This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

{York Stenographic Services, Inc.}

RPTS ALDINGER

HIF062.020

UNDERSTANDING THE CYBER THREAT AND IMPLICATIONS FOR THE 21ST CENTURY ECONOMY

TUESDAY, MARCH 3, 2015

House of Representatives,

Subcommittee on Oversight and Investigations

Committee on Energy and Commerce

Washington, D.C.

The subcommittee met, pursuant to call, at 2:30 p.m., in Room 2322 of the Rayburn House Office Building, Hon. Tim Murphy [Chairman of the Subcommittee] presiding.

Members present: Representatives Murphy, McKinley, Burgess, Blackburn, Bucshon, Brooks, Mullin, Hudson, Collins, Cramer, DeGette, Clarke, Kennedy, Green, and Pallone (ex officio).

Staff present: Charlotte Baker, Deputy Communications Director; Leighton Brown, Press Assistant; Melissa Froelich, Counsel, Commerce, Manufacturing, and Trade; Brittany Havens, Legislative Clerk; Charles Ingebretson, Chief Counsel, Oversight and Investigations; Paul Nagle, Chief Counsel, Commerce, Manufacturing, and Trade; John Ohly, Professional Staff, Oversight and Investigations; Chris Santini, Policy Coordinator, Oversight and Investigations; Peter Spencer, Professional Staff Member, Oversight; Jessica Wilkerson, Legislative Clerk; Christine Brennan, Democratic Press Secretary; Jeff Carroll, Democratic Staff Director; Chris Knauer, Democratic Oversight Staff Director; Una Lee, Democratic Chief Oversight Counsel; and Elizabeth Letter, Democratic Professional Staff Member.

|

Mr. {Murphy.} Well, good afternoon. I now convene this hearing of the Oversight and Investigations Subcommittee, entitled Understanding the Cyber Threat and Implications for the 21st Century Economy. This is the first in a series of hearings by this committee focused on cyberspace, the Internet, and the challenges and opportunities that they present for the 21st century economy.

These are big, important issues, so it is imperative that we establish a clear understanding of the issues we face. So today, we are going to do something a little different. We are not here to examine a specific cybersecurity incident, policy issue or legislative proposal. Today, we are going to take a step back and explore some fundamental questions with our experts. Such things as what is the breadth and depth of the cyber threats? Is it something that can be solved? And what does this mean for the future?

In 1969, computers at four universities connected to the ARPANET, thus providing--thus proving a computer networking concept that evolved into what we now know as the Internet.

Since its inception, the Internet has been an open platform, designed to facilitate the transfer of data and information between remotely located computing resources. It doesn't discriminate against any network or device, nor the transmission of the data. It is merely a conduit for information. This open architecture, end-to-end system design is what makes the Internet such a benefit to society. It provides endless possibilities for innovation. It gives any individual with an Internet connection an opportunity to share their opinion with the world, and to access a nearly infinite amount of information. It has revolutionized the way we conduct business, interact socially, learn and consume information, be it true or false. As a result, the Internet fostered widespread development and adoption of computing and communications technologies, collectively known as information technologies. Today, we depend on these technologies for everything from social interaction to home security, the operation of critical services like power plants and the electric grid. This integration of the Internet and information technologies into nearly every aspect of modern life has created the virtual world commonly known as cyberspace.

The Internet's strength, however, is also its weakness. It is by nature an open system with many interconnections, creating multiple opportunities for disruption. Likewise, information technologies are inherently complex systems, increasing the probability of ingrained vulnerabilities. As a result, the same technological and cultural factors that facilitate real-time global interaction, rapid innovation and freedom of expression empower malicious actors to thrive and create risk in cyberspace.

The challenge arises from the fact that cyberspace creates an asymmetric imbalance that strongly favors malicious actors. Anyone, from an individual to a nation state, can target a victim halfway around the world at minimal cost and with little risk of being caught. Because the cost of failure and the consequences of crime are minimal, the threat evolves rapidly. In contrast, the costs of defense, as well as potential consequences, are significant. Because this asymmetric threat is rooted in the fundamental structure of the Internet and information technology, there is no way to solve cybersecurity without undermining the benefits of the cyberspace. There is no silver bullet or technological solution. While we certainly can do more improve the security of cyberspace, these decisions require a thoughtful cost benefit analysis. How will a potential security measure affect the cost or convenience of a product? How will it affect the pace of innovation? What will it mean for privacy or civil liberties? Cyberspace is no longer a place that we visit; it is the place where we live. Ten years ago, smartphones were a novelty, in fact, the iPhone didn't even exist. Today, mobile devices serve as a credit card, they can track our health, unlock our homes, start our vehicles, and document our daily travels. A pacifier can monitor your infant's temperature and send that information directly to your computer or mobile device. Through what is known as the Internet of things, we have connected kitchen appliances, you can start dinner from the office, check social media accounts from your grill, or know when you are low on milk.

Cyberspace is, and will increasingly be, the economic engine of the 21st century economy, and at the same time as the Internet and information technology becomes increasingly entwined in our daily routines, cyberspace becomes a limitless and adaptive attack surface. The security challenges will be more diverse and harder predict, and the consequences will be more severe. We may not be able to secure cyberspace, but it is our collective responsibility to understand the threat in order to minimize its effect on our privacy, civil liberties, national security and economic prosperity. We should embrace this unique opportunity this hearing presents, not to debate data breach legislation or other specific policy issues, but to listen.

We are privileged to have an impressive panel of experts who can help us understand the challenges of cybersecurity in context. In particular, I want to recognize Dr. Shannon from Carnegie Mellon University in Pittsburgh, home to the Nation's first computer emergency response team. The Pittsburgh region boasts some of the Nation's foremost experts in the field of cybersecurity, and I am pleased to have one of those experts, Dr. Shannon, joining us here today.

[The prepared statement of Mr. Murphy follows:]

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

*************** COMMITTEE INSERT ***************

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

Mr. {Murphy.} I will now recognize the ranking member of the O&I Subcommittee, Ms. DeGette of Colorado, for 5 minutes.

Ms. {DeGette.} Thank you, Mr. Chairman. I am glad we are having the time to do a deep dive into this important topic. O&I has a long history of exploring issues related to cybersecurity. Over the years, we have had hearings on cybersecurity risks. We have passed bipartisan legislation to promote security and resiliency for critical infrastructure systems. We have also examined in detail both cyber attacks and vulnerabilities within many of the sectors under this committee's jurisdiction. I hope that this hearing--series of hearings will help us have additional productive conversations about how both to understand the cyber risks and how to respond to them.

Information systems connected to the Internet are integral to the operation of our economy. While this interconnectedness is essential, the vulnerabilities that it can pose, pose serious challenges. Every day, the Internet is under attack by those with malicious intent. In the last few years, cyber attacks on federal agencies and also no private entities have skyrocketed. Every week it seems, there is a new series of headlines about cyber attacks and vulnerabilities in our system. Last week, for example, Uber revealed a breach of its driver database that had gone unreported for months. Anthem reported that millions of people who were not its customers could be victims of cyber attacks on their systems. Last year, we heard of attacks on Home Depot, Target, and JP Morgan Chase that involved the personal information of tens of millions of Americans.

