Kansai University Keynote

July 15, 2016

John B. Higginbotham
Blue Ridge Networks, Inc.

Mr. Kusumi, Mr. Nambu, Distinguished Colleagues, Ladies and Gentlemen.

Kon nichi wa. Yoroshiku Onegai Shimasu.

It is my sincere honor to be with you today on this historic occasion of the 130th Anniversary of Kansai University. As a leading higher education institution, Kansai University has a rich heritage of making important contributions to Japan and indeed the world at large. We join in congratulating the University for its many decades of exemplary service and wish it continued success for many centuries to come.

Let me also congratulate my friends in Japan for the selection to host the 2020 Olympic and Paralympic Games here in Tokyo. This will be a great opportunity for the world to experience the warm hospitality of the Japanese people in addition to enjoying the exciting Games.

In keeping with its tradition of exploring topics important to society, the University has brought us together today to discuss cybersecurity. This is clearly an issue on the forefront for our governments, our businesses, and our citizens. Every day we hear reports in my country about harmful malicious attacks that expose private information, steal intellectual property and money, and threaten our national security. The unfortunate recent breach of JTB Corporation here in Japan underscores the reality that no civilized society is immune from these egregious acts.

Major effort is clearly underway to try to address cybersecurity threats. US Federal government unclassified spending this year for cybersecurity is approximately $14 billion which will increase more than 30% next year. Estimated spending this year here in Japan is over $6 Billion and is expected to grow more in the coming years. Various industry estimates place worldwide cybersecurity spending at more than $175 Billion with a projected compound annual growth rate approaching 10% for the next five years.

Yet despite these massive expenditures and the concerted efforts of many of the smartest people on the planet to address cybersecurity threats, the frequency and severity of harmful breaches continues to escalate.

How can this be?
What else can we do to address the challenge?
How can we measure progress?

Examining these questions is not an easy or comfortable task. There are no “silver bullets” or “crystal balls” to address the challenge. The difficulty in mitigating cybersecurity exposures in the face of our attempts to do so forces us to reexamine our perceptions, adjust our perspective, and try to think innovatively about the problem. My goal today is to hopefully offer some observations and insights that might be useful in that regard.

So, with all the money and effort being expended, how can it be that the problem is so bad and getting worse?

Over the course of the last couple of decades the world has experienced a digital revolution brought about through interconnectivity. The Internet with its relevant protocols was developed to maximize digital interoperability to create this globally connected world. For over two decades, we have designed, built, and deployed Information Technology and Telecommunications systems and networks to purposely deliver these open Internet architectures with an objective of creating this digital revolution. We can take pride in the fact that it worked. The adoption of Internet and the creation of an interconnected world transformed our traditional industries, created whole new industries such as social media, and provided global opportunity at a scale unimaginable a generation ago.

It should therefore come as no surprise that we have been challenged to try to place security controls, access restrictions, and use limitations on the very systems and networks we deployed to maximize open access and interoperability. Efforts to reconcile these conflicting objectives evolved toward conventions to define legitimate uses, monitor operations and react to undesired activities with minimal impact on the operational utilization desired. Accordingly, conventions for legitimate use evolved toward password, certification, authentication, and similar control mechanism. The predominant protection approach to maintain efficacy of these use controls emerged as detection and response to anomalous events as observed. This allowed us to continue to utilize open architectures with little operational impact while providing some ability to identify and react to misbehavior in some fashion. Cybersecurity products using this approach, such as anti-virus, white-listing, and breach detection systems were designed to monitor or scan activities, identify compromises or anomalies, and, if detected, try to stop or limit the damages.

This approach to cybersecurity security worked very well for many years. But as more and more valuable data became digital in form and accessible in an open interconnected ecosystem, compelling incentives emerged for cyber adversaries to acquire more sophisticated capabilities and organized their efforts to systematically engage in their misdeeds. Their efforts have been successful. The costs to an enterprise for addressing a successful breach have steadily escalated to millions of dollars per event. The damage to a large enterprise from lost customers, enterprise value, disrupted operations, and other liabilities are in the billions of dollars. Consumers face spending hundreds of dollars per year each to remediate breached computers and try to repair the effects of identity theft. Nations face increasing cybersecurity budget demands in fiscally constrained environments to try to address risks to public safety and national security. In short, this business has become big business with big risks.

