**Statement for the Record**
**Caleb Barlow, Vice President, Threat Intelligence, IBM Security**

**Before the United States Senate Committee on Commerce Regarding**
**The Promises and Perils of Emerging Technologies for Cybersecurity**

**Wednesday, March 22, 2017**

Chairman Thune, Ranking Member Nelson, and distinguished Members of the Committee, I am pleased to appear before you today to discuss how emerging technologies can help American companies more effectively defend themselves against cyberattacks. In my testimony, I will focus on the state of cybercrime, the importance of sharing data on cyber threats, and how emerging technologies, such as blockchain and cognitive systems that learn and reason, help dramatically reduce cybercrime while also closing the looming cybersecurity skills gap.

## The State of Cybercrime

Before discussing emerging security technologies, it's important to describe the current state of cybercrime. Today, just about everything we hear about involves the exfiltration of data. A cybercriminal breaks into a system, gets access to information, downloads that data and extorts it for profit or influence. Over 2 billion records were stolen last year alone. And in 2015, over 100 million people – most of whom were Americans – had their healthcare records stolen.[1]

From my vantage point working in one of the largest security intelligence operations in the world – IBM manages 35 billion security events *per day* for our clients -- I see not only how many records are being stolen, but other changes that are unfolding. For example, it's not just the amount of records being stolen, but what cybercriminals are doing with the information. Rather than just stealing the data to profit from it, what would happen if a cybercriminal changed it? What would happen if they manipulated a financial record or rerouted a supply chain?

These types of attacks are emerging. Before the 2016 Summer Olympic games, a group of hackers who call themselves "Fancy Bear" accessed athletes' data in the World Anti-Doping Agency's database. They then released sensitive data; for example, they listed athletes who were given permission to use otherwise banned substances such as certain types of asthma medication.

But what is particularly alarming is that this hacker group allegedly did more than just steal and release data. According to the World Anti-Doping Agency, the hackers also made changes to the data prior to releasing it, in an attempt to swing public opinion.

By breaking trust, even the smallest of actions can have tectonic implications. For example, if cybercriminals manipulate the data consumers have come to inherently trust – from the financial reporting of the companies they invest in to their healthcare records – we move beyond stolen information and money to an even more damaging issue: a loss of trust. This, of course, could

[1] See: IBM Security Intelligence by Caleb Barlow, Attackers Shift Sights from Retail to Health Care in 2015 http://ibm.co/1Vpruus

have many damaging ramifications. Imagine the uncertainty you would face regarding the soundness of your investments if you read that a cybercrime gang had manipulated the financial records of companies in your portfolio.

We are seeing security attacks and techniques continue to evolve, and it's important to understand where they are originating from, not necessarily geographically but from an economic and sociologic perspective. The United Nations estimates that 80 percent of cybercrime is from highly organized and ultra-sophisticated criminal gangs[2]. It is now estimated to be one of the largest illegal economies in the world, costing the global economy more than $445 billion dollars a year[3]. To put this in perspective, $445B is greater than the GDP of more than 160 different countries, including Ireland, Malaysia, Finland, Denmark, and Portugal, among many others.[4]

The most sophisticated thieves operate like a well-oiled global business. They build development tools and collaborate on software. They share knowledge about targets and vulnerabilities. In fact, each successful attack proliferates the skills, tools and ecosystem because hackers often reuse malware and other vulnerabilities that they know are proven to work. Think of it as on-the-job training.

They operate on a regimented schedule like many legitimate companies; their employees work Monday through Friday and take the weekends off. We know this because our security researchers see repeated spikes of malware launched on Fridays as hackers head home for the weekend. On Monday, the criminals regroup to see how well things went.

They collaborate and share expertise on a global scale via the "Dark Web" – a term used to describe the anonymous Internet where identity-masking tools enable criminals to operate without detection. Networks of thieves steeped in both IT and business skills work together to steal intellectual capital to damage businesses, and take your money.

The Dark Web is where these criminals build and peddle attack software to steal data from businesses and other institutions. Their cohorts can purchase everything online from base-level attack platforms to premium versions, which might offer a gold, silver and bronze-level of service -- and even a money-back guarantee if they don't get a successful hack. There are different products and prices, along with ratings and reviews of the "merchants." If you buy a hack from a "reputable criminal" with good ratings, you are far more likely to purchase a hack that is going to work.

Another major trend in cybercrime involves the Internet of Things. In our increasingly interconnected world, the devices, the data they produce and use, and the systems and applications that support them, are all potential attack points for malicious actors. Unlike a traditional computer, these IoT devices often operate without human supervision. They can be deployed for an extended lifetime and often lack simple methods to update and patch their

[2] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, February 2013

[3] Net Losses: Estimating the Global Cost of Cyber Crime, Center for Strategic and International Studies, June 2014

[4] See: http://statisticstimes.com/economy/countries-by-projected-gdp.php

software, which leads to poor security. Worse yet, to ease the deployment of these IoT devices, many often ship with minimal security controls, default user ID's and passwords that are never updated by the end user, making them easy targets for an attacker.