So this past year alone has been a stark reminder that all industries are vulnerable, and neither the private sector or government is safe from cyber attacks. These attacks are becoming more and more frequent, and more and more sophisticated. I am personally concerned about how the loss of personally identifiable information is affecting American consumers. It is starting to appear that there are 2 types of these Americans. Number one, people whose data has been subject to a breach, and number two, people whose data will be subject to a breach. That seems to be how it is breaking out.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

So I look forward to hearing from our witnesses today about the cybersecurity landscape. I have a couple of questions. Number one, what are the threats that we now face, and number two, what are our biggest vulnerabilities. Also, I want to hear what we are doing now, and what we can improve in the future. What are the existing standards in both the government and private industry for keeping personal information safe, and providing notification when there is a breach. How can we make sure that both the public and private sectors are using their expertise to ensure that cybersecurity measures are appropriately tailored to address the specific needs in the different sectors. More fundamentally, what is the appropriate role of government and of the private sector in securing the systems, managing cyber risks and assessing cyber threats. How do we promote the optimal level of cooperation and information sharing within this division of labor. Unfortunately, this is a problem that doesn't have an immediate or a fissile solution.

So I am hoping that our witnesses throughout the hearings can advise us on how we can make the right strategic investments in cybersecurity in both the short and long-term.

They are all smiling because they know what an impossible task this is. But, you know, this is a problem that exists far beyond our Nation's borders. We should be thinking about how we can ensure international cooperation to protect against cyber threats around the world. I understand we need to make substantial changes in the way we think about cybersecurity. This is not a problem that we have the tools to deal with immediately. And I do want to hear from our witnesses about that today, but even while rethink our approach to cybersecurity and make necessary long-term investments, I want to know what we can do right now to protect consumers and their personal information. If data breaches have become inevitable, we need to think about how to make that data unusable once it is stolen, and that seems to be a short-term key. I want to hear from the witnesses about creative solutions in the post-breach environment. On the battlefield, a strategy for preventing the enemy from successfully using your technology against you is to render it useless if it falls into the wrong hands. I think we need to figure out ways to do this now with certain types of consumer information if it is stolen.

As Chairman Murphy said, this is just the first in a series to explore cyber threats in a variety of sectors. I want to thank the witnesses, and I look forward to our continued work.

I yield back.

[The prepared statement of Ms. DeGette follows:]

*************** COMMITTEE INSERT ***************

|

Mr. {Murphy.} Gentlelady yields back.

Now recognize the vice chair of the full committee, Mrs. Blackburn of Tennessee, for 5 minutes.

Mrs. {Blackburn.} Thank you, Mr. Chairman, and thank you for the attention to this issue. And witnesses, we appreciate that you are here as we begin to think through this process.

Cyberspace is really a place where a lot of our information now resides. It is not just something that we click onto and off of, but it is a place of residence for what I term our virtual you, which is you and all of your information. And interestingly enough, and the chairman noted the end-to-end open architecture of the system, the backbone that permits this, and you do have that original platform, that openness, which makes it what it is, and makes it a successful information service. So now, we have all of these incursions, and the malware and the spyware and the bots, and this and that, and some of these are embedded in hardware, some are there via software, and we are looking at an increased number of these attacks on our critical infrastructure every day.

Now, the chairman mentioned a little bit about the Internet of things, or as I like to say, the Internet of everything. And we know that by the end of this decade, Sysco says we are going to have 50 billion, 50 billion devices that are connected to the Internet. That is a lot of vulnerabilities. So as we look at the steps that need to be taken for privacy and for data security, we welcome your expertise and your insights, and we thank you for helping us think forward on this.

And I yield at this time to Dr. Burgess.

[The prepared statement of Mrs. Blackburn follows:]

*************** COMMITTEE INSERT ***************

|

Mr. {Burgess.} I thank the vice chairwoman for yielding. Chairman Murphy, thank you for having the subcommittee have this hearing on reviewing the current state of cybersecurity. It is an issue that is vital to the future of commerce and our economy. Developing a strong grasp of the engineering and technical realities underpinning computer networks, and what that means for business models is an integral part of understanding cybersecurity.

I do want to acknowledge, Chairman Murphy, your comments that this is not a data breach hearing. The Subcommittee on Commerce, Manufacturing and Trade is working to finalize legislation establishing a data security requirement, and a single set of breach notification rules for entities under the Federal Trade Committee's jurisdiction. But that is just one piece of the broader puzzle, and I look forward to the broader discussion of cybersecurity at today's hearing.

Thank you, Mr. Chairman. I will yield back the balance of the time.

[The prepared statement of Mr. Burgess follows:]

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

*************** COMMITTEE INSERT ***************

|

Mr. {Murphy.} Thank the gentleman.

And now I turn to Mr. Pallone for 5 minutes.

Mr. {Pallone.} Thank you, Mr. Chairman.

I want to borrow the words of one of our witnesses here today. Dr. Shannon, in summarizing the cybersecurity landscape, says this in his written testimony, and I quote, ``Currently there is no manner in which an entity, public or private, can be fully protected without simultaneously destroying its value. Today, there are either the--there are neither the tools, technology, nor resources to stop all serious cyber attacks and allow for efficient function of electronic commerce. We simply do not yet know how to do both of these together, which makes enabling continued technology research an innovation essential.'' and that is the end of his quote.

Dr. Shannon, you captured perfectly the problems we face in this area, and the challenges and responding. This committee has a long history on cybersecurity issues, and I look forward to this series of hearings as we continue to examine this area.

Unfortunately, our ability to protect against cyber attacks while improving still appears to lack what is needed to prevent these intrusions. We are seeing more frequent and more severe attacks in both the public and private sectors. In just the past few years, millions of Americans have had their information compromised in data breaches. At the same time, our dependence on the Internet and interconnected information systems has only increased. Disconnecting from the Internet is not an option for a vast majority of individuals and companies alike.

The private sector seems to be no better at preventing attacks than the Federal Government. In the last year or so, we have seen breach after breach where attacks are placing Americans' personal data at risk. Attacks on Target, JP Morgan, Home Depot, Sony, and now Anthem have all underscored this fact. And these attacks illustrate that even the biggest companies with considerable resources at their disposal are not immune to these intrusions. We must also face the reality that it is much cheaper for the attackers to infiltrate than it is for us to protect and respond, and unfortunately, there is no one solution at this time to guarantee that stored information will remain secure. But we can't ignore cybersecurity until we have a solution. Instead, we need to find ways to manage the problem, and I hope this series of hearings can bring out some creative solutions on how to do just that.

In addition, we need to start thinking about post-breach protections, particularly as it relates to consumers. Clearly finding ways to strengthen existing systems is necessary, but we also need to make it harder for thieves to use stolen data after breaches occur. It is not enough for companies to simply offer a free year of credit monitoring as an answer. Rather, we need to explore ways to make consumer data less useful if it falls into the hands of the bad guys.

So, Mr. Chairman, coming up with effective solutions to these problems will be a long process, but I applaud you and our ranking member, Ms. DeGette, for starting this series of hearings, and I look forward to working with you to better protect our institutions, companies, and citizens.

I yield the remaining of my time to the gentlewoman from New York, Ms. Clarke.

[The prepared statement of Mr. Pallone follows:]

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

*************** COMMITTEE INSERT ***************

|

Ms. {Clarke.} I would first like to thank both our Chairman Murphy and Ranking Member DeGette for having this hearing, and I would like to thank the gentleman from New Jersey, the ranking member of our full committee, Mr. Pallone, for yielding me time.

I thank our witnesses for lending their expertise, time and talent to today's Oversight and Investigations hearing.