The cybersecurity threat landscape that has now evolved presents persistent threats designed to evade detection and limit our ability to react to it. PandaLabs recently reported that there are more than 200,000 new forms of malware every day which include file-less malware, weaponized documents, in-memory attacks, phishing attacks, ransomware, and many other forms of threats designed to evade detection by even the best-in-class providers of detection and response based products. Unfortunately, the TrendMicro prediction that 2016 would be the Year of Online Extortion from ransomware has come true evidenced by the almost daily reports of such widespread attacks throughout the world. It is a disappointing admission of the helplessness of conventional cybersecurity protections that the typical response of our law enforcement authorities in the US to a company breached by ransomware is to pay the ransom. The US House of Representatives Small Business Committee has estimated that more than

60% of small businesses successfully attacked by ransomware and similar malicious cyberattacks cannot survive the economic damage and will go out of business.

Efforts by larger enterprises that can afford to deploy multi-layered defense architectures in response have primarily manifested as deployment of multiple vendors at multiple locations in a network all using some form of a detection and response technique. This approach at defense-in-depth, however, does not necessarily yield a diversified defense against emerging undetectable threats. Reliance on the same protection technique at all layers potentially introducing a common vulnerability across all layers. If an adversary can defeat a common technique, it can likely defeat any vendor's manifestation of that technique anywhere in the enterprise. This risk factor can actually be exacerbated through the laudable effort to establish best-practice standards for compliance if those standards are all based upon the same convention. If all defensive systems are built using the same standard protection convention, then all an adversary has to do to defeat any particular system or architecture is to determine how to defeat the standard convention. Compliance with standards therefore is not necessarily protection.

Thus, perceived best-in-class compliant multi-layer defenses continue to be vulnerable to attacks that can remain undetected for weeks, months, or even years, before a breach is discovered, often only as disastrous effects become known. The breaches of the US Office of Personnel Management (OPM) went undiscovered for almost a year extracting sensitive information of more than 20 million US government employees their families. The disastrous implications of the permanent damage to their privacy and safety from the exposure of their valuable personal information for the rest of their lives and the risks for the US government from this breach is hard to predict.

As interconnectivity expands to more and more operational environments, the exposures are moving from economic and privacy risks to matters of public safety. Potential vulnerabilities have already been identified in the automotive control systems, maintenance networks, and mobile passenger networks of most automobile manufacturers. Increasingly interconnected air, rail, and other transit systems have been demonstrated to have similarly exposures. Vulnerabilities in industrial control systems for power, natural gas, and other forms of energy production and distribution introduce exposures at a national scale. The recent successful attack on Ukrainian power plants by fileless malware undetected by conventional protections affected power systems throughout the country disrupting government and businesses and endangering their citizens.

The difficulty of trying to evolve and extend effective classical detection and response multi-layer defense protection to endpoint interconnectivity in the Cloud is clearly apparent. This challenge will escalate as the marketplace expands from over 10 billion connected endpoints today to potentially more than 50 billion interconnected Internet-of-Things (IoT) devices globally by 2020. Relying on an ability to detect and respond to every attack, anomaly, or malicious behavior in such an IoT world as a first-line cybersecurity defense seems a bit incredulous. I liken it to trying to monitor every grain of sand on every beach in the world every time a wave hits to try to detect and identify the individual "bad" grains of sand. The processing and operational overhead on systems, networks, and personnel for this approach is likely infeasible particularly for low cost, low capability systems at the IoT edge. Erosion of productivity, user and administrator frustrations, and increasing sustainment costs may overtake the benefits of any perceived protection from relying on such reactive cybersecurity approaches.

No one questions the value of monitoring systems and enterprise operations with the ability to detect and respond to anomalous conditions to ensure information assurance compliance and provide overall

sound maintenance of enterprise network operations. But the marginal utility of reliance on compliant detection and response approaches for the purpose of a first-line primary cybersecurity defense may well have reached the point of diminishing returns.

So what else can we consider to help address the challenge?

There is an emerging recognition in the cybersecurity industry of a need to evolve from a perspective of Compliance to a perspective of Resilience. Compliance conventions provided us with the ability to try to define best-practice then systematically manage to implement it. But static compliance rules and regulations often locked us into technology choices and operational methods our defenses more predictable, and, therefore, targets more exploitable. Reexamining our cybersecurity posture in the context of Resilience affords an opportunity to leverage the foundation created from Compliance efforts to introduce new conventions to address the evolving cybersecurity challenge. This enlightened perspective allows us to examine methods that can proactively prevent harmful breaches even in an ever changing threat environment.

Our industry has classically perceived Information Technology challenges in a context of tangibles such as systems, networks, or people. As we move more and more toward a digital, interconnected, virtual world, we are being driven to reorient our perspective to a context of intangibles, such as processes, states, and outcomes. Our company, Blue Ridge, has found viewing the cybersecurity challenge in this manner useful in developing axioms for guiding us in developing effective cybersecurity solutions resilient to the threat environment. Some of these axioms may be of interest and offer some useful perspective in our discussions today.

- The target is the data or a process - not a system, network, or person.
- The attacker is a thing (malware) – not a person.
- The attack itself is a process - not a thing (malware).
- The compromise is a change in state in the target (data or legitimate process) brought about by a successful attack (malicious process).

The objectives of any malicious cybersecurity adversary are primarily data exfiltration or modification of a legitimate process to create an undesirable outcome. Isolating the target (the data or legitimate process) from the attack (the malicious process), rather than trying to find the attacker (the malware), provides a path to resilient protection without dependency on identifying or detecting the attacker (the malware) or the attack (the process). If an attack (a malicious process) cannot “detonate”, it is defeated before it can ever occur (no malicious process occurs, therefore, no compromise occurs).

This concept of isolation of targets from attacks for next generation cybersecurity protection is now being recognized as a viable path to create proactive breach prevention. With the advent of the Cloud, network perimeter defense moved to the new battlespace of endpoints and servers. moved to the hosts (endpoints and servers). W with the introduction of isolation concepts for protecting processes and roots of trust, the potential for defining virtual perimeters at the host level have emerged. This provided an opportunity to contain, or guard, these isolated processes to deliver proactive, prevention defenses.

We can extend this perspective of examining the intangibles to generate potentially useful insights for network and Cloud operations.

- All networks (and by extension the Cloud) are inherently untrustable.
- Sharing secrets in these networks (Cloud) is therefore inherently vulnerable to exploit.
- Isolating data-in-transit sessions and processes can provide protection from vulnerabilities.

Increasingly networks and by extension the Cloud are being viewed as inherently untrustable, a viewpoint shared by Blue Ridge. By its very nature the Internet Cloud is created from an open interconnected network of disparate networks of multi-vendor, multi-generational systems rendering it is essentially impossible to trust. Standards for encryption, authentication, certification, authorized libraries, and other controls are as readily available to adversaries as they are legitimate users and providers. Thus attempts to protect legitimate operations within the Cloud have remained vulnerable to exploit. By applying isolation and containment techniques in a virtual context, our firm has been able to demonstrate that it is feasible to isolate session authentication processes, data-in-transit, and network management from the Cloud eliminating exposure to persistent Cloud vulnerabilities.

Introducing these isolation and containment techniques to create preventive protection can lead to enhancements for predictive threat intelligence. Most detection and response approaches rely on identifying Indicators of Compromise (IoC) to characterize an attack after it has successfully occurred in an effort to respond as quickly as possible to limit the effects of a breach. Recording or capturing the data associated with an attack attempt that was prevented provides valuable Indicators of Attack (IoA) without the compromise actually occurring. This delivers the earliest possible characteristics of unknown, undetectable attacks without having the crisis of a breach. This IoA data can actually enhance the value of detection and response endpoint and network tools to proactively maintain cybersecurity hygiene, accomplish comprehensive compliance reporting, and maintain an effective information assurance posture. The effectiveness of multi-layer defenses can be enhanced by materially reducing or eliminating the overhead associated with inefficient monitoring, patch processes, and administrative dependencies. Threat intelligence effectiveness can be enhanced by the reduction or elimination of false positives and false negatives for threat analytics and the identification of system and operational vulnerabilities for remediation proactively before a compromise actually occurs.

Introduction of protection capabilities utilizing isolation and containment principals in conjunction with detection and response capabilities already widely deployed has demonstrated great promise for creating a resilient, preventative cybersecurity posture. My colleagues at Blue Ridge have been able to develop and patent pioneering technologies that can isolate and contain virtual processes to create Trusted Enclaves and Trustable Communities in a dynamic environment for endpoint operations and network sessions through the Cloud. Our AppGuard breach prevention system has been recognized by Gartner and others as a leading example of this new industry approach for endpoint protection. Our experience in the field with this technology has proven that it is feasible to deliver effective breach prevention without requiring detection or having enterprise dependencies. Our firm is proud that our endpoint protection and network security solutions have been proven effective in the field for many years with customers for their use cases with no reported breaches.

So how can we determine if we are making progress?

At one level, for many enterprise operations, the economics of cybersecurity can be measured in a predictable fashion. When we see the frequency of successful breaches and the cost of a successful

breach begin reducing, we will know we are making progress. The investments needed to accomplish this outcome can be measured and analyzed to determine a cost-benefit ratio.

But in an uncertain dynamic interconnected environment with ever changing threat parameters, this assessment of cybersecurity posture is not so simple to produce. The need to create resiliency necessarily forces us to engage in looking forward for many years to come as to the nature of the threats and the exposures they create relative to often unpredictable demands from the business environment of the enterprise. This becomes therefore a complex process of making tradeoffs of choices in technologies, management systems, organizational priorities, and many other variables that are difficult to assess. How does one really measure cybersecurity in an economic context when the ultimate outcome is that nothing happens and there is no economic loss? Where does the threshold cross from making necessary investments for effective cybersecurity to inefficient allocation of resources? Where does the liability shift from customer responsibility to enterprise responsibility to personal responsibility for Directors and Officers? What is the right level of regulation to ensure cybersecurity effectiveness without detracting from the benefits of the good and services it is protecting?

Thus, cybersecurity is not a state or condition but rather requires an on-going diligent management process to maintain efficacy. With this recognition, many organizations have elevated cybersecurity to a core corporate function led by a Chief Information Security Officer (CISO). Enlighted organizations recognize that in an increasingly interconnected world with ever more sophisticated cyber adversaries, on-going vigilance is needed to continue to provide effective, resilient, futureproof cybersecurity solutions to keep the trust and confidence of customers and the public. An effective CISO can help integrate cybersecurity as a part of the operations of the enterprise in an effective and affordable manner with benefits for its operations, its customers, and its reputation with the marketplace

Which emphasizes that we have reached an inflection point for cybersecurity. It is now about earning and keeping the trust of our customers and the public to protect their safety. Their very lives are at stake for our decisions and actions making this serious business with serious consequences. As interconnected operations increasingly include energy, transportation, healthcare, and other critical infrastructure sectors, the stakes for malicious exploit to create harm have never been higher. The decisions we make today for cybersecurity will define the posture of tomorrow on which our customers, employees, citizens, and indeed the world at large, will rely. There is no higher standard of care that can motivate us to do the things necessary to deliver effective, resilient, and reliable cybersecurity to safeguard public safety.

Reexamining the current performance of conventional detection oriented cybersecurity in the context of safety emphasizes the nature of the challenge. Some detection-based cybersecurity vendors proudly proclaim detection rates approaching 99%. Even if that were true, what this means is they fail to detect malware 1% of the time. With over 200,000 new malware forms per day, as mentioned earlier, that means even some perceived best-in-class detection tools fail to discover over 2,000 new malware forms every day. There are over 1 billion cars in the world interconnected to some degree already. Would we accept 10 million life threatening automotive accidents per day from exploits of common vulnerabilities? There are now more than 100,000 airline flights per day highly dependent upon digital interconnectivity. Would we accept over 1,000 life threatening accidents per day from cybersecurity exposures? Clearly in the context of safety, the performance of conventional detection oriented

cybersecurity is not acceptable exposing the fallacy of the marketing hype. To address safety for the public good, the industry needs to adopt a zero tolerance for failure mentally. It needs to embark with a concerted effort to integrate quality cybersecurity technologies and processes as a core part of the interconnected world that can resiliently prevent cybersecurity failures from happening in the first place. I hope you find some of the concepts presented useful for our discussions today and look forward to a productive conference.

Again, thank you to Kansai University and the sponsors for organizing this event and for the opportunity to offer these remarks. I also look forward to a safe and enjoyable 2020 Olympic and Paralympic Games here in Tokyo.

Doumo Arigato Gozaimashita.