the disruption? Are human lives at risk? Are there national security consequences?
- Did the threat actor steal sensitive data?
- Does the threat actor still have access to the network? Can they escalate their attack further?
- Is the threat actor sanctioned?

In the future, once organizations attain a higher level of cybersecurity maturity and proficiency, the U.S. government may consider limiting or restricting ransomware payments to reduce these types of attacks. The proliferation of payments is assisting in the continuation of these attacks in the U.S. and globally. In the meantime, Mandiant recommends lawmakers consider legislation that would strengthen law enforcement's response to ransomware criminals and mandate reporting requirements for ransom payments.

---

[4] U.S. Department of the Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Oct. 1, 2020) (home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf).

The OFAC advisory is well-intentioned and designed to minimize payments to criminals. We are aware of sanctioned entities that have not received extortion payments from victim organizations because it was known (or suspected) that the victim would be paying a sanctioned entity.

However, sanctions also present some challenges:

- It's challenging for victim organizations to determine exactly who was responsible for the intrusion and extortion and whether they are sanctioned.
- Sanctioned threat actors may try to create different personas and malware families so that the community is not aware that they are paying a sanctioned entity.
- There are disagreements in the security community as to whether certain personas/groups are sanctioned or affiliated with a sanctioned entity.
- Some victim organizations that are compromised by a sanctioned entity may have no ability to recover their business operations without paying the threat actor for a decryptor, which creates further complexity and stress to the victim organization.
- Many threat actors leverage ransomware-as-a-service (RaaS) wherein many players are involved. Profit is shared between its owners and partners, or affiliates. Attributing all these actors and determining how many degrees of separation are between the recipient of payment and a Specially Designated Nationals and Blocked Persons could be extremely complex and slow.

3. During the hearing, you mentioned that smaller organizations do not have the IT resources to have the necessary level of cyber hygiene to prevent ransomware attacks. Are there ways to incentivize companies to invest in their information technology systems so that they are more resilient against ransomware attacks?

Unfortunately, smaller organizations may struggle to defend their networks for a few reasons:

- There is a general shortage of cybersecurity talent.
- It's hard for smaller organizations to attract and retain strong cybersecurity talent.
- Smaller organizations may not have the funding available to spend on strong cybersecurity capabilities, solutions, and talent.

Mandiant recommends the government take the following actions to help organizations defend their networks:

- Increase efforts to identify, indict, and arrest cyber criminals.
- Actively share threat intelligence that will enable organizations to defend their networks more quickly and effectively.
- Continue to disrupt the infrastructure that threat actors use to conduct their intrusions, distribute malware, steal data, communicate with each other, and receive payments.
- Provide early notifications to victim organizations in which the government becomes aware of intrusion or potential intrusion activity.

Mandiant recommends the government consider the following actions to incentivize organizations to invest in IT modernization and cyber security:

- Tax credits, deductions, or other incentives for appropriate and authorized cyber investments.

- Liability protections or limitations for organizations that can prove cyber security investments or that coordinate with the government for breach disclosures and reporting.
- Make block grants available to critical infrastructure sectors for investments in cyber security technology, program maturity, training, and modernization.
- Additional investments into CISA and State agencies to enhance direct outreach, support, and engagement with critical infrastructure owners and operators.

4. During the hearing, you also mentioned smaller organizations do not know about digital forensics. You mentioned the need for government involvement in the indictments of individuals involved in these attacks, especially for attacks on small businesses.

a. If these smaller organizations do not have the staff and resources to revamp their cyber security hygiene, can you elaborate on the most beneficial support the federal government can provide to small businesses to deter further ransomware attacks?

Please refer to my response above.

The Honorable Michael C. Burgess, M.D. (R-TX)

Many cybersecurity experts do not believe a federal reporting requirement for ransomware and other cyber-attacks is helpful because the victims often do not have a full understanding of the attack until 24 hours or more later, and the federal government can inhibit an effective response by getting involved too early in recovery efforts.

a. Do you believe there should be a federal reporting requirement for cyber-attacks, particularly ransomware attacks? Why or why not?

Mandiant is supportive of a federal cyber incident reporting requirement, assuming requisite protections and incentives.

Any legislation on this matter should take into consideration the evolving cyber threat landscape; the increasingly sophisticated tactics, techniques, and procedures used by adversaries; and lessons learned from existing voluntary information sharing models, as established by the "Cybersecurity Information Sharing Act of 2015." Simply put, while we support a reporting requirement, any reporting framework must be agile and include opportunities for the federal government to pivot or adjust its reporting requirements to keep pace with the threat environment and bad actors. We also believe that any reporting requirement should preserve existing trusted relationships and partnerships, have reasonable yet effective timelines, ensure compliance is non-punitive, and require information to flow back into the community.

The U.S. government should consider a federal incident reporting program that goes beyond voluntary sharing of threat indicators as authorized under the 2015 law – it should also include mandatory disclosure requirements for cyber incidents.