As you know, I was on the Homeland Security Committee for the past 8 years, and of those 8 years, I was ranking member of the Cybersecurity and Critical Infrastructure Subcommittee for 4 years, and chairwoman for 2 years. Needless to say, this issue is extremely important to me, but more importantly, to our Nation. There is no doubt that we face a challenge of incredible proportions when it comes to cyber threats. Comprehensive and effective cybersecurity policy has always been a complicated endeavor, but in the face of technological--of the technological landscape that is constantly evolving and developing new mechanisms that threaten the integrity of our Nation's virtual presence, we stand in unchartered territory as we try to shape a government and corporate response that is effective, adaptable, and a step ahead of any threat we may encounter.

We hear about a new breach in security or impending cyber threat almost daily, so it is inarguable that the time to set our House in order has come and it is now. The security of our Nation's cyber infrastructure and our response to cyber threats is not a partisan issue. We have to work together; democrats and republicans, government and private industry, academics and public advocates, to not only protect the privacy of our citizens, but also identify and respond to security threats. Ultimately, however, it is the expertise of today's witnesses, and many others across the cyber community, that will allow us to act in the best interests of our Nation.

I look forward to listening to and learning from what today's witnesses have to share with us.

I yield back to Ranking Member DeGette.

[The prepared statement of Ms. Clarke follows:]

*************** COMMITTEE INSERT ***************

|

Mr. {DeGette.} I yield back.

Mr. {Murphy.} All right, thank you. Thank you.

We are expecting votes from between 2:15 and 2:45, so we will move quickly through these questions. 2:45, 3:15? All right, 2:45, 3:15, so we should have plenty of time.

So now let me introduce the witnesses on the panel for today's hearing. First, Dr. Herbert Lin, Senior Research Scholar for Cyber Policy and Security at the Center for the International--for International Security and Cooperation, a Senior Fellow at the Hoover Institute in Stanford University, his research relates broadly to policy-related dimensions of cybersecurity and cyberspace, and particularly interested in knowledgeable--and is knowledgeable about the use of offensive operations, cyberspace, especially instruments of national policy. Welcome here, Dr. Lin.

Next, Dr. Richard Bejtlich. I say that right?

Mr. {Bejtlich.} Yes, sir.

Mr. {Murphy.} Good. Is the chief security strategist at FireEye, Incorporated, and was Mandiant's chief security officer when FireEye was acquired by Mandiant in 2013. In this role, he empowers policymakers, international leaders, global customers, and concerned citizens to understand and mitigate digital risks through strategic security programs.

Our third panelist is Dr. Greg Shannon, Chief Scientist for the CERT Program at the Software Engineering Institute at the Carnegie Mellon University. In this role, he is responsible for working with the director and SEI leadership to plan, develop and implement research strategies, initiatives and programs that further the mission of CERT and SEI, as well as developing, conveying and executing innovative ideas for the Nation's cybersecurity research agendas. In addition, he was recently named chair of the Institute of Electrical and Electronics Engineers Cybersecurity Initiative.

I will now swear in the witnesses. As you all are aware, the committee is holding an investigative hearing, and when doing so, has the practice of taking testimony under oath. Do any of you have objections to testifying under oath? Seeing no objections, the chair then advises you that under the rules of the House and the rules of the committee, you are entitled to be advised by counsel. Do any of you desire to be advised by counsel during your testimony today? And they have all indicated no. In that case, would you please rise and raise your right hand, I will sear you in.

[Witnesses sworn.]

Mr. {Murphy.} Thank you. All the witnesses answered in the affirmative. So you are now under oath and subject to the penalties set forth in Title XVIII, section 1001 of the United States Code. We will recognize you each for a 5-minute summary. The rules are press the button on the mike, pull it close to you. Watch for the red light, that means your time is up.

Dr. Lin, you may begin.

|

^TESTIMONY OF HERBERT LIN, SENIOR RESEARCH SCHOLAR, CENTER FOR THE INTERNATIONAL SECURITY AND COOPERATION, SENIOR FELLOW, HOOVER INSTITUTION, HARVARD UNIVERSITY; RICHARD BEJTLICH, CHIEF SECURITY STRATEGIST, FIREEYE, INCORPORATED; AND GREGORY SHANNON, CHIEF SCIENTIST, CERT PROGRAM, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY

|

^TESTIMONY OF HERBERT LIN

} Mr. {Lin.} Mr. Chairman, members of the subcommittee, thanks for the opportunity to testify. Testimony today is personal, although my professional work informs it.

Let me start with two definitions. Cyberspace is computers, smartphones, the Internet, stuff with computers inside them. It is also the information inside these things, and our dependence on all of this is growing.

Here is a definition of cybersecurity that--with words like negative impact and bad guy. What is important here is that the words are--definitions of these words are policy matters, and also cybersecurity isn't just technology.

Economics, psychology, organizations, they all matter because they help to shape user behavior, which affects cybersecurity.

On security, a computer in a sealed metal box, which is the--there is supposed to be a computer inside that one on the left. There is one on mine. And it is a sealed metal box, so I guess you can't see it. There is--that is perfectly secure, but it is useless. Okay. The one on the right is useful but potentially insecure because--it is useful because you get information in and out of it. You only want good data to get into it. That requires a judgment about what counts as good, and such judgments are fallible.

Here is a network of nodes that represents the Internet. At each node that--there is another network or a computer. The Internet is designed with just one function really; to transport data from A to B without regard for what it means. Usefulness of the Internet comes from the computers that sit at the nodes, and this principle is what has really enabled the Internet to grow so quickly in the past. But if you believe in this principle, it also means that the network in the middle doesn't handle security. Many people want to put security in the middle, but that would violate this basic principle that has driven Internet growth and innovation, and also the change wouldn't entirely solve the cybersecurity problem. There are some exceptions to this story--to this description, but they don't really change the basic story.

Complexity is the enemy of cybersecurity. What we want from our computers requires complex systems. We put components into a system. When the system is complex enough, nobody understands the system very well, and so the system, in fact, may not be secure. And here is an example of complexity at work. You have done this before, from a browser you go into a--you type in the URL, like EnergyCommerce.House.gov, and then in less than a second the Commerce site--the E&C Commerce site appears. Okay. This is what is going on behind the scene. It is not worth going over each of these elements, I don't have time for it either, but at every one of these boxes, an adversary could interfere with your Web experience.

Also, adversaries adapt, and here is an example from safecracking. Good guys don't get the last move here. When we put money in wooden boxes to protect them, robbers use axes. When we used metal safes to stop them, they drilled wedges between the door and the safe. When you put in step doors, they poured in nitroglycerine, and so on. And we still haven't entirely stopped bank robberies.

The result of this is the--is this chart. Over time, we get better at cybersecurity, that is the bottom line, but the top line, how much we depend on cyberspace and, therefore, how much the threat that we face has grown even faster, and that gap, therefore, is growing. The defenses of today would be good against the threats of, you know, 10 years ago, but the threat has changed too.

This leads to conclusion one, which is that cybersecurity is a never-ending battle. You will not find a decisive solution forever, and so you have to find ways to manage it at an acceptable cost. This really leads to two questions; why bother with cybersecurity at all, and how can we manage the problem? On the why bother, here are some reasons. You deal with the unsophisticated threats, you make yourself less vulnerable so the other guy--so the bad guys go after the next guy rather than you. You give the--you can give the bad guy less time to do his dirty work, and you give--you help out law enforcement focus on the harder cases. Okay. Second, why is it so hard to solve this as a policy problem? Well, the reason is that we want cybersecurity, but we want other good things as well. We want rapid innovation, and it is always faster to do something without attention to security. We want convenience on cybersecurity. It mostly gets in your way. How often have you been at a computer that you couldn't get on because you forgot a password? There is also interoperability, which means sometimes you can't fix a known security problem because you are afraid of damaging existing programs. And we want privacy for us but not the bad guys. That means when we try to collect data on the bad guys, sometimes we collect data inadvertently on the good guys. And the tradeoff is that we don't know how much we are willing to--how much inadvertent collection we should tolerate to gain security. Tradeoffs are unavoidable, and that means it makes consensus hard to reach. How do you do better? Well, you can do--part one is you reduce the gap between the average and the best, and part two is you reduce the gap between the best and what you actually need.

