Input to the Commission on Enhancing National Cybersecurity

David Kleidermacher, Chief Security Officer
BlackBerry, Ltd.

Executive Summary

[Relevant to the following Topic Areas: Critical Infrastructure Cybersecurity; Cybersecurity Insurance; Federal Governance; Internet of Things; Public Awareness and Education]

The United States continues to suffer from a constant stream of data breaches and other cybersecurity failures that harm not only the economy but also public trust in national cybersecurity systems and confidence in the ability of the public and private sectors to meet emerging cybersecurity challenges. As governments and enterprises increasingly leverage connected electronic systems, including the Internet of Things, these concerns and failures are likely to increase. Many reactionary initiatives, both public and private sector, focus on the need for new and improved cybersecurity technologies and best practice guidelines. Yet despite enterprises spending $75 billion on cybersecurity technology in 2015 and massive equity investment in cybersecurity companies, the rate and cost of breaches continues to rise.

Introducing new security technologies to counter threats is like experimenting in new ingredients without understanding how they will translate into a great meal. We are missing the critical first step in our cybersecurity strategy, the recipe if you will: effective security assessment programs to generate assurance, or confidence, in the ability of critical systems, components, and applications to protect themselves against relevant threats. An effective assessment program leverages security technologies, but the assurance horse must lead the tools and technology cart.

The need for these programs has been noted by NIST with regards to its excellent cybersecurity framework: NIST has "*no plans to develop a conformity assessment program*." Rather "NIST encourages the private sector to determine its conformity needs, and then develop appropriate conformity assessment programs."

We believe the Federal government must expand its leadership role in making sure this happens. In the near-term, we propose NIST work with industry to perform a broad comparative study of modern security assurance programs used throughout the world. However, our primary recommendation is that NIST contribute to the promulgation of these programs, such as DTSec, that are dedicated to open, multi-stakeholder, cost-efficient security assurance for critical national security systems and components. Without open, independent assessment programs to gain assurance, technical mechanisms and guidelines alone will never generate the confidence we need to address the current threat imbalance. We can't hope to raise the cybersecurity bar if we don't first know how to measure its height.

Current Challenges in Cybersecurity Assurance by Assessment

Current security assurance programs that exist today are challenged due to a perception that too much time and money are spent to achieve a relatively low level of assurance. As a technology supplier that puts its products through numerous security evaluations, it seems likely that the amount of money and time developers, test labs, and assurance program administrators spend could be dramatically improved without assurance degradation (or we can enhance assurance with the same spend).

FedRAMP is a newer, promising effort. FedRAMP's inclusion of vulnerability assessment and penetration testing represents a meaningfully improved level of assurance relative to other programs, although a rigorous cost-benefit analysis is premature at this point. In addition, FedRAMP targets cloud systems used directly by federal government. Critical infrastructure assurance programs must expand to cover systems and components developed and deployed in critical environments beyond direct use of federal government. For example, the European smart card integrated circuit market has achieved a great many successful security evaluations (backed by non-profits EMVco and Eurosmart) over many years at relatively high assurance, implying a reasonable assurance-to-cost balance in these systems used across the world' financial sectors. In the connected medical device industry, a new security assessment standard called DTSec (described in more detail later in this document), also tries to achieve higher assurance at reasonable cost, but is also new and lacking federal backing to assist adoption.

The realm of cybersecurity assessment standards, similar to safety and quality standards that also impact electronic systems and their developers, can be broken into two categories:

1. Process/Methods-Based: Standards that focus on organizational process and maturity (including the system development lifecycle)
2. Systems-Based: Standards that focus on the systems, subsystems, and components (collectively referred to as "systems" herein) developed by those organizations

Most of us in the cybersecurity professional world believe that ultimately the first type deserves more developer and industry attention, investment, and focus than the second: if we can't institutionalize the proper processes and practices within our development organizations, good security in production systems will remain elusive.

However, the second type is necessary, and is the only way to generate independent assurance that the first type has been applied successfully in the systems that matter. In fact, an assessment program for systems is the carrot (or stick) that drives organizations to adopt the first type. Consumers of technology ultimately care more about the system being secure, rather than an organization's internal practices. For example, we drive vehicles, not car companies. Ultimately, the system must protect us. In essence, the first type is the means to an end, the second type.

The two types of standards need not be mutually exclusive. For example, a system-based standard can (and often does) reference and incorporate organizational lifecycle processes as a method of enhancing confidence that the system meets its security functional requirements. However, a separation of these two standards types may provide increased

flexibility for developers. A developer can choose potentially from multiple high quality process-based standards, as well as proprietary lifecycles, as long as the produced systems can fulfill their security objectives. Nevertheless, if a developer chooses not to follow standardized lifecycle processes, subsequent system assessments may be more expensive and take longer to complete.

Determining a System's Security Objectives and Functional Requirements

Modern computer and electronic systems are exposed to a complex set of constraints and stakeholders that make it nontrivial to determine the appropriate set of security controls. Poorly selected security controls can have unintended, deleterious effects. Other commercial influences can impact security control selection, including product and component cost, power constraints, wireless network and protocol throughput and latency characteristics, and threat model – just to name a few. Ultimately, each system must be associated with a set of security controls that represents the collective best practice view of applicable stakeholders. Furthermore, the appropriate set of controls will vary over time and across system instances as new threats and remediations emerge. NIST has done a great job in creating control catalogues (e.g. NIST SP 800-53), which have been leveraged successfully in federal assessment programs (e.g. FedRAMP), but we must extend these programs to many more places, products, and systems.

Obtaining Assurance in the System's Ability to Meet its Security Functional Requirements

The digital world widely suffers from an assurance crisis: systems routinely fail to deliver on explicit or implied security promises, resulting in a lack of consumer confidence and trust in those systems. The problem is so pervasive that even the most trusted electronics vendors and security companies have been subject to embarrassing, confidence-killing hacks. For example, RSA, one of the world's foremost security firms, was hacked in 2011. iMessage, touted by Apple as an exemplary secure messaging system and used for trillions of messages by hundreds of millions of users, was found to be vulnerable by Johns Hopkins researchers who discovered multiple security flaws in its design. A hospital infusion pump manufactured by one of the largest healthcare companies in the world was recently found to have severe security vulnerabilities, prompting the FDA to issue a warning and recommendation to detach these systems from hospital networks. These examples are but a small set of a practically unending litany of security problems across all electronic products and industries. As far as can be deduced in the public domain, none of these systems underwent an independent (results made available to the applicable stakeholder community, including customers), rigorous security assessment as part of the process of developing and fielding the product.

Recently, a cybersecurity research firm alleged that security vulnerabilities in a connected cardiac medical device – a "smart" pacemaker and monitor combination – made by St. Jude Medical might put patients' lives at risk. The alleged vulnerabilities exploit security flaws to crash the implantable pacemaker or drain its battery. Either could be fatal to patients whose heart can't beat correctly without a functional pacemaker. In an precedented move, the cybersecurity researchers sold their findings to a hedge fund, which shorted St. Jude's stock, and the security research firm is being compensated by the fund's performance. While St. Jude and other researchers are disputing the claims, the public is left with a "he-said, she-said" situation that contributes to the crisis of confidence in digital system security. While much will be debated about the veracity, legality, and ethics of these researcher and hedge

fund activities, the important takeaway is that it reinforces the