CYLANCE™

WRITTEN STATEMENT FOR THE RECORD OF

MALCOLM HARKINS

CHIEF SECURITY AND TRUST OFFICER

CYLANCE INC.

Before the

UNITED STATES SENATE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

On

“THE PROMISES AND PERILS OF EMERGING TECHNOLOGIES FOR CYBERSECURITY”

MARCH 22, 2017

Good morning Chairman Thune, Ranking Member Nelson, and other members of the Committee. Thank you for the opportunity to testify today. I am Malcolm Harkins, Chief Security and Trust Officer for Cylance Inc. I am pleased to address the Committee on how emerging technologies such as artificial intelligence, the internet of things, blockchain (the technology behind Bitcoin), and quantum computing will drive a new generation of cyber vulnerabilities. Every evolution of technology holds the promise of innovation and creates unique security risks. However, with the proper design and forward looking considerations these emerging technologies can also be used to combat cyber threats more effectively.

My testimony will focus on the following areas

- The innovation cycle and how that is fueling emerging technologies which are leading to digital transformations that present tremendous opportunity for economic as well as societal benefit.
- The information risk and security implications for these emerging technologies. The potential impacts and concerns to individuals, business, and government agencies if the creators do not provide proper security capabilities as they design, develop, implement, and maintain these new innovations.
- The cybersecurity opportunities these technologies offer to enable better risk mitigation thru prevention rather than today's norm of react and response.
- How we should be framing the digital opportunities in front of us so that we can achieve digital transformation and digital safety to ensure tomorrow is better than today.

First, I would like to provide some background on my experience and Cylance's commitment to cybersecurity.

As Chief Security and Trust Officer for Cylance, I am responsible for enabling business growth through trusted infrastructure, systems, business processes and staff training. I have direct organizational responsibility for information technology, information risk and security, as well as security and privacy policy. I am also responsible for peer outreach activities to drive improvements and understanding of cyber risks. I work with business leaders, industry peers, security experts and regulatory partners to develop best practices for managing and mitigating those risks.

Prior to joining Cylance in 2015, I spent almost 24 years at Intel Corporation. My last role at Intel, which I held for more than 2 years was Vice President and Chief Security and Privacy Officer (CSPO). In that role, I was responsible for managing the risk, controls, privacy, security, and other related compliance activities for all of Intel's information assets, products, and services. Before becoming Intel's first CSPO, I was the Chief Information Security Officer (CISO) reporting into the Chief Information Officer. Over my years at Intel I also held roles in Finance, Procurement, and other business operational positions.

I have been fortunate to receive both peer and industry recognition over the years including the RSA Excellence in the Field of Security Practices Award, Computerworld Premier 100 Information Technology Leaders, Top 10 Break-away Leaders at the Global CISO Executive Summit, and the Security Advisor Alliance Excellence in Innovation Award. I have authored many white papers, blogs, and articles. In December 2012 I published my first book, Managing Risk and Information Security: Protect to Enable®. I was also a contributing author to Introduction to IT Privacy, published in 2014 by the International Association of Privacy Professionals. The 2nd edition of my book, Managing Risk and Information Security: Protect to Enable®, was recently published in August of 2016.

CYLANCE's COMMITMENT TO CYBERSECURITY

Cylance was founded in 2012 by Stuart McClure and Ryan Permeh with the sole purpose of revolutionizing cybersecurity by replacing outdated reactionary security models with proactive prevention based security using artificial intelligence and machine learning to stop attacks before they occur.

Stuart McClure previously served as the Global CTO of McAfee/Intel Security business and is the founding/lead author of the international best-selling book Hacking Exposed. Ryan Permeh previously served as Chief Scientist at McAfee/Intel Security and is the brain behind Cylance's mathematical architecture and new approach to security. In building Cylance, Mr. McClure and Mr. Permeh brought together the best data science, security and executive minds from the likes of Cisco, Sourcefire, Google, Symantec, McAfee and several federal intelligence and law enforcement agencies to create a new security model that is focused on prediction of attacks and preventing them from occurring.

Cylance® is the first company to apply artificial intelligence, algorithmic science, and machine learning to cybersecurity and improve the way companies, governments, and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated artificial intelligence and machine learning with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be truly predictive and preventive.

Leveraging cutting-edge artificial intelligence and machine learning, our flagship product CylancePROTECT offers future-proof prediction and prevention of the most advanced threats in the world including advanced persistent threats, zero-days, and exotic exploitation techniques never seen before. CylancePROTECT also guards from everyday viruses, worms, ransomware, spyware/adware, Trojan horse attacks and spam.

The problem with legacy security solutions is that adversaries can continually evolve their techniques and tactics to bypass them, leaving enterprises exposed to attacks. This means that traditional solutions are reactive in nature and rely on a constant stream of "signature updates" that tell these solutions what type of files to look for after an attack was successful on some other system, these are called "zero-day" attacks. Traditional security solutions are built around a basic set of rules and signature files that are costly and high risk because they require a zero-day "sacrificial lamb" before they can create the ability to block an attack, meaning it is not possible to identify a new threat until after the damage is done. But CylancePROTECT is different — it can identify and defuse even never-before-seen attacks prior to execution. This means that we can stop new variations of attacks without a zero-day sacrificial lamb. Our AI-based solution is flexible and can support new generations of technologies such as the internet of things and many others.

Our commitment to cybersecurity was well demonstrated and documented in September 2016 House Oversight committee report on the OPM data breach. "The committee obtained documents and testimony that show internal bureaucracy and agency politics trumped security decisions, and that swifter action by OPM to harden the defenses of its enterprise architecture by deploying PROTECT would have prevented or mitigated the damage that OPM's systems incurred." OPM IT Security Officer Jeff Wagner said in an email that Cylance was able to find things that other tools could not "because of the unique way that Cylance functions and operates. It doesn't utilize a standard signature or heuristics or indicators, like normal signatures in the past have been done. It utilizes a unique proprietary method." The effectiveness of Cylance at OPM meant that upon our engagement in less than 10 days 2,000+ pieces of malware were identified that had previously not been stopped or detected across 10,000+ hosts that are now protected by CylancePROTECT.

THE INNOVATION CYCLE OF EMERGING TECHNOLOGIES:

Understanding these innovations and the digital opportunities they offer

The march of technology can be viewed as a succession of major waves, each lasting roughly 100 years (Rifkin 2013). Each wave has brought transformative benefits to society, but also significant challenges. The first wave, starting in the 1760s, included steam power, railways, and early factories as well as mass education and printing. The second wave, starting roughly in the 1860s and continuing well past the mid-1900s, included automobiles, electricity, mass production, and had an even bigger effect on society.