So here is my summary of this, which is all in your--

this is a one-page summary. And this referenced, from which much of this testimony is drawn, I would like to incorporate that into the record of the hearing, if I may. And I think it has been distributed to members. So that is it. Thank you.

[The prepared statement of Mr. Lin follows:]

*************** INSERT 1 ***************

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

Mr. {Murphy.} Thank you.

Now our next witness, go ahead, 5 minutes.

|

^TESTIMONY OF RICHARD BEJTLICH

} Mr. {Bejtlich.} Chairman Murphy, Ranking Member DeGette, members of the committee, thank you for the opportunity to testify. I am Richard Bejtlich, Chief Security Strategist at FireEye. Today I will discuss briefly digital threats, how to think about risk, and some strategies to address these challenges.

So first, who is the threat? We have discovered and countered nation-state actors from China, Russia, Iran, North Korea, Syria, and other countries. The Chinese and Russians tend to hack for commercial and geopolitical gain. The Iranians and North Koreans extend these activities to include disruption via denied service and sabotage using destructive malware. Activity from Syria relates to the regional civil war, and sometimes affects Western news outlets and other victims. Eastern Europe continues to be a source of criminal operations, and we worry about the conflict between Ukraine and Russia extending into the digital realm.

I began by saying who is the threat, and that brings

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

about threat attribution. Threat attribution, or identifying responsibility for a breach, depends on the political stakes surrounding an incident. For high-profile intrusions such as those in the news over the last few months, attribution has been a priority. National technical means, law enforcement, and counterintelligence can pierce anonymity. Some elements of the private sector have the right experience and evidence to assist with this process. So attribution is possible, but it is a function of what is at stake.

So who is being breached? In March of 2014, the Washington Post reported that in 2013, federal agents, most often the FBI, notified more than 3,000 U.S. companies that their computer systems had been hacked. This count represents clearly identified breach victims. Many were likely compromised more than once. How do victims learn of a breach? In 70 percent of the cases, someone else, likely the FBI, tells a victim about a serious compromise. Only 30 percent of the time, the victims learn of the intrusions on their own. The median amount of time for when an intruder first compromises a victim to when the victim learns of a breach is currently 205 days. This means that, unfortunately

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

for nearly 7 months after gaining initial entry, intruders are free to roam within victim networks.

Well, what is the answer? Before talking about solutions to digital risk, we need to define it. Always ask risk of what. Are we talking about the risk of a teenager committing suicide due to cyberbullying, or the risk of a retiree's 401(k) being emptied due to electronic theft, or the risk of a week-long power outage due to state-sponsored attack? Step one is to define the risk, and step two is to measure progress by combining means and ways to achieve defined ends.

To measure success, I recommend that a security team track the number of intrusions that occur every year, and you will see this in the FISMA report that was just released yesterday, although, honestly, it seemed buried in the report. So you want to count the number of intrusions per year, but more importantly, you want to measure the amount of time from when the intruder first gets into the enterprise to when someone notices, and when from someone notices to when you kick them out. And these are the metrics that I don't see recorded too often.

It is also important to think in terms of how to define risk, and security professionals, like the ones at this table, tend to think in terms of threat vulnerability and cost. And we use a pseudo equation where risk is the product of threat vulnerability and cost. We are not trying to calculate a number; just show that, as you influence each one of these factors, you either raise risk or lower risk.

So I think in general, there is a lot of attention paid to vulnerability, you know, the vulnerability in a computer and an iPhone, that sort of thing, but we need to spend a lot of time as well on the threat and the cost. Law enforcement and counterintelligence are the primary means by which you can mitigate the threat. In an editorial for Brookings that I wrote, I asked what makes more sense; expecting two billion Internet users to adequately secure their personal information, or reducing the threat posed by the roughly 100 top tier malware authors? So that is the threat side.

On the cost side, we need to think of ways to reduce the cost of dealing with a security breach, not only for companies but also for consumers. So we are seeing this in a couple of different areas. One step in place is the tokenization of payment card system data where you replace a credit card number with a string of numbers in its place. A second step would be eliminating the value of the social security number to identity thieves. I recommend reading the Electronic Privacy Information Center suggestions on effective social security legislation for some policy changes.

In brief, defenders win when they stop intruders from achieving their objective. It is ideal to stop the adversary from entering the network, but that goal is increasingly difficult. I recommend you quickly detect the intrusion, respond to contain the adversary, and then kick them out.

And finally, we must appreciate that the time to find and remove intruders is now. There is no point in planning for future theoretical breaches. If you were to hire me to be your chief security officer, the very first step I would take would be to hunt for intruders already in the network.

I look forward to your questions.

[The prepared statement of Mr. Bejtlich follows:]

*************** INSERT 2 ***************

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

Mr. {Murphy.} Thank you.

Now, Dr. Shannon, you are recognized for 5 minutes.

|

^TESTIMONY OF GREGORY SHANNON

} Mr. {Shannon.} Thank you. Thank you, Chairman Murphy, Ranking Member DeGette, and distinguished subcommittee members. I am honored to testify to you before today on cyber threats and implications for the 21st century. I am Greg Shannon, the Chief Scientist for the CERT Division at the Software Engineering Institute, which is a DoD, FFRDC, operated by Carnegie Mellon University.

To sustain and expand our economy, consumers and businesses need to trust the cyber infrastructure ecosystem upon which commerce and innovation now depend. Those ecosystems must also thwart capable adversaries who seek to execute economy-disrupting cyber attacks. Today, in cyberspace, as noted before, there is no manner of--there is no manner in which an entity, public or private, can fully protect itself without simultaneously eroding its own value. There are neither existing technologies nor any amount of money that would stop all serious cyber attacks, and allow for the efficient function of electronic commerce. We simply do not yet know how to do both.

As technologists, what are we to do? In the short term, we need to push for more and better measurement of outcomes, as noted earlier. Security successes as well as breaches. Collectively, if most everyone practices good cyber hygiene, we are unlikely to be undone by the weakest link, however, you cannot expect everyone to adopt a new idea without proof of efficacy, especially when implementing--when implementation isn't free. The opportunity of measuring outcomes directly applies to two promising risk management frameworks, the NIST Cybersecurity Framework, and the Department of Energy's Cybersecurity Capability Maturity Model. Both of these frameworks are being measured for efficacy and will soon produce data telling us which practices matter. We need that feedback. The best-secured organizations continuously monitor how their performance correlates with their practices. Without meaningful feedback, the state-of-the-art cannot improve.

In the medium-term, we need to improve access to data, specifically for security and privacy innovation. Cyber solutions are only as good as the data they are created from.

And currently, researchers and developers have limited access to data, resulting in subpar solutions and slower innovation. Sadly, just this morning, I listened to research results based on 15-year-old synthetic dataset with known serious limitations. Fortunately, I have also personally seen security innovation accelerated when scientists and engineers have access to good data; i.e., when modeling insider threats. If we can determine which subsets are essential for combatting those cyber threat, then less data would need to be shared and thereby possibly moderating privacy concerns.