IoT devices are accumulating massive amounts of personal and sensitive data, like voice searches, GPS locations, and heart rate readings. If the data isn't managed and secured, its exposure can lead to a loss of privacy and data ownership. This makes the security of the data, how it's created, used and deleted extremely important.

Simply put, if a device connects to the internet, consumers need to understand not only what data it collects and how it is used, they must also have a way to maintain and update its security for the usable lifetime of the device.

**Battling Cyber Crime via Threat Sharing**

So how do we stop this? Cybercrime rings operate with anonymity and often seemingly outside the reach of the law. What we need to do is change the economics for the bad guys.

Our response to cybercrime needs to be similar to how we manage a healthcare pandemic. Sars, Ebola, Bird Flu, Zika – what is the top priority when handling an outbreak? It is knowing where infections are occurring and how they are being transmitted. First responders, physicians, hospitals, governments and the private sector all share information rapidly and openly. This is a collective and altruistic effort to stop the spread of sickness in its tracks, and then rapidly get the word out on transmission modality so that anyone not infected can protect themselves.

Unfortunately, this is not what we see today in the event of a cyberattack. Organizations are much more likely to keep the attack to themselves because of a perceived risk to their reputation. When a major breach is publicly revealed, typically all that is reported (by the media) is how many records were stolen. Even if a company makes a disclosure, rarely do organizations talk about <u>how</u> they were infected because they are worried about the risk of litigation or regulation.

Adding to the problem, many security vendors see threat data as an opportunity for profit – something of value to be shared only with high-paying customers and used for competitive advantage. And many government agencies continue to operate with Cold War-era strategies, when keeping critical information hidden from a major adversary was paramount. But in today's world, with an asymmetric enemy that operates anywhere and with impunity, keeping government information secret can work against us. Governments, too, need to disclose cyber threat indicators, vulnerabilities, breaches and hacking schemes, when appropriate, much faster. We call this concept the "default declassification of threat data at speed."

The good news is that we are seeing signs of progress in this area. The enactment of the Cybersecurity Information Sharing Act of 2015 (CISA), for example, was an important and helpful step forward, and we have seen progress in our discussions and work with various government agencies on sharing cyber threat data. But the scale and pace of information sharing needs to be accelerated.

Cyber threat sharing is only actionable when it happens with speed, but most governments are still keeping that data confidential for extended periods of time.

As a result, we've reached a point where new actions and strategies are required. Security vendors, governments and other organizations need to open their arsenal of information on threats – the types of threats, where they are coming from, how they work – and share them openly, at scale and without significant financial remuneration. Simply put, we must democratize threat intelligence data to compete with cybercriminals at their own game.

By uncovering criminals' devises closer to real time, we foil their schemes. We analyze and break their plans, and share their methods with the potential victims and general public a lot sooner than the adversaries expect. By consistently keeping pace with threat intelligence and using it to out-maneuver the criminals, we gradually make cybercrime not pay. We change the economics for the bad guys.

And if it does not pay, what's the motivation to do it in the first place?

To begin addressing some of the barriers to real time threat sharing and improve the sharing ecosystem, IBM supported the enactment of CISA. However, even before CISA became law, IBM took the initiative to practice what we are preaching, to share our data on cyberthreats. In 2015, IBM opened one of the largest treasure troves of threat data in the world and created the IBM X-Force Exchange. We put it all on the internet for free. IBM published nearly 700 terabytes of actionable threat data from around the globe, including real-time indicators of live attacks, which can be used to defend against cybercrimes. We keep publishing, every day, every hour.

**Battling Cybercrime with Cognitive and Blockchain Technology**

So how can we democratize threat data while reducing attribution risk to governments and private institutions?

This is where emerging technologies can play a big role in cybersecurity. Cognitive security technologies, for example, has enormous potential.

The number of risks and events is growing exponentially, and security operations teams are struggling to keep up with the volume. The threat landscape is changing rapidly, with the sophistication and numbers of threat variants becoming too great to keep pace with or stay ahead of using traditional approaches. The repercussions of incidents and breaches are increasing, with the financial costs and risks growing rapidly.

At the same time, many organizations are faced with a dearth of security experts with the right skills. These different factors make it difficult for organizations to maintain the healthy digital immune systems they need to protect themselves and are driving the need for new cognitive security technologies.

Specifically, we need new technologies that can serve as a cognitive security assistant to analyze massive amounts of data to make recommendations on remediation actions with much greater speed and precision.

To highlight the amount of security information available today, there are about 60,000 security blogs per month and 10,000 security reports per year[5]. We estimate that organizations are spending $1.3 million a year dealing with false positives alone, wasting nearly 21,000 hours[6]. Cognitive security technologies can make a huge difference by helping security professionals keep up with all this information and extract value from it with greater speed and accuracy.

Last month, IBM launched a cognitive security technology called Watson for Cyber Security. About 50 organizations – Fortune 500 companies across all major industries – are now using Watson to fight cybercrime.

The scale of what Watson is doing is enormous. In less than a year, Watson for Cyber Security has analyzed more than 1 million security documents on the Internet. It is now analyzing 15,000 security documents *per day* – amounts that no army of people alone could ever process.