Major tenets of such a program should:

- Safeguard the protection and integrity of electronic and other types of data.
- Ensure confidential sharing.
- Encourage entities to adopt recognized cybersecurity standards and practices with a minimum threshold.
- Provide greater incentives for private sector entities, including liability protections and statutory privilege to not be disclosed in civil litigation (e.g., confidentiality obligations).
- Protect privacy and civil rights.
- Provide outreach and technical assistance to entities that do not have cybersecurity expertise or capabilities.

Mandiant encourages lawmakers to consider harmonizing reporting requirements with existing federal acquisition regulations and standards to provide for a consistent and streamlined regime that simplifies business processes and compliance.

The Honorable Gary Palmer (R-AL)

I am told that FireEye has a wealth of information about cybercrime actors. One of my constituents tells me that they have a list of 3,300 companies that have had their private data – information about them, their corporate secrets, and their clients and customers – put on a ransomware leak site and been told that if they didn't pay a ransom, even more documents would be leaked. Mr. Reiner's group shared in their report that 199 cryptocurrency addresses received 80% of all the payments that were made for ransomware, and that just 25 addresses accounted for 46% of all ransom payments.

a. With the skills FireEye and Mandiant have in attribution, would you say that you could tell us who those people are? Do you know the names of the people behind these attacks? And if you do, what would you recommend we do to disrupt them?

The most prevalent cyber threat today is ransomware and multifaceted extortion. Threat actors that engage in multifaceted extortion steal data from victim environments, disrupt business operations by deploying encryptors that lock organizations out of their data, and publicly shame victims by posting their stolen on "victim shaming" websites.

There are varying degrees of threat actor attribution. Depending on the nature of the activity, and our involvement in the detection or response to the activity we may have different levels of visibility, and therefore varying levels of information to assist in attribution. While attribution is always a goal, we most often do not identify who the human is behind the keyboard, but attribute the activity to a cluster, cyber-crime group, or nation state. In most cases, we leverage a variety of information to include the tactics, techniques, or procedures (TTPs) leveraged by the actor, their target/victim organizations, technical information, along with assessed motivation to make a broad assessment of the cluster of activity or organized group believed to be behind the activity. Attributing the "group" based on the characteristics is still beneficial so organizations can determine their threat landscape and prepare to defend against that type of actor or group and the TTPs they use.

Reiner IST QFR: 7/20 Subcommittee on Oversight and Investigations Hearing

1. Context: The Honorable Frank Pallone, Jr. (D-NJ) says "The Department of Homeland Security, FBI, and other law enforcement assist with incident response, but I would like to understand whether we are providing victims the variety of resources needed beyond traditional law enforcement, such as technical expertise, recovery strategies, best practices on how to deal with the malicious actors, and other resources that may be required in order to ensure continuity of operations."

Question:

A. What more do you think the U.S. government can and should be providing to victims of ransomware attacks?

Answer:

In order to improve organizations' ability to respond to ransomware attacks more effectively, the U.S. government should increase the resources and information available to ransomware victims. This could include establishing Cyber Response and Recovery Funds and potentially other ransomware emergency response authorities, which could help cover business continuity and remediation costs for organizations attacked with ransomware; establishing rapid response teams to assist critical organizations to restore functionality quickly; providing liability protection for business interruptions caused by refusing to pay ransoms; and improved awareness of legal requirements prior to payment. Together, these and other strategies will decrease the number of organizations that feel compelled or trapped into paying ransoms.

Question:

B. Do you have any recommendations for actions Congress may take in order to assist in those efforts?

Answer:

Congress should consider the development of a special cyber-disaster authority that would enable federal agencies to assist victim organizations with additional resources in the event of a significant ransomware attack. Congress should also consider requiring organizations to take certain actions before paying a ransom, including reporting the attack and payment request to the appropriate government agencies. Congress should broaden the Cybersecurity Information Sharing Act of 2015 to allow victims to report ransomware attacks anonymously, except in the case that a victim is required to disclose the attack under existing privacy laws. Additionally, Congress could increase funding for agencies to respond to ransomware-related inquiries so they can meet demand, through a combination of additional staff and improved technology. Treasury will likely need additional resources to meet demands from the private sector, as will the SEC, IRS, DHS, DOJ/FBI, Commerce, HHS, and others. For example, even if an

organization asks OFAC whether a particular recipient falls into a prohibited category or seeks a payment license, OFAC is not resourced to provide answers rapidly enough for a company facing tight extortion timelines. The recommended funding could include, for example, creation of a concierge or ombudsman service at the Department of Homeland Security's CISA for private-sector entities seeking guidance on ransomware-related questions. Under this approach, CISA would not be responsible for interpreting another agency's guidance, but it would direct the inquiry to the correct office within the Federal government. This assistance would facilitate better decision-making within the private sector.

2. Context: The Honorable Diana DeGette (D-CO) says "I am encouraged by the actions the Biden Administration has taken thus far, including the announcement of forthcoming cybersecurity performance goals for critical infrastructure and the formalization of the Industrial Control System Cybersecurity Initiative. Given the critical role the private sector plays in both the operation and security of our critical infrastructure, I would like to hear your take on its response to these threats and to the initiatives and requirements being announced by DHS and other agencies."

Question:

A. **How do you rate private industry's response thus far and is there anything Congress can be doing to further incentivize the private sector to take these threats seriously?**

Answer:

Both industry and government have historically underinvested in cybersecurity. The private sector will almost certainly require more incentives - both carrots and sticks - to take these threats more seriously. Some private sectors actors do all they can within their power to take the right steps - and even some of them still get hit. Others, however, simply choose not to take the steps they know they should, banking on the lack of consequences for doing so. They are playing a game of roulette when it comes to ransomware, and it puts our public health nad national security at risk. The Ransomware Task Force recommended that the U.S. government consider offering conditional access to grant funding or utilizing tax breaks as financial incentives for organizations to adopt secure IT services. Investigating the alleviation of fines for certain critical infrastructure entities may also incentivize a more serious approach to these threats. For some small- and medium-sized businesses with constrained budgets, a higher level approach incentivizing Managed Service Providers (MSPs) to develop their cybersecurity capabilities may provide more benefits - to include potentially mandating baseline security practices that MSPs must adopt. Finally, it would both incentivize greater protective measures - while also building up the requisite body of data needed to defeat the threat - to mandate the reporting of ransomware payments to the federal government *before* making such a payment, requiring organizations to review alternatives before making payments, and requiring organizations to conduct a cost-benefit assessment prior to making a ransom payments.

3. Context: The Honorable Gary Palmer (R-AL) says: "Thank you for your leadership in directing the IST Ransomware Task Force and the excellent report that you produced. I feel that many of your recommendations helped to shape the StopRansomware.gov website and the excellent educational materials provided there. However, there is one area that your task force was bold enough to address that is entirely missing from the StopRansomware website, and that is the area of Cyber Insurance and Ransomware Payments. I can't find any guidance at StopRansomware.gov that tells me How To Pay a Ransom and Where To Report a Payment."

Question:

A. **Does the Task Force agree that failing to discuss this and give guidance will make the problem go away?**

Answer:

Understanding federal guidance for ransomware payments is critical to stemming the spread of ransomware. Private industry needs clear understanding and guidance on federal regulations and reporting requirements after a ransomware attack. Without that, the response from industry will likely continue to be misaligned, which enables criminals to take advantage of the seams between our public and private organizations. It would both incentivize greater protective measures in industry, while also building up the requisite body of data needed to defeat the threat, to mandate the reporting of ransomware payments to the federal government *before* making such a payment, requiring organizations to review alternatives before making payments, and requiring organizations to conduct a cost-benefit assessment prior to making a ransom payments. One of additional recommendations of the Task Force was the development of clear decision frameworks for entities that have been hit by a ransomware attack - to include decision-trees for Executives. These are tools/kits that can be developed together between CISA and the private sector, with help from non-profit organizations like IST, GCA, CTA, and others.

Question:

B. **We know that the best way to track payments is through more information about payments that have been made. Could you speak to that point – what specifically are you recommending to "disrupt the system that facilitates the payment of ransom?" And should reporting those ransom payments be mandatory?**

Answer:

Ransomware groups use cryptocurrencies to facilitate victim payments and skirt regulatory enforcement. To counter the spread of ransomware, the U.S. government needs to more effectively interact within the ransomware financial process - what we called the "ransomware kill chain". This can come in the form of developing new levers for sharing cryptocurrency payment indicators; requiring cryptocurrency exchanges, crypto kiosks, and over-the-counter trading "desks" to comply with existing laws; and centralizing expertise in cryptocurrency seizure. Additionally, the government should consider placing an increased emphasis on cyber

insurance by improving civil recovery and asset forfeiture processes as well as establishing an insurance-sector consortium to share ransomware loss data and accelerate best practices. Interacting with the cryptocurrency market and emphasizing cyber insurance might more efficiently disrupt the system that facilitates ransom payments. Additionally, disruption of criminal activity within the cryptocurrency ecosystem requires an order-of-magnitude better understanding of the ways via which these criminal actors abuse these technologies in order to better pinpoint the chokepoints where their illicit transactions occur - whether at the beginning, before payments are disbursed, as the funds traverse the exchanges and tumblers, or where they cash back out into fiat. Identification of the opportunities for disruption must come first if we are to be able to more effectively do so.

That, in part, would be greatly assisted if ransomware payments were to be reported to a central node for aggregation and analysis, to create a broader more comprehensive picture of the “kill chain”. Congress should pass regulations that require organizations to disclose a ransomware attack and payment request to federal entities before paying a ransom. Hiding the ransomware attack, or otherwise covering up the loss of data, only contributes to the culture that enables cyber criminals to take advantage of industry and government organizations.