In the long-term, we need coordinate national--in the long-term, we need a coordinate national strategy to sustainably build trust and thwart our cyber adversaries. For example, we need to eliminate the possibility that a single weakness can threaten the economy. Consider--considering computational and human energy as a barrier, it is possible to create and operate a strategically advanced cyber infrastructure that would require adversaries to expend exceptional energy in order to pose serious cyber threats to our economy. Today, it takes only modest computing and human energy to find and execute economy-threatening attacks, creating an environment that favors the adversary by orders of magnitude. Given the energy we already expend on security defenses, we can optimize our energy investments to create a more robust defense, and simultaneously apply recent research results and new technologies that makes the computational cost of finding and executing a compromise exceptionally high. In June, a DIMACS- and IEEE-sponsored workshop at Carnegie Mellon will discuss the technical foundations of this strategy. If we can create and operate a strategically advanced cyber infrastructure that requires adversaries to expend astronomical amounts of energy to find and execute economy-threatening attacks, then energy becomes the currency in which one traffics to protect or attack commerce around the world. Ultimately, access to energy could become a deterrent to economy-threatening cyber attacks.

Over the last 45 years, we have created the Internet and a modern evolving 21st century economy. Paradoxically, our own innovation and collective success have created today's trust and resiliency challenges. Nevertheless, I am optimistic that over the next 45 years, we will make our 21st century economy fully trustworthy and resilient.

Thank you.

[The prepared statement of Mr. Shannon follows:]

*************** INSERT 3 ***************

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

|

Mr. {Murphy.} I thank all the panelists for their testimony. And now I am going to recognize myself for 5 minutes for questions.

So we have heard a lot about the nature of cyber threats and cybersecurity. We heard it is very asymmetric, it favors those who wish to misbehave in cyberspace, and defenders have to spend a great deal of time and money and very complex systems all at once. So this is a question for any of you. Can this asymmetric imbalance be corrected to favor defenders instead of attackers? Any of you want to weigh in on that? Dr. Lin?

Mr. {Lin.} Sure. I don't know if it will ever be able to favor the defense, but you can certainly make it a lot harder for the attackers. I mean I think there is no question about that. I think all of my colleagues here basically said that, that we can do a much better job than we are doing now. So we--for example, there are known technologies and known procedures, and so on, that we can deploy that will increase security, but we just don't use them, for a variety of reasons.

Mr. {Murphy.} Anyone else want to weigh in on that before I go on to my next question?

Mr. {Bejtlich.} Sir, just briefly, I could give you a tactical answer. The iPhone is an example of a more security technology that people love, and the reason is is Apple has an App Store that it polices closely; it is very difficult to get something malicious in there. So when you look at vulnerabilities on phones, there is a fraction of what is on Android as compared to Apple because Android is much more open, Apple is more closed. Now, if you want to be able to run whatever you want on your iPhone, you lose that, but it is more secure.

At a more strategic level though, we have to realize that it does take effort for intruders to get their objectives done. It is not like a silver bullet attack where they press a button and the end of the world happens. We have seen intruders take days, weeks, even months, to get to the data that they need. So sometimes it is a question of your perspective as well.

Mr. {Murphy.} So let me jump onto that and, Dr. Shannon, maybe you could follow this. So are there opportunities that we can increase the cost of doing--for the bad guys in doing business, so we can do some technical things, which you just described Apple does, but are there other things, perhaps legal or technological solutions that we can take steps on?

Mr. {Shannon.} At the technological level, as I point out in my written testimony, there are some long-term research and development opportunities. Technology that is coming to fruition is becoming practical. Essentially, it makes the computations similar to--if you were to break the computation, it would be similar to breaking encryption. And so the goal is to make it so that database queries, remote computation in the Cloud, is just as difficult of disrupting and compromising as it is encryption. And these typically are encryption-based technologies, and hence, my comments about high energy, that the amount of energy it would take an adversary to compromise those systems, or to find a way to thwart those systems, would be comparable to breaking encryption.

Mr. {Murphy.} Let me jump onto a different part here. So let us talk about the Internet of things. We are going to have all these things controlling parts of our lives, from running our dishwasher to opening and closing garage doors, turning the heat on and off, tracking where we are, finding where our kids are, is it possible to keep pace with these threats, and let alone increase the cost of attackers, as we are talking about here, to malicious actors? Dr. Lin, can you weigh in on that?

Mr. {Lin.} Is it possible to do better than they are likely to do? Sure, but the problem is that getting stuff out first to market is a very--is a time--sorry, is an effort-intensive thing, and you don't want to put in effort to focus on security before you can get to market. And the--it is--they do this for perfectly reasonable economic reasons, but it is very hard to get people to focus on cybersecurity in the absence of some sort of mandate before they have gotten the product out.

Mr. {Murphy.} So that becomes something we can work on in Congress.

Mr. {Bejtlich.} Sir, there is an opportunity here, and that is, with traditional security, you have been relying on a person to secure their computer. Someone who is not an expert, someone who is just a user. With a vendor, you have a centralized place where you could apply some pressure of a variety of means to get them to have their act together as far as, for example, securing my refrigerator. There is nothing I can really do to my refrigerator. It is not like my PC. So you can apply some pressure on the vendor to make sure that they have their act together.

Mr. {Murphy.} Okay. Let me ask one more question in my brief amount of time. Dr. Shannon, you referred to the importance of trust and trustworthy things. We want to be able to trust so many things that we are involved, with interstate commerce, with energy, telecommunications, all the things within the jurisdiction of this committee. So let me go back here, if we were to redesign, if the Internet was starting up today, how would we design it differently to take care to have that trust, still have something that is accessible, but is secure?

Mr. {Shannon.} A big part of it is to look at the ecosystem that actually creates the components for the environment, the software, the hardware. Part of the challenge is that there is a very large shared data--shared base, and those systems are fundamentally--are what in--are--have been created in an insecure manner. And so it provides ample adversary--opportunities for adversaries to work their way into, and they really create the, you know, the opportunity to steal the private data and to bring down a banking site, or whatever. So it is--that is where the real opportunity is if you designed it properly from the beginning.

Mr. {Murphy.} Thank you.

Ms. DeGette, you are recognized for 5 minutes. My time is up.

Ms. {DeGette.} Thanks, Mr. Chairman. As I mentioned in my opening statement, the Federal Government and also private businesses have been targeted by cybercriminals, and I talked about Target, I talked about Home Depot, JP Morgan Chase, the health insurer Anthem. From the Federal Government side, also we have had substantial attacks. In July of 2013, there were hackers who stole social security numbers and other information from over 100,000 employees at the Department of Energy, for just one example.

So, Mr. Bejtlich, I heard a number that seems high, but it--but if you add all these together, the number I heard is that over 100 million Americans could potentially be at risk from these cyber attacks. Does that number sound plausible to you?

Mr. {Bejtlich.} Yes, just given the Anthem hack alone, close to 80 million records include social security numbers. So you get to 100 million pretty quickly.

Ms. {DeGette.} Yeah. And so typically what companies do is they tell people they can have a year of free credit monitoring if they have had their data stolen. Do you think that is sufficient, or do we need to explore additional remedies?

Mr. {Bejtlich.} I concur that that is not sufficient. I don't want to blame the victims in this case, but I was personally affected by the Anthem hack, as was my family, so the ability to recover from that doesn't exist in our system. It does exist for something like a credit card number. We have all had credit cards stolen and not suffered that much damage, but it is a whole other ballgame when you are dealing with social security numbers and other data.

Ms. {DeGette.} And what--do you have some ideas what we could do, aside from giving people free credit monitoring?

Mr. {Bejtlich.} Well, I think the first thing is to go through an exercise that says what data exists, and what happens when that data is an intruder's hands, in a criminal's hands, what can be done with that data. And if there is no friction from having the data to opening a new line of credit, getting a mortgage, whatever it is, we need to introduce some friction there, whether it is some type of physical agreement that has to be passed through the mail, or something that makes it easier--or makes it more difficult for the intruder, and allows the victim to know something is going on here and not just wait until you have gotten an adverse credit report.

Ms. {DeGette.} Yeah, and is that something that you think Congress should be involved in?

Mr. {Bejtlich.} It is not my place to say what you should do, I believe, but I do think we need more industries thinking in terms of what happens to data post-breach, because I agree with your statement that we are either post-breach or pre-breach for most organizations.

Ms. {DeGette.} Right. Right, and I mean what you are saying is, if somebody hasn't had their data stolen, it is likely that they will have their data stolen, correct?

Mr. {Bejtlich.} Some data, yes, of some type. As we have all heard, more of our data is out there.

Ms. {DeGette.} So do you think it might make sense to let consumers lock their credit down with credit agencies? Do you think that might be one solution?

Mr. {Bejtlich.} Ma'am, I am not an expert in the credit system, although my understanding of the current system is that that is not an easy proposition. I think we may need to look at something that would allow that to happen, for example, I have young children, there is no reason for them to have any credit taken out in their name until there is some type of formal approval.

Ms. {DeGette.} And that was my next question is that would be one thing that would be easy to do. Is there some other way we can protect children from early identity theft?

Mr. {Bejtlich.} I do know that the act of credit monitoring, and this has come out through the disclosures that I have received as a victim of some of these cases, the act of trying to do credit monitoring, or to do a credit

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

check for a child makes them more likely, or makes it easier for an intruder to use their identity. So that seems like a situation that needs to be changed.

Ms. {DeGette.} So I have one more question for anybody who wants to answer it. My staff here recently--you met with Sysco?

{Voice.} Citigroup.

Ms. {DeGette.} Citigroup? Citigroup. And they did a test on their own systems, and what they found was that these breaches were actually interactive. So they could breach one machine and then it would actually morph when it went to the next machine. It would actually change. And so that is the sophistication they are getting now. What can we do to start trying to protect against those sorts of breaches? Anybody.

Mr. {Shannon.} Well, the cyber threat analysis is a key part of that in terms of being able to track an adversary, and track their TTPs, their tools, techniques and procedures, so that, you know, you can--once you realize there is a breach, you realize what the next step for that adversary might be. And it is about using the cyber intelligence--

Ms. {DeGette.} Do we have the ability to do that now?

Mr. {Shannon.} There are commercial organizations that actually do that. I believe that is part of what you guys do for your bread and butter.

Mr. {Lin.} The problem that you have described is what is known as a perimeter defense, and once you have breached the perimeter of an organization, you can do anything you want inside. Most organizations believe that they just erect a big enough of perimeter on the outside and they are safe, but they are not. And so organizations have to learn to practice and operate as though they had already been penetrated, and getting them to do that is a tough thing to do.

Ms. {DeGette.} Thank you.

Thank you, Mr. Chairman.

Mr. {Murphy.} Thank you. They have called a vote, early as it is. So what we are going to--no, I guess it is on-time. So what we are going to do is take a break. Don't go far because as soon as Members come back--I know Mr. McKinley ran so he will beat me back, and I know--so we can just continue on as soon as we get back here and have a chair. So don't wonder far, we will be right back. Thank

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

you.

[Recess.]

Mr. {McKinley.} [Presiding] We--now that we have some balance here, we can continue. And so we will continue the hearing. I believe--who--

{Voice.} You are up.

Mr. {McKinley.} I am the next questioner. So thank you very much for your patience on that, and now that we have a balanced panel, we can continue.

I am trying to follow some of the hyperbolae that goes on in Washington often about cybersecurity, terrorism, climate change, everyone has their--I was interested in the last few days the--Lee Hamilton with the 9/11 Commission came out and said the biggest threat facing America is not ISIS, but cyber attacks. The FBI director said it is the greatest threat to national security. And the director of national intelligence, Clapper, said that the online assaults undermine U.S. national security.

Do you agree that that is one of our biggest threats that we--if not the biggest threat that we face is the issue we are talking about here today? Each of you, just kind of a yes or no.

Mr. {Shannon.} It is clearly a big threat. I think given that many other threats will result in direct loss of life, I think in the cyber arena, you know, it is pretty hard to make a compelling case based on experience to date. Is the potential there? Absolutely, but it is not, you know, thank God, it hasn't manifested itself on a regular basis like it has in other areas.

Mr. {Bejtlich.} Sir, I tend to think in terms of the actor, so cyber is a vector and a target, but at the end of the day, there is someone behind it, whether we are talking about the Russians or someone else, and I think that is why DNI Clapper elevated the Russian threat as above the China threat right now. The Russian threat is seen as more acute. It is linked to geopolitical events. It could be seen as a potential response to activity that is going on in Ukraine, whereas the activity from China is more steeling secrets and it is more of a chronic issue. So I tend to think in terms of who is it that we worry about, and less the way that they are going to do it.

Mr. {McKinley.} Okay. Dr. Lin?

Mr. {Lin.} I would agree with both of those two--with my two colleagues here, that the--it is one of the biggest threats. I would have a hard time thinking that it is worse than a nuclear weapon going off--

Mr. {McKinley.} Sure.

Mr. {Lin.} --improvised nuclear weapon going off, you know. I--

Mr. {McKinley.} But if I could just continue with that because if it is a threat, and I think of small businesses, the Mildred Schmidt who lives next door to you, lives next door to me, she has no idea that she has been hacked, and they are getting into her information. I think if small companies--like my company--former company, that we did business with the Federal Government, and people could hack into my computer, and by virtue of that, get into the Federal computers. So we know it is out there. But what I did like was, I guess it was, Mr. Bejtlich, your--something in your testimony, you said it may take 7 months before we know they are in there. This thing is just so broad, are we spending too much attention trying to focus on prevention and keeping actors out, or is there a better way to address this, because we seem like we may be shortening the time frame. Is this the best thing we should be doing?

Mr. {Shannon.} Yeah, that is a--certainly a concern. I mean we want to be able to build better infrastructure. You know, I am part of the Software Engineering Institute, part of our goal is to develop better methodologies for creating software assurance, and part of the challenges, as we were discussing during the break, is that, you know, the libraries that are out there that developers use, there are 15 million C programmers in the world, and they all go to places like GitHub and other open-source repositories to get a lot of their code, or to look at the code to see how it is done. And those codes haven't been hardened.

Mr. {McKinley.} And--but, Doctor, how do we deal with the small businesses that can't afford to build in all the software protection? How do we deal with that?

Mr. {Shannon.} You want to provide a national asset where they can go to and get that as a given. If you provide repositories where there are already pre-hardened components, the developers would be using that they, you know, if they are going to actually do some development. That--

Mr. {McKinley.} Well--

Mr. {Shannon.} --is part of the benefit of the IOS--ecosystems like IOS. Developers go there and they already know that they are using components that have been tested and approved.

Mr. {McKinley.} Tested, okay.

Mr. {Bejtlich.} I think insurance--

Mr. {McKinley.} Mr. Bejtlich, it looks like you--okay, you wanted to say something?

Mr. {Bejtlich.} Sorry, sir. I think insurance is also going to play a much greater role here. It is important to think in terms of--cyber isn't--it is unique in some senses but in other cases it is not. So there are plenty of other real-world elements we can bring to bear on this, and insurance would be one of them. There is no reason for your small business to go out of business because of a hack if you can buy a policy that would help you recover from that.

Mr. {McKinley.} Dr. Lin?

Mr. {Lin.} And I would say that there is a role for a single one-point stop--one-point, one-stop shopping for help if you have a computer security problem, that it would be helpful if your small business owner could know who to call. The problem with something like that is that it is a very individual--the--what is going on in this person's computer is a very individual thing and it is going to be--there are going to be problems in responding, but at least people should be able to get help, and right now there isn't any good way to do that.

Mr. {McKinley.} Okay. So my time has run out on that, but thank you very much for that. I hope we can pursue that a little bit further.

Now, who do we have next? Our chairman is back.

Mrs. Blackburn, 5 minutes.

Mrs. {Blackburn.} Thank you, sir. I appreciate that, and I appreciate the patience that you all are showing by hanging with us as we are back and forth to the floor in different things.

Let me pick up right where Mr. McKinley left off. And as I said in my opening, that when you look at cyberspace, it is a place now where our information actually resides. Our virtual you lives there. And what we hear from constituents is how do I protect this, why can't they do something to make this safer in. As my colleagues have heard me repeatedly say, there is nothing that women hate more than a peeping Tom, and they don't like them looking at their networks and their pictures and their photos and their passwords, and things of this nature, and the way they feel that violation is something that we hear about. So what I would like to hear from you all, and, Dr. Lin, you just alluded to this, you know, when you said people want to know where to get help. So what do you see as a group of best practices that should be there for companies and their virtual space, whether they are a click business or a brick and mortar business, and then talk a little bit about B to C, and how businesses deal with consumers and inform and educate them as to what they are doing to make that virtual marketplace, and prohibit and incursions in cyber.

So let us start and just go down the line. We have 3 minutes, and I would like about 30 seconds from each of you on it.

Mr. {Lin.} One thing--sorry. One thing that businesses can do with respect to the consumers is to be more transparent about their--the ways in which they protect data and are willing to use it. Most companies--many companies are less than fully transparent in the ways in which they--

Mrs. {Blackburn.} So how they are crunching the data--

Mr. {Lin.} That is correct.

Mrs. {Blackburn.} --and what they are pulling from it, and get that--go ahead and get permissions on the frontend.

Mr. {Lin.} Well, that is right, and to be fully disclosive about what you are--what they are actually going to--

Mrs. {Blackburn.} Okay.

Mr. {Lin.} --what they could do with it.

Mrs. {Blackburn.} Okay.

Mr. {Bejtlich.} I would like to hear about the steps they take to protect data. Lots of times you hear, well, we can't talk about that because it will show too much to the adversary. I would--really don't believe that. I would like to know, for example, that my bank has an incident response team, that they exercise at regular intervals, they are staffed with these people that you may have heard of in the press. That, to me, would give me some comfort that they are taking that seriously.

Mrs. {Blackburn.} Okay.

Mr. {Shannon.} I think, actually, the marketplace has an opportunity to make this decision. I have seen some startups coming out that are promoting security higher to the users. And so if the company can indicate we are making things maybe a little more inconvenient for you, but it also makes it extremely more inconvenient for the hacker.

Mrs. {Blackburn.} Dr. Shannon, why do you think companies have not done that?

Mr. {Shannon.} Well, because it is--they see it as an impediment to their profit loss, they want to retain users, they want to make their services easy to use, and so they haven't been forced to, essentially, admit that--

Mrs. {Blackburn.} But then their customers become very angry--

Mr. {Shannon.} That is correct.

Mrs. {Blackburn.} --when there is an incursion.

Let me--and it is Mr. Bejtlich, right? Am I saying that right?

Mr. {Bejtlich.} Bejtlich. Thank you.

Mrs. {Blackburn.} Bejtlich. Okay. I am close. That works. Okay, let us see, Mandiant's M-trends 2015 report, something that caught my eye there was that you could have a--some malicious activity and a malicious actor on your system for 205 days. That was the average before it was discovered. And I found this so interesting because we had a company in my district there around Nashville that had a major breach this year, and the amount of time that the--that actor was on the system and then moved the information to a different system before they exported it and left--

Mr. {Bejtlich.} Right.

Mrs. {Blackburn.} --the country with it. So is there--do you concur with that 205 days, or is there a different--I know you all do a lot of remediation work, so--

Mr. {Bejtlich.} Right. That is absolutely our number. That is based--

Mrs. {Blackburn.} Okay.

Mr. {Bejtlich.} --on our consulting work from last year. It is down from the year before which--we are moving in the right direction, but 7 months is still way too high.

Mrs. {Blackburn.} I agree with you.

And with that, I yield back. Thank you, Mr. Chairman.

Mr. {Murphy.} Now recognize Mr. Collins for 5 minutes.

Mr. {Collins.} Thank you, Mr. Chairman. I want to thank the--you for coming in today to testify. The last Congress, I was the subcommittee chairman of Health and Technology on small business. I had a hearing on cybersecurity, and maybe to--I don't think we can say this too often to small business, there is a threat to them, there is a threat to their very existence. And so maybe today we could just, Mr. Bejtlich, continue this discussion more as a PR to small business.

What I found was most small businesses are naïve to the threat. They operate under, it won't happen to me. They are going to go after Target or Citibank or someone, they are not coming after my small business, which, in fact, and maybe you could expand on this, I think many of these folks see small businesses as the easy way into bigger companies. If they are a supplier to General Electric, if they are a supplier to a big company, an attacker can get into that small supplier and work through their connection to get into--through the supply chain, so to speak. But what we found was the staggering percentage of businesses that are out of business within 12 months of a data breach. It threatens their very existence because as, and you can expand on this really as well, if someone gets into their employee information, they have to provide credit insurance for that employee for some extended period of time, and that it out of their pocket, but also if a big corporation finds that that supplier was the access point, guess what, that big company is not going to buy from that supplier. If the customers find out, as we have seen, their data has been breached, they are not going to shop at that store.

So we are trying to say, you know, and alert to small business--most of them don't have security policies, cybersecurity policies, they are sloppy with passwords, and they are just begging to be the target. So I don't know if you would want to just expand on a little bit of what I just said to--the warning to small businesses--

Mr. {Bejtlich.} Sure.

Mr. {Collins.} --it can happen to you, and if it does--

Mr. {Bejtlich.} I totally agree. The thing you should do as a small business is to say, first, what do we have that somebody else wants. That includes data as well as the money itself. I mean we have seen cases where ACH transfers of money just straight out the door and that is it, but it is also what data do we have, and what would be the consequences if that data were stolen. And then you have to go through the exercises of, well, how would that happen? Does it only take, say, an email from the CEO that looks fake, that authorizes the money to be transferred out of our account. We have seen that happen as well. And once you figure out, okay, what do we have, what could happen to it, now you want to introduce friction into that system that would not make it easy for an intruder to carry that out. It could be something as simple as you have an email address, and if that single email is taken over by a bad guy, they could reset all your passwords, they could take over your bank account, so you want to make sure what are we doing to protect that.

It--a lot of this is just sort of thinking this through, just as you would, you know, estate planning or that sort of thing.

Mr. {Collins.} You would think it is commonsense, but it is not where you are worried about getting an order, getting it shipped, paying your bills, and it is just the thought that it can't happen to me. We have found so many companies, they don't even have a basic policy on passwords where many people use the same password at 100 different Internet sites. That way, they only have to remember one. But then these folks will take--they will get into that one, and then in a very short period of time, they can bounce that password into any number of other sites, and low and behold it hits. And the next thing you know, they are into that small business. They don't know it, as you pointed out. They are either taking their money, but worse yet, they are stealing customer information, IP, they are stealing--they are accessing the vendors and other customers. So to me, it is--it starts with, you have to understand it can happen to you, number two, have a basic policy. You know, we even published, when I was on the Small Business Committee, some dos and don'ts and the like, and, you know, just as an alert to small businesses who think it is only big companies. So you are confirming that it is--small businesses are very much a target of the cyber--

Mr. {Bejtlich.} Yes, sir. And I would add, talk to your bank and find out what can a bank do to tell you if something suspicious is happening. What is their policy, could they give you an alert of some kind, could you ask for a phone verification, an in-person verification. Put this friction in place so that it is not easy for a bad guy to steal all your money.

Mr. {Collins.} Yeah, because they are out there.

Mr. {Bejtlich.} That is right.

Mr. {Collins.} Thank you, Mr. Chairman. I yield back.

Mr. {Murphy.} Gentleman yields back.

Now recognize Mr. Green of Texas for 5 minutes.

Mr. {Green.} Thank you, Mr. Chairman. And I want to thank our witnesses. I apologize for goings and comings of the members because we had votes today. I guess for this hearing, the good news is that Homeland Security will stay in business.

But as we all know, last month, with the health insurer, Anthem, disclosed a significant breach of up to 80 million of its customers and employees. It is my understanding that the breach does not involve any credit or banking information, nor that there is evidence at this time that any medical information was obtained. While I appreciate the steps

Anthem has taken to make it right with their customers, I do have some general questions on cybersecurity in the healthcare sector.

Dr. Shannon, is there any reason to believe that the healthcare industry is more vulnerable than other sectors to these type of data breaches, and do we have any reason to believe that the health sector is underinvesting in cybersecurity protections?

Mr. {Shannon.} No, I think with the HIPAA Act that that has pretty much incented them to making investments.

Mr. {Green.} Which--that was in 1996, so--

Mr. {Shannon.} Well, and that is really what has driven a lot of the cybersecurity thinking in that sector for the last 15 years. So I think similar to other organizations, they are investing. Fortunately, there is--they are part--they are typically large organizations, so they often have resources and can, you know, it is not quite the small business challenge that--

Mr. {Green.} Yeah.

Mr. {Shannon.} --we just heard.

Mr. {Green.} Okay. Mr. Bejtlich?

Mr. {Bejtlich.} Healthcare is definitely a target. They are not as well defended as the top tier. The top tier tends to be the defense companies and the financial sector. So yeah, there is definitely an issue there.

Mr. {Green.} Okay. Mr. Bejtlich, a different question. Is the health sector a particularly attractive target to hackers seeking to sell that personally identifiable information in the black market because, you know, even though they didn't get maybe medical records, but they get social security numbers and everything else. Is that--

Mr. {Bejtlich.} Yes, and one way, sir, we can measure that is how much does that sort of information sell for. You can get credit cards from $1 to $10, maybe a little bit more for an Amex or something like that, but if you are looking at a healthcare record with a social security and such, you are looking at $300 perhaps. And so clearly, that information is more valuable.

Mr. {Green.} Who are the potential buyers for that kind of information?

Mr. {Bejtlich.} You know, it is not something we spend a lot of time on at Mandiant FireEye, although there are

Eastern European criminal groups that apparently want to trade in that. I don't know if they are trading it in in bulk or individually. There is some thought that they trade for that information because it is so durable. You know, you can change your credit card, you can't change a social security number.

Mr. {Green.} Okay. Could stolen medical data be used to falsely bill for medical services, such as Medicaid or Medicare?

Mr. {Bejtlich.} That is not an area that we work, but I have heard of that, yes.

Mr. {Green.} Okay. I thank you. I would like to move the issue of notification of the patients in the event of a breach of medical information. Under current law, healthcare entities must provide notification of breaches of unsecured protected health information. Health information is considered unsecured essentially if it is not encrypted. Covered entities must notify affected individuals of a breach of unsecured protected health information within 60 days following the discovery of the breach. I think it is important to note that healthcare entities and medical information are already governed by a set of federal guidelines. I would like to ask all three panelists an open question about applying these standards. First, you know, if you have 60 days to notify them, you know, that--it is already--the cat is already out the door, it seems like, if you have that much time. Are there some basic standards such as encryption of certain data, or breach notification standards, that we may want to consider adopting as part of a federal cybersecurity guideline or national standard?

Mr. {Lin.} One--

Mr. {Shannon.} One--go ahead.

Mr. {Lin.} One can certainly imagine mandates, well, encouragement for healthcare companies to protect their data. Internally, for example, you can do encryption of data even when it is within your system.

Mr. {Green.} Um-hum.

Mr. {Lin.} Theft of laptops has been a--historically been an important vector out of--where people steal information. If you encrypt the data on the laptop, it is a good thing. I caution that encryption is a costly--not costly, but I mean it is great--that results in greater inconvenience for the companies, and so they are going to complain about such mandates.

Mr. {Shannon.} One of the challenges with regulations is that it encourages a compliance mentality, and I think we would all agree that compliance mentalities do not usually improve security dramatically. That is why I would encourage the healthcare industry to look at the NIST Cybersecurity Framework as a basis for managing cybersecurity risks, as opposed to compliance as the real driver.

Mr. {Bejtlich.} And I would briefly like to encourage those companies to first look to see if there are intruders already in your network, and secondly, to have someone test to see how difficult it is for them to get into your network, and then act on the results.

Mr. {Green.} Okay. Thank you, Mr. Chairman. I yield back my time.

Mr. {Murphy.} Thank you.

I know Mr. Mullin was on his way, but that may be it for the hearing. I really want to thank you. This is valuable information, and let me--do you have any final closing comments you want to make? First, Ms. DeGette.

Ms. {DeGette.} I think this is a good scene-setter for our future hearings, and I would just advise the--I know, Mr. Chairman, you will let people know that people might give written questions after this hearing. I know some of the Members on our side wanted to come back but they got stuck after the vote. So we appreciate your wisdom and you may have some written questions coming after this. Thank you. I yield back.

Mr. {Murphy.} I thank you. And I would certainly--we will probably be calling upon your expertise. We thank you for taking time out, and for the caliber of this. We will be dealing with a number of serious issues in this committee. Dr. Burgess is on this committee, he is also chairman of Commerce, Manufacturing and Trade legislation risk committee, but also Mr. Walden is chairman of Communications and Technology, we have the Energy and Power Committee, they have the Health and Subcommittee, all of these things here will be dealing with some multiple levels. The way I like to review it is we have the dot-coms, the dot-mils, the dot-govs, the dot-orgs, the dot-edus. Have I left anything out? We have to do what the committee--the dot-Greens, the dot-Tex,

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

whatever. But thank you so much for this. It--to that end, I ask unanimous consent that the Members' written opening statements be introduced into the record. So without objection, the documents will be entered into the record, including the one that you have, Dr. Lin.

[The information follows:]

*************** COMMITTEE INSERT ***************

|

Mr. {Murphy.} And in conclusion, I want to thank all the witnesses and Members that participated in today's hearing. I remember Members they have 10 business days to submit questions to the record, and I ask that all witnesses agree to respond promptly to the questions. Thank you so much.

And with that, this committee is adjourned.

[Whereupon, at 3:41 p.m., the subcommittee was adjourned.]