What is even more significant than the scale of the data being analyzed, is what cognitive security technologies, such as Watson, can do with this sea of information. Specifically, true cognitive security technologies are systems that learn versus systems that are programmed. They can scour unstructured data across the Internet – the blogs and reports, media articles, social media, and many other sources – that were previously inaccessible by traditional security tools.

Cognitive systems can be trained to understand imprecise human language in those documents – for example, understanding that in security terms a "bug" is a software defect and not an insect.

Watson for Cyber Security is the first cognitive technology that is doing all of this. Our early findings are that Watson's capabilities are 60-times faster than complex manual analysis, with 10-times more actionable indicators to uncover new threats.[7]

It is also important to underscore that cognitive technologies like Watson do not replace people, but help them to be more productive, precise and efficient in defending their organizations from cyberattacks.

At the same time, they will help bridge a looming skills gap – an estimated 1.5 million unfilled security jobs by the end of this decade – by making the existing security workforce more effective and efficient.

Cognitive technologies also can help create new jobs. At IBM, for example, we're now tapping professionals who may not have a traditional college degree, but who have the needed skills and

---

[5] See: Watson for Cyber Security: Shining a light on human generated data, August 2016 - http://ibm.co/2mXuZj7

[6] *The Cost of Malware Containment, by Ponemon Institute, January 2015*

[7] IBM Watson for Cyber Security Beta Testing Results

aptitude to help us in a variety of disciplines, including cybersecurity. We refer to these new professionals as "new collar" workers, who may join an organization, for example, with base-level security skills from a P-Tech school or with an Associate's Degree.

Cognitive security technologies like Watson can help these "new collar" workers by providing them with much greater levels of security analysis and insights. Essentially, with cognitive security products, new collar employees can be paired with technology that is like the equivalent of a highly seasoned and experienced human security analyst, but one who can examine massive amounts of data at incredible speeds.

New collar jobs are one way to help reduce the security skills gap, but we also need institutions of higher education to expand their cybersecurity curricula. We need more choices for earning cybersecurity degrees and more students in the pipeline. We also need to focus on ways to develop more female experts in this field, as women represent only about 10 percent of today's cybersecurity workforce.[8]

At IBM, we're also looking at other ways to help our new collar and traditional security employees alike to benefit from cognitive security. One example is our new research project, code named Havyn, which brings a voice to cognitive security.

Havyn is a voice-powered security assistant that can interact verbally with security analysts in real-time on a variety of topics, from information on new threats, to data on an organization's security posture.

Havyn creates a "second-screen experience" for security analysts. It works in the background on command, pulling data from different security tools and sources, and brings the relevant information to the surface for further investigation by human analysts.

Voice-powered tools like Havyn can greatly expand the value of cognitive security intelligence sources like Watson. Just think of Watson for Cyber Security as the brain of the Security Operations Center, and think of Hayvn as bringing a voice to the brain, making Watson's expertise even more valuable.

Blockchain is another important example of emerging technology.

Blockchain is a technology for a new generation of transactional applications that helps establish security, trust, accountability and transparency. One of the key capabilities of blockchain is the ability to maintain a record of the history of all transactions in a way that cannot be manipulated.

Not only is it inherently more secure than other protocols, but blockchain has the potential to be used by multiple parties to share cyber-threat intelligence in a way that maintains the reputation of the source of the data without revealing the identity of the source. Governments and private institutions can combine data into threat feeds that ensure transactional integrity and maintain reputation, but without identifying the contributor.

[8] 2015 report by (ISC)2

Blockchain also has potential security benefits for IoT where supply chain integrity is critical. Although there may be dozens of parties involved in an IoT supply chain, a Blockchain can ensure transactional integrity and visibility of logistical and quality metrics from manufacturer to point of use.

Blockchain has inherent qualities that provide trust and security, but, to fulfill its promise, the core technology must be further developed using an open source governance model to make it deployable on a grand scale. The federal government must invest in scientific research to accelerate progress. The National Institute of Standards and Technology can help shape standards for interoperability, privacy and security. And government agencies can become early adopters of blockchain applications. In addition, government has a key role to play in certifying the identities of participants in blockchain-based systems.

**Conclusion**

Cybercrime is one of this generation's most vexing societal problems. As with all historic societal challenges, it requires radical change at great speed.

The public and private sector need to collaborate on a much deeper level to make the sharing of cyberthreat data a standard practice. This level of interaction and sharing will result in highly organized cybercrime fighting to thwart the massive collaboration of cybercriminals today.

We need the partnership to incubate, develop, and institute emerging security technologies such as cognitive systems and blockchain. We need higher education institutions to also step up in cultivating a new generation of security experts for our workforce.

In the process, we will not only chip away at cybercrime, but radically reduce it by changing the economics of this significant illegal economy. In doing so, we will experience many benefits, including instilling trust in global interconnected systems, creating new jobs while reducing a skills shortage, and increasing the diversity of the workforce.

Thank you Chairman Thune, Ranking Member Nelson and distinguished Members of the Committee for the opportunity to provide IBM Security's perspective on this important topic.