Version 1.0: 1760s	**Version 2.0: 1860s**	**Version 3.0: 1990s**
Steam and coal	Electric lights	The Internet
Railways	Communications	Molecular biology
Factories	Oil & gas	Renewable energy
Printing press	Mass production	"Smart" everything
Mass education	Automobiles	

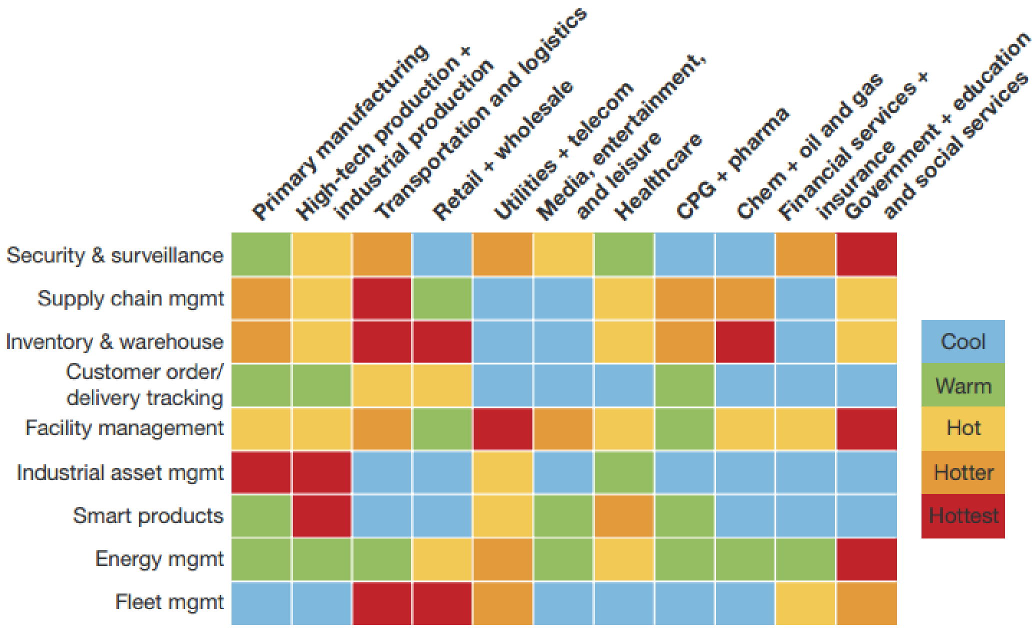
The third wave began in the 1960s, with early computers, but only really gained momentum in the 1990s. It includes the Internet and smart "things", molecular biology and genetic engineering, and renewable energy. Arguably, this technology wave may have the broadest impact on society of any to date. Each previous wave lasted about 100 years, so history suggests that we are far from reaching the crest. To provide some perspective - if we thought of this wave as a movie, we'd still be watching the opening credits.

The Internet of Things (IoT) has come upon us at a fast and furious pace. It gets discussed and hyped constantly, but sometimes without a clear definition. And, as such, the phrase can mean different things to different people. But a simple way to think about it is that any powered device will compute, communicate, and have an IP address – meaning it is connected to a network. The Internet of things allow devices to be sensed or controlled remotely across the Internet. This has created opportunities for more direct integration of the physical world into computer systems. When IoT is augmented with various sensors we have what is often defined as smart grids, smart homes, and smart cities. Each IoT device has an embedded computing system and is able to interoperate within the existing Internet infrastructure. Many estimate indicate that the IoT will consist of more than 50 billion devices by 2020, some estimates top 70 billion devices.

IoT devices or objects can refer to a wide variety applications including everything from a heart monitoring implant or pacemaker to biochip transponders on farm animals or children's toys such as an internet connected Barbie doll. Current market examples include home automation, such as Google Nest, which can provide control and automation of lighting, heating, ventilation, air conditioning (HVAC) systems, and appliances such as washer/dryers, robotic vacuums, air purifiers, ovens or refrigerators/freezers that use Wi-Fi for remote monitoring.

In November of 2016, Louis Columbus from Forbe's wrote, "This years' series of Internet of Things (IoT) and Industrial Internet of Things (IIoT) forecasts reflect a growing focus on driving results using sensor-based data and creating analytically rich data sets. What emerges is a glimpse into where IoT and IIoT can deliver the most value, and that's in solving complex logistics, manufacturing, services, and supply chain problems."

FIGURE 6 Heat Map Of Key IoT Opportunities Varies By Industry And Application



	Primary manufacturing	High-tech production + industrial production	Transportation and logistics	Retail + wholesale	Utilities + telecom	Media, entertainment, and leisure	Healthcare	CPG + pharma	Chem + oil and gas	Financial services + insurance	Government + education and social services
Security & surveillance	🟩	🟨	🟧	🟦	🟧	🟨	🟩	🟦	🟦	🟧	🟥
Supply chain mgmt	🟧	🟨	🟥	🟩	🟦	🟦	🟨	🟧	🟧	🟦	🟨
Inventory & warehouse	🟧	🟨	🟥	🟥	🟦	🟦	🟨	🟧	🟥	🟦	🟨
Customer order/ delivery tracking	🟩	🟩	🟨	🟨	🟦	🟦	🟦	🟩	🟦	🟦	🟦
Facility management	🟨	🟨	🟧	🟩	🟥	🟧	🟨	🟩	🟨	🟨	🟥
Industrial asset mgmt	🟥	🟥	🟦	🟦	🟨	🟦	🟩	🟦	🟦	🟦	🟦
Smart products	🟩	🟥	🟦	🟦	🟨	🟩	🟧	🟩	🟦	🟦	🟦
Energy mgmt	🟩	🟩	🟩	🟨	🟧	🟩	🟨	🟩	🟩	🟩	🟥
Fleet mgmt	🟦	🟦	🟥	🟥	🟧	🟦	🟦	🟦	🟦	🟨	🟧

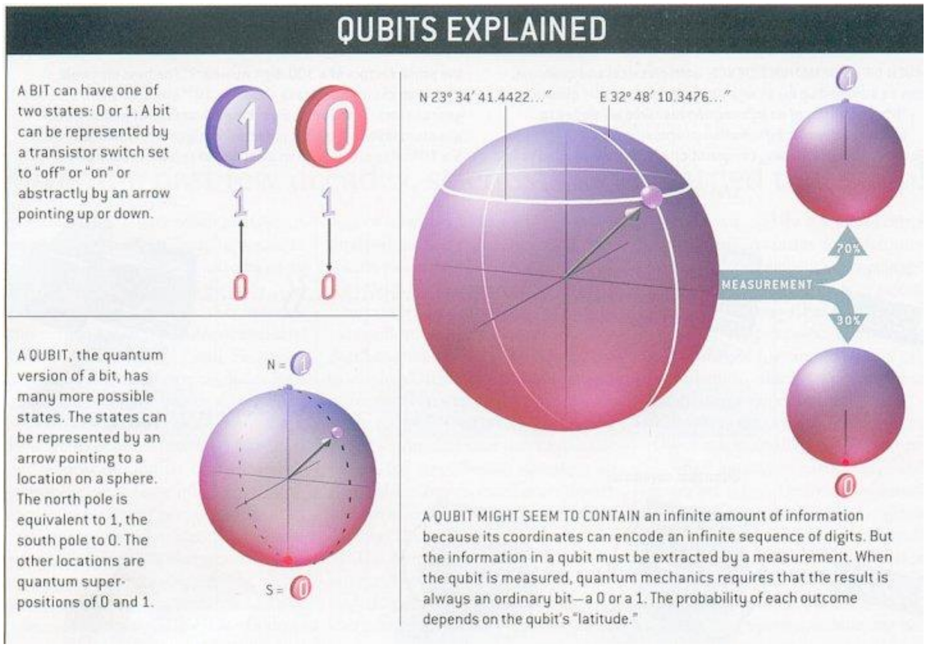
🟦	Cool
🟩	Warm
🟨	Hot
🟧	Hotter
🟥	Hottest

Source: Forrester - The Internet Of Things Heat Map 2016, Where IoT Will Have The Biggest Impact On Digital Business by Michele Pelino and Frank E. Gillett January 14, 2016

Quantum Computing is also emerging quickly. In 2011 Microsoft created a Quantum Architectures and Computation Group with a mission to advance the understanding of quantum computing, its applications and implementation models. In February 2017, Brian Krzanich, CEO of Intel said he was "investing heavily" in quantum computing during a question-and-answer session at the company's investor day. Earlier this month in March 2017, IBM announced that it's planning to create the first commercially-minded universal quantum computer.

Today's computers work by manipulating bits that exist in one of two states: a 0 or a 1. Quantum computers aren't limited to two states. By harnessing and exploiting the laws of quantum mechanics to process information a quantum computer can encode bits which contain these multiple states simultaneously and are referred to as Quantum bits or "qubits". Quantum computing has the potential to be millions of times more powerful than today's most powerful supercomputers. Last year, a team of

Google and NASA scientists discovered a D-wave quantum computer was 100 million times faster than a conventional computer.



A BIT can have one of two states: 0 or 1. A bit can be represented by a transistor switch set to "off" or "on" or abstractly by an arrow pointing up or down.

A QUBIT, the quantum version of a bit, has many more possible states. The states can be represented by an arrow pointing to a location on a sphere. The north pole is equivalent to 1, the south pole to 0. The other locations are quantum super-positions of 0 and 1.

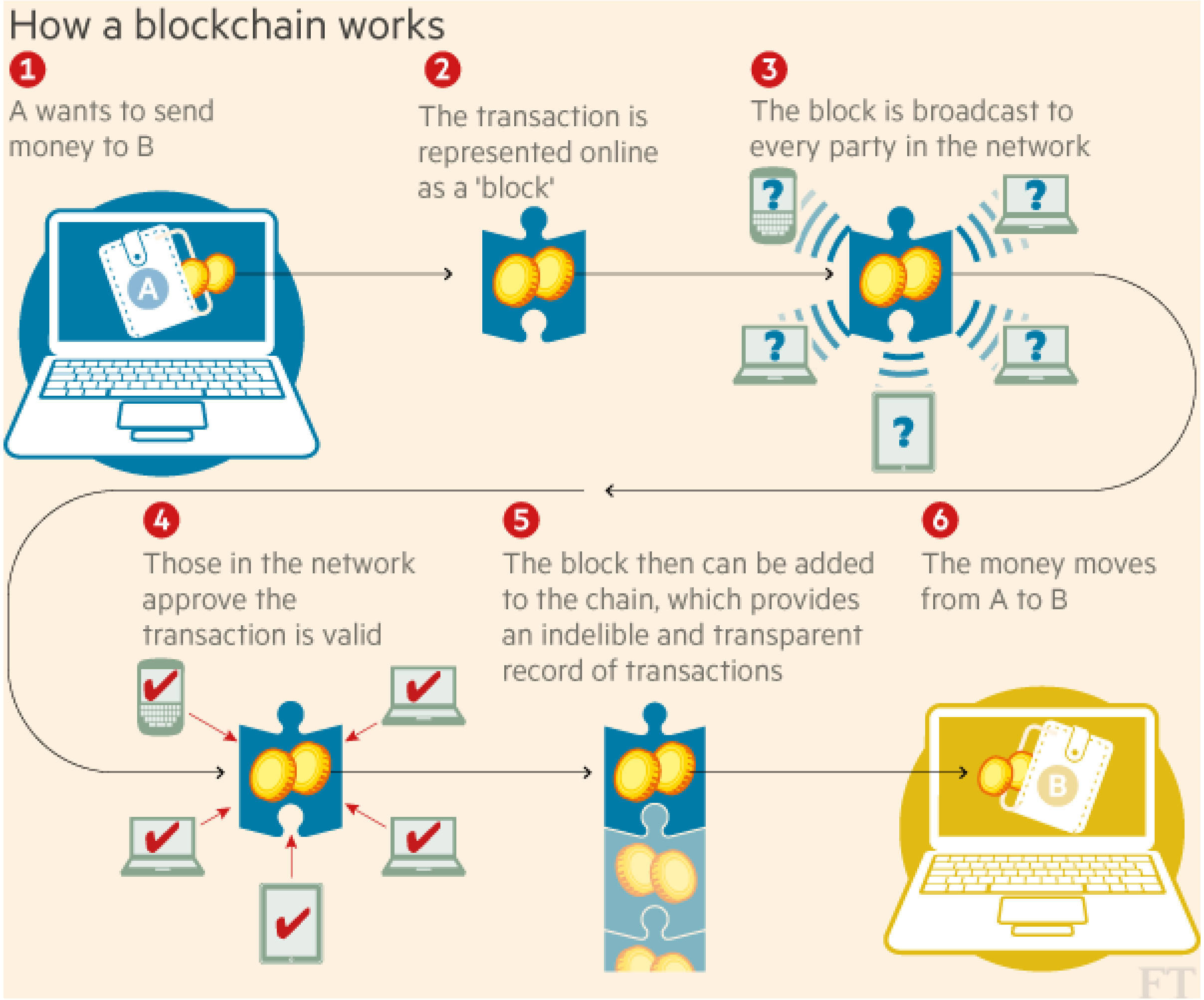
A QUBIT MIGHT SEEM TO CONTAIN an infinite amount of information because its coordinates can encode an infinite sequence of digits. But the information in a qubit must be extracted by a measurement. When the qubit is measured, quantum mechanics requires that the result is always an ordinary bit—a 0 or a 1. The probability of each outcome depends on the qubit's "latitude."

Source: Universe Review

This means that may computing challenges and difficult computation tasks, long to be thought impossible (or "intractable") for classical computers will be achieved quickly and efficiently by a quantum computing. This type of leap forward in computing could allow for not only faster analysis and computation across significantly larger data sets. It would reduce the time to discovery for many business, intelligence and scientific challenges which include improving energy grids, protecting and encrypting data, simulations of molecules, research into new materials, development of new drugs, or understanding economic catalysts. Quantum Computing can reduce time spent on physical experiments and scientific dead ends resulting lower costs and faster solutions that can provide economic and societal benefit.

Blockchain as many people know it is the technology behind Bitcoin. A blockchain is a distributed database that maintains a continuously growing list of ordered records called blocks. Each block contains a timestamp and a link to a previous block. By design, blockchains are inherently resistant to modification of the data. Once recorded, the data in a block cannot be altered retroactively. Blockchains are an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically.

The technology can work for almost every type of transaction involving value, including money, goods and property. Its potential uses are wide ranging: from collecting taxes to more effectively managing medical records to anything else that requires proving data provenance.


How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B
?
FT

Source: WEFORUM.ORG

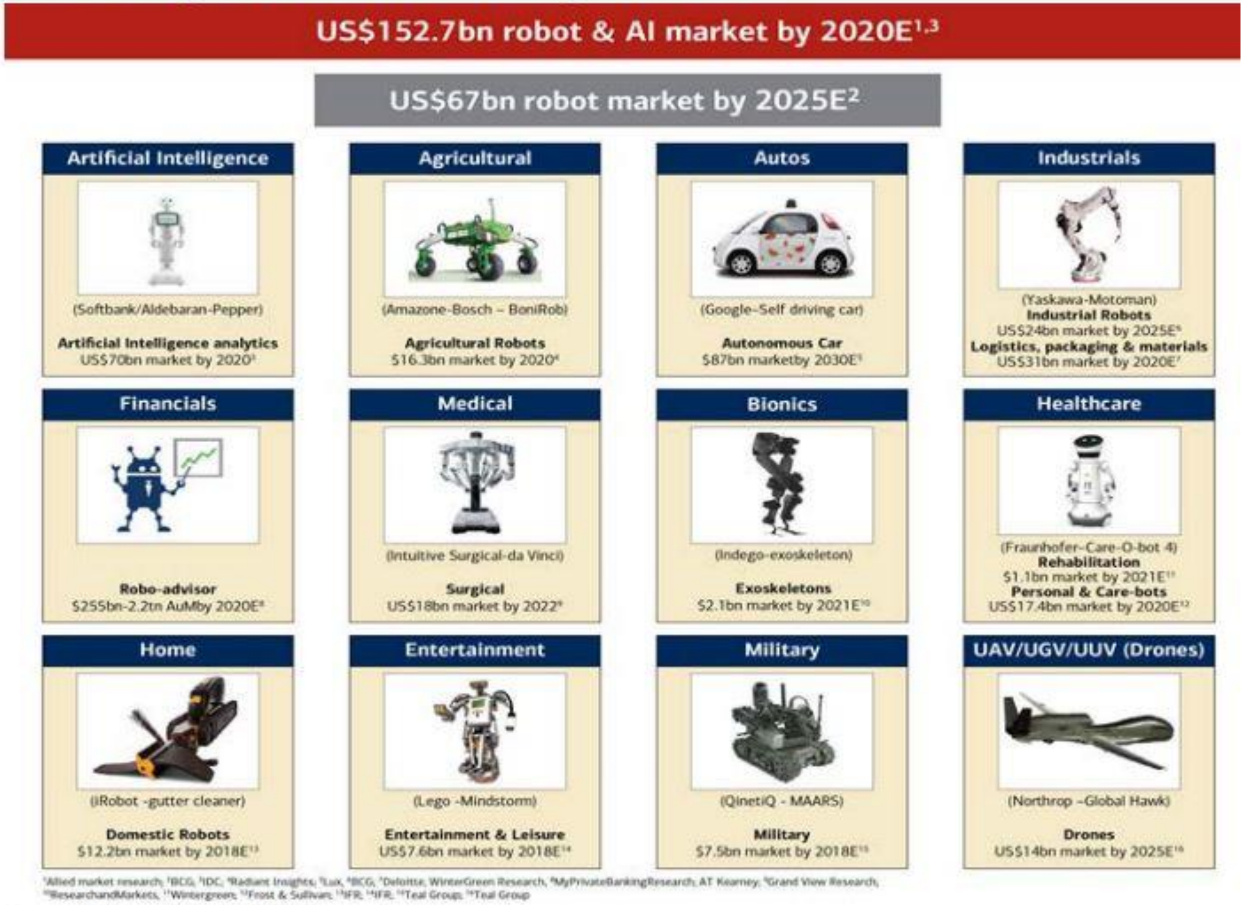
Artificial Intelligence is progressing rapidly with everything from SIRI to self-driving cars relying on it automate specific tasks. While there is a wide variety of definitions of AI. Artificial intelligence today is properly known as narrow AI (or weak AI), in that it is designed to perform a narrow task (e.g. only facial recognition or only internet searches or only driving a car). However, the long-term goal of many researchers is to create general AI (or strong AI). While narrow AI may outperform humans at whatever its specific task is, like playing chess or solving equations, general AI would outperform humans at nearly every cognitive task.

Machine learning is a branch of artificial intelligence (AI). Machine learning is also one of the most important technical approaches to AI. It is the basis of many recent advances and commercial applications of AI. Machine learning is a statistical process that starts with a body of data and tries to derive a rule or procedure that explains the data or can predict future data.

A simple way to describe how ML works is as follows: In traditional programming, you give the computer an input - let's say 1+1. The computer would run an algorithm created by a human to calculate the answer and return the output. In this case, the output would be 2. Here's the crucial difference. In machine learning, you would instead provide the computer with the input AND the output (1+1=2). You'd then let the computer create an algorithm by itself that would generate the output from the input. In essence, you're giving the computer all the information it needs to learn for itself how to extrapolate an output from the input. In classrooms, it's often stated that the goal of education is not so much to give a growing child all the answers, but to teach them to think for themselves. This is precisely how machine learning works.

AI has applications in everything from Agriculture for crop monitoring, automated irrigation/harvesting (GPS-Enabled) Systems to the Media and Advertising industry with Facial Recognition Advertising.

Exhibit 1: The global robots & artificial intelligence market



US$152.7bn robot & AI market by 2020E[1,3]

US$67bn robot market by 2025E[2]

Artificial Intelligence
(Softbank/Aldebaran-Pepper)
Artificial Intelligence analytics
US$70bn market by 2020[3]

Agricultural
(Amazone-Bosch – BoniRob)
Agricultural Robots
$16.3bn market by 2020[4]

Autos
(Google-Self driving car)
Autonomous Car
$87bn marketby 2030E[5]

Industrials
(Yaskawa-Motoman)
Industrial Robots
US$24bn market by 2025E[6]
Logistics, packaging & materials
US$31bn market by 2020E[7]

Financials
Robo-advisor
$255bn-2.2tn AuMby 2020E[8]

Medical
(Intuitive Surgical-da Vinci)
Surgical
US$18bn market by 2022[9]

Bionics
(Indego-exoskeleton)
Exoskeletons
$2.1bn market by 2021E[10]

Healthcare
(Fraunhofer-Care-O-bot 4)
Rehabilitation
$1.1bn market by 2021E[11]
Personal & Care-bots
US$17.4bn market by 2020E[12]

Home
(iRobot -gutter cleaner)
Domestic Robots
$12.2bn market by 2018E[13]

Entertainment
(Lego -Mindstorm)
Entertainment & Leisure
US$7.6bn market by 2018E[14]

Military
(QinetiQ - MAARS)
Military
$7.5bn market by 2018E[15]

UAV/UGV/UUV (Drones)
(Northrop -Global Hawk)
Drones
US$14bn market by 2025E[16]

[1]Allied market research; [2]BCG; [3]IDC; [4]Radiant Insights; [5]Lux; [6]BCG; [7]Deloitte, WinterGreen Research; [8]MyPrivateBankingResearch; AT Kearney; [9]Grand View Research; [10]ResearchandMarkets; [11]Wintergreen; [12]Frost & Sullivan; [13]IFR; [14]IFR; [15]Teal Group; [16]Teal Group

Source: BofA Merrill Lynch Global Research

THE INFORMATION RISK AND SECURITY IMPLICATIONS

The digital disasters that could be created if we don't manage the risks ahead

These day, it's hard to read an online news source, pick up a newspaper, or watch TV without seeing reports of new threats: cybercrimes, data breaches, industrial espionage, and potential destruction of national infrastructure. These reports inevitably leave the impression that we are drowning in an inexorable tide of new and terrifying threats. Reports such as; "CloudPets' woes worsen: Webpages can turn kids' stuffed toys into intrusive audio bugs" read the headline on March 1, 2017 posted on The Register by Richard Chirgin. "Fatal flaws in ten pacemakers make for Denial of Life attacks" wrote Darren Pauli on December 1st 2016. Whether it is these headlines or the ones from June 2015 reporting "that hacker's show how to remotely crash a Jeep from 10 miles away" or the countless other headlines communicating vulnerabilities found or the breaches that have occurred, there is one common denominator that exists today and will exist tomorrow. Any device that executes code has the ability to be compromised and execute malicious code.

Emerging technology such as IoT, Blockchain, quantum computing, and artificial intelligence offer tremendous promise for benefit, but if poorly designed, developed, and implemented and there is a likely ability to execute malicious code harm will occur. The variety of risks and impacts to individuals, to our businesses, the economy, and potentially to society could be wide ranging and financial significant.

When assessing risk, I think it is important to look at data. Here is some data from recent surveys and studies:

2016 Europol Internet Organized Crime Threat Assessment Report

- Increase acceleration of previous threat and vulnerability trends
- APT and cybercrime boundaries blur
- Majority of attacks are neither sophisticated nor advanced: techniques are reused, recycled, and re-introduced
- Investing in prevention may be more effective than investigating

2016-2017 National Association of Corporate Directors Public Company Governance Survey

- Cybersecurity threats are expected to have the fifth greatest effect on a company in the next 12 months
- 75% of respondents report short term performance pressures compromise management and the board's ability to focus on the long-term
- Directors continue to wrestle with effective oversight of cyber risk. Many of them lack confidence that their companies are properly secured and acknowledge that their boards do not possess sufficient knowledge on this growing risk

ISSA - Through the Eyes of Cyber Professionals – Part 2

- 45% of cyber professionals think their organizations are significantly vulnerable to cyberattacks
- 47% think their organizations are somewhat vulnerable to cyberattacks
- 40% of cyber professionals want goals established for IT around cybersecurity

- 44% of cyber professionals indicate they do not get enough time with the board
- 21% say that business and executive management treat cybersecurity as a low priority
- 61% of CISO turnover is due to a lack of a serious cybersecurity culture and not active participation from executives

The conclusion that I can draw from this data, as well as all the headlines we see daily on breaches, including the March 9th 2017 headline from Tara Seals at Information Security Magazine that read "61% of Orgs Infected with Ransomware" is this: We are not in aggregate doing a good job today managing our risk. We need to do better. We have to do better. Not only do we need to make immediate improvements today we need to get in front of our future risks. Otherwise, the potential we have in front of us with technological advancements, which can benefit individuals, business, government and our society will be called into question.

WE CAN DO BETTER AT CONTROLLING FOR RISK TODAY AS WELL AS TOMMOROW

Emerging technologies, coupled with the right risk profile and control assessment frameworks enable better risk mitigation.

In the world of cybersecurity, the most frequently asked question focuses on "who" is behind a particular attack or intrusion – and may also delve into the "why". We want to know whom the threat actor or threat agent is, whether it is a nation state, organized crime, an insider, or some organization to which we can ascribe blame for what occurred and for the damage inflicted. Those less familiar with cyberattacks may often ask, "Why did they hack me?"

These questions are rarely helpful, providing only psychological comfort, like a blanket for an anxious child, and quite often distract us from asking the one question that can really make a difference: "HOW did this happen?"

The current focus on the WHO and the WHY does the industry and everyone else in general very little service. We need to rethink and refocus the Security Risk Equation to examine how the attack occurs to prevent them in the future.

Let's start by looking at the popular "risk equation" commonly used when assessing the possibility of a breach or cyberattack:

Risk = Threat x Vulnerability x Asset Value or Consequence/Impact

As someone who has been responsible for managing information risk and security in the enterprise for 15-plus years, I have thought through this equation countless times strategically, as well as tactically, during an incident. The conclusion I have arrived at over and over and over again is that I have little control or influence over threat actors and threat agents - the "threat" part of the above equation. The primary variable I do have control over is how vulnerable I am – meaning the strength of my present as well as my future control.

From a consequence and impact perspective there are only three primary consequences we need to focus on Confidentiality, Integrity, and Availability. Each of these have different potential impacts to an individual, to an organization, or more broadly to society depending on the technology or data attacked. When we examine "how" attacks are accomplished we see three core targets for attacks:

- Attacks on identity credentials
- Attacks focused on the execution of malware
- Attacks that create a Denial of Service

So what must always be analyzed and reported on is HOW an intrusion or attack was successful, so we can give attribution to either the control(s) that failed, the lack of control(s), and to those responsible for maintaining proper control.

A great example of this sort of investigation and analysis is the House Committee on Oversight and Government Reform OPM breach report which occurred in September of 2016 and in the subsequent report published in January 2017 by the Office of the Director of National Intelligence on Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. There are a few important items to note from the upfront background section:

1) "Intelligence Community judgments often include two important elements: judgments of how likely it is that something has happened or will happen (using terms such as "likely" or "unlikely") and confidence levels in those judgments (low, moderate, and high) that refer to the evidentiary basis, logic and reasoning, and precedents that underpin the judgments."

2) The nature of cyberspace makes the attribution of cyber operations difficult, but not impossible. Every kind of cyber operation — malicious or not — leaves a trail. U.S. Intelligence Community analysts use this information, their constantly growing knowledge base of previous events and known malicious actors, and their understanding of how these malicious actors work and the tools that they use, to attempt to trace these operations back to their source.

The government - which has badges, guns, jails and laws to enforce - should continue to focus law enforcement and other government agencies on attribution related to the source(s) of attacks, so they can take action to deter (via conviction and jail time) the threat actors who wish to do harm. They can also post an incident if enough evidence exists, attempt to detain and prosecute those responsible. However, this alone is a completely insufficient forum of attribution and per the report itself, has a degree of judgment.

Learning from the History of Attribution

One thing that can be done with complete certainty is to look closely at HOW the threat actors were successful, and hold those people and organizations accountable. We can also look back in history and learn how every other reported intrusion occurred in the past decade, including the now-infamous attacks on Sony, Home Depot, OPM, Yahoo, Target, Anthem, and JPMC. This attribution is irrefutable, and the only question we now have left to answer is why the same story has presented itself over and over again, and why are we (as an industry) failing to pay attention to it.

All of these intrusions have been successful due to one or both of the following incidences occurring:

1) Control(s) that failed, and/or

2) Incomplete or lack of control(s)

We can attribute the source of these items very simply and with certainty by answering two basic questions:

1) Who is accountable for the control environment?

2) Who created the control(s) that failed?

So, whom should we really hold accountable for the success of all these intrusions? The none- too-flattering answer is that while the breached organizations or the creator of the technology that was vulnerable may shoulder some of the blame, we can attribute the success of these attacks to the in many cases to cybersecurity industry itself.

Here is the simple reason: the security industry sells controls that fail, and do so repeatedly. And here's the rub. These products and services don't just fail in extreme conditions or due to highly unusual or sophisticated attacks. Every one of the organizations that suffered a breach was relying on the capabilities of a security provider that failed to prevent the attack.

Why are these vectors so easy? The simple reason is that in many cases, the security solutions deployed don't work with high enough success rate to make an attack difficult or even challenging.

Disengaging from the Blame Game

In order to move forward and refocus our industry's energies on making attacks more difficult for malicious actors, we need to break free from our own obsessive infatuation with attribution. By investing all of our resources into finding out "whodunnit," we get to play the victim card to minimize our own responsibilities and limit our liabilities. None of that helps the organizations that have been breached or the customers and clients who trusted those companies with their private information.

Instead, we need to focus on WHY those intrusions were successful, so we can give attribution to the real source of the intrusion – the controls that failed or lack of control.

This form of attribution will bring real accountability, and recalibrate our collective sights to take aim at the one variable in the risk equation that we have real influence over - our strength of control. Then, and only then, can we start to make a difference and put a bend in the curve of risk we have been witnessing, versus continuing to let it grow unchecked.

Control frameworks that add value

I have said for years that the core of business-driven security and the mission of the information risk and security team is "Protect to Enable." When you are protecting to enable people, data, and the business, you are proactively engaged upfront and aligned with the business on the evaluation of how to achieve the business objective, while best optimizing your controls.

I achieve that through my "9 Box of Controls" approach that was published in September of 2016 in the second edition of my book – Managing Risk and Information Security: Protect to Enable. Let me explain my perspective on controls. My perspective is rooted in my experiences as a business leader and in my many years in Finance, including my role as a profit and loss manager for a billion dollar business unit in the late 90s. It is a control philosophy that I have carried forward in my roles in security, but one that I believe is lacking in the industry.

An important aspect of this perspective is the concept of control friction. I've developed a simple framework called the 9 Box of Controls, which takes the issue of control friction into account when assessing the value as well as the impact of any control, including information security.

I believe that the 9 Box of Controls includes some actionable perspective that may be valuable to many organizations facing these universal risk challenges. My conversations with peers at other companies have validated this view. Many of them are now using the 9 Box to drive not only tactical, but also strategic discussions in their organizations around where they are spending their resources today, and where they should be headed long term.

Types of Security Controls

There are three primary types of security controls: prevention, detection and response:

- Prevention occurs when an action or control prevents a vulnerability up front in the design and development, or prevents an infection or cyberattack in its tracks before it affects users or the environment

- Detection means identifying the presence of a vulnerability or detecting something malicious that has already entered the environment

- Response is a reaction to the discovery of a piece of malicious code, attempting to remove it after it has already affected the user or the organization

From a risk perspective, prevention focuses on minimizing vulnerability and the potential for harm, while detection and response focus on minimizing damage. When you are focused on minimizing damage, the main variables to turn the reactive risk dials are a) time to detect and b) time to contain.

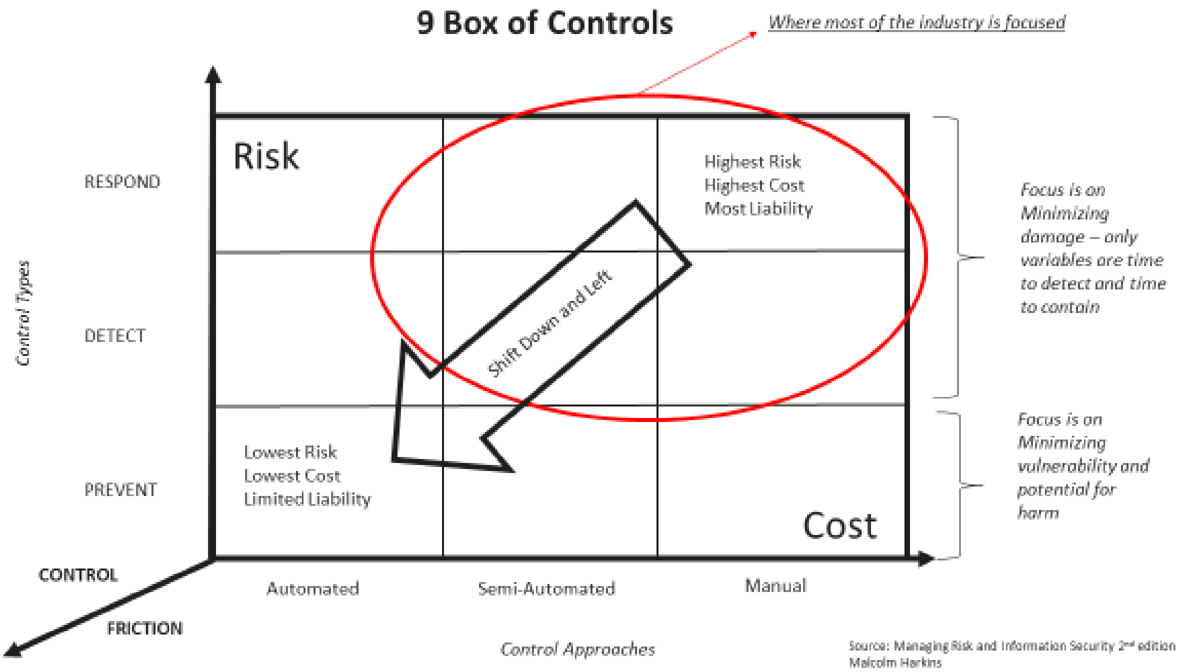
There are also three primary approaches one can take to implement a control: automated, semi-automated, and manual.

- Automated control occurs entirely through machines

- Semi-automated control involves some level of human intervention

- Manual controls are managed entirely by hand

The combinations of these control types and automation levels comprise the cells of the 9 Box, as shown in the figure below. Risk increases as we move from prevention, to detection, to response. Cost increases as we move from automated to semi-automated to manual controls.



Source: Managing Risk and Information Security 2nd edition
Malcolm Harkins

A Note on Control Friction

However, there is a third dimension to the 9 Box: control friction. As we know, friction is the force that causes a moving object to slow down when it comes into contact with another object. Similarly, controls can impose a “drag coefficient” on business velocity—they can slow the user or a business process. Just think of the groan issued by PC users when they switch on their machine to complete an urgent task, only to find it indisposed for the next half hour due to a patch or virus scan. Or think of the impact on time to market if your design or development practices are bogged down with slow and cumbersome security development lifecycle or privacy by design efforts.

However, friction is not a fundamental, immutable force like gravity or electromagnetism. Instead, we have the ability to determine exactly how much control friction we apply. Apply too much control friction, and business users may choose to circumvent IT security controls or the product security controls in the upfront design of technology. This adds not only cost but it also adds risk: because the security team lacks visibility into the technology being created or used. So it cannot prevent vulnerabilities or compromises, detection becomes difficult due to lack of visibility, and in many cases, response after the fact becomes the only option.

If a business adheres to high-friction controls, the long-term effect can be the generation of systemic business risk. High-friction controls can hinder business velocity; the organization can lose time to market and the ability to innovate, and over the long term it may even lose market leadership.

Implementing the NIST (National Institute of Standards and Technology) Cybersecurity Framework and continuously walking through the macro steps that it outlines is also another approach we should all continue to adopt and promote.

- Prevention Steps: Identify and Protect.
- Reaction Steps: Detect, Respond, and Recover.

If implemented properly, the NIST framework can set the stage for having the right discussion within an organization on information risk. It can also, when viewed in the context of the 9 Box of Controls, drive a "shift left and shift down" to better enablement, which results in the lowest risk, lowest cost, least amount of liability, and lowest control friction spot – so we can all "Protect to Enable" not only our organizations for today and tomorrow but also our customers.

I also hope that with the right discussion we can all focus on "not" positioning the work of managing risk as an "either this or that" function. We need to recognize and remember compliance does not equal security. We need to avoid positioning business velocity vs. business control. We need to avoid positioning privacy as a balancing act against the need for security. If we start with a mindset of trading these items off against each other, we will not be successful, because we will design our digital transformation to be at odds with the digital control needed to do this right. And then, we will be left with throwing money at symptoms after the fact, reactively detecting and responding to risk rather than fixing the problem from the ground up.

How emerging technologies can help

Any future security architecture we implement must provide better prevention, and it must also be more flexible, dynamic, and more granular than traditional security models. A new architecture also needs to greatly improve threat management. We need to do this in the upfront design, development, and validation during the creation of technology to reduce vulnerabilities well before the technology gets deployed. And as new attacks appear, we need a security system that is able to recognize good from bad in milliseconds, so that it can stop the bad and allow the good. For any attack that gets past these preventive controls, we need to be able to learn as much as we possibly can without compromising the user's computing performance or privacy. This information enables us to investigate exactly what occurred, so we can take immediate action to mitigate the risk whilst also learning how to prevent similar attacks in the future.

A control architecture should assume that attempts at compromise are inevitable—but we should also understand that it is possible to achieve real prevention for 99% or more of risks that could occur, including that of malicious code and zero-day attacks caused by mutated malware. Should a piece of malicious code attempt to execute, we can then instantly apply artificial intelligence and machine learning to analyze the features of files, executables, and binaries to stop the code dead in its tracks before it has a chance to harm the environment. For the remaining attacks—representing less than 1% of malware—we need to focus heavily on survivability.

Blockchain as explained early has significant value well beyond well beyond the implications a new form of money. By design, blockchains are inherently resistant to modification of the data. Once recorded, the data in a block cannot be altered retroactively. The implications then to use blockchains as a method to overcome many of the current weaknesses and vulnerabilities of the Internet and usher in a new age of trusted secure transactions is significant.

Quantum computing also offers exciting possibilities to enhance security as well. As mentioned earlier this type of leap forward in computing could allow for not only faster analysis and computation but across more data sets. Reducing the time to discovery in simulations can be used not only to aid research into things like new materials, drugs, or industrial catalysts. The tactic can reduce time spent on finding vulnerabilities in the design and development cycle for technology. This will then lower control friction on the developers of technology and increase the probability that they can find and fix a vulnerability prior to deployment. Doing so will not only lower secure design costs, it will speed up an organizations time to market with technology that is inherently less vulnerable to attack. The final result will be a broad reduction of societal and individual risks.

Artificial intelligence and more specifically machine learning are here today and Cylance is already demonstrating the impact it can have. As I mentioned in the initial section of my testimony Cylance is the first company to apply artificial intelligence, algorithmic science, and machine learning to cybersecurity and improve the way companies, governments, and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated artificial intelligence and machine learning with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be truly predictive and preventive.

In the future artificial intelligence and machine learning will also be able to solve other vexing issues that we face today such as passwords and identity management used to authenticate and authorize users. We will also be able to mitigate distributed denial of service attacks using the ability to predict and thus prevent in automated fashion the flood of requests that can so easily disrupt an organization today.

JFK once said, "The problems of the world cannot be solved by skeptics or cynics whose horizons are limited by the obvious realities. We need men who can dream of things that never were and ask why not." When AI, quantum computing, and blockchain are combined with right approach and right architecture the reduction in risk, the reduction on the cost of control, and the reduction in the control friction experienced by users and business will be dramatic.

MAKING SURE TOMMOROW IS BETTER THAN TODAY

The Perils and the Promise of Emerging Technologies for Cybersecurity

I read an article by Forbes leadership advisor and author Mike Myatt just a few weeks ago. I was reminded of something I was told a long time ago; "If there is a conversation you have been avoiding, that's the one to have."

I think there is a broader conversation that we as a security industry, as well as a tech industry, have avoided, and in some cases have intentionally distracted others away from having. In reality, there are two discussions – one for the creators/users of technology and one for the security industry. Both share a common conclusion that results in harm to others. Beyond that, both problems have a path forward that can address these failings.

What Every CEO Should Know

Myatt wrote a great piece last month titled Digital Transformation or Digital Free Fall: What Every CEO Must Know.

In the article, he astutely explains, "Innovation has always been synonymous with business survival and that hasn't changed. What has changed is the pace and scale at which businesses must innovate to remain competitive in a digital world. The speed of technology advances in the market are making the old paradigm of first mover versus fast follower largely irrelevant – every business must now become some version of a first mover.”

He also goes on to point out that “Digital transformation is really more of a leadership, culture, strategy, and talent issue than a technology issue. Real digital transformation occurs when business models and methods are reimagined by courageous leaders willing to manage opportunity more than risk, focus on next practices more than best practices and who are committed to beating their competition to the future."

In my second book, I published a set of 9 Irrefutable Laws of Information Risk. Law #9 states: "As our digital opportunities grow, so does our obligation to do the right thing." I believe this is a crucial point that was left out of Myatt’s piece.

Courageous leaders in digital transformation realize that business survival is also about managing risk, not just managing or chasing opportunity. Too many organizations today are chasing digital opportunities while risking their customers, and in some cases, society. Richard Rushing, CISO at Motorola Mobility, posted in December a picture from a presentation that read, "We're building self-driving cars and planning Mars missions - but we haven't even figured out how to make sure people's vacuum cleaners won't join botnets."

The Real Life Implications of Digital Transformation

Digital transformation as discussed throughout my testimony is embedding technology into the fabric of our lives. Typically, these technologies are meant to help or assist users, but one key element is often overlooked: Exploits that take advantage of technological vulnerabilities will increasingly impact the well-being of almost everyone in our society. So, it is incumbent upon all of us to properly shape the way we design, develop, and implement digital transformations to best manage and mitigate the information security, privacy, and other risks that are being generated, while still challenging ourselves to create technology that helps people.

The World Economic Forum 2017 Global Risk Report had Cyber Dependence in its top five risk trends, just below climate change and polarization of societies. It also indicated that "…technology is a source of disruption and polarization." I also believe technology is a tremendous opportunity for economic and societal benefit. I believe that technology can connect and enrich peoples’ lives − if done correctly and for the right reasons.

The 2017 Edelman Trust report, published recently, agreed that “we have a trust collapse”, adding, “We have moved beyond the point of trust being simply a key factor in product purchase or selection of employment opportunity; it is now the deciding factor in whether a society can function…the onus is on business to prove that it is possible to act in the interest of shareholders and society.”

A growing digital economy relies on trust. Breaking someone's trust is like crumpling up a perfectly good piece of paper - you can work to smooth it over, but it's never going to be the same. I have said it before and I will say it again: Managing information risk isn't about saying "No," it's about protecting to enable people, data, and business. We have to run towards risk to shape the path of the risk curve. CISO's need to do this, ideally, in front of business and technological opportunities or, at a minimum, in line with them. That is the best way we have to understand the risk dynamics to our organizations, shareholders, customers, and society. That is the best way to prevent risk that is avoidable in a proactive fashion.

If we carelessly implement technology in order to chase opportunities or simply prove that we can, we won't be successful in realizing digital transformations that can change lives and protect our people. Instead, we will be setting ourselves up for a digital disaster. By focusing on the opportunities along with our obligations to implement them right way, we can achieve digital transformation and digital safety to ensure tomorrow is better than today for everyone. With this mindset, we can avoid not only the digital free fall about which Myatt discussed, but also avoid the digital disaster that could lie ahead.

CONCLUSION

Thank you again for the opportunity to provide testimony. I will be happy to answer any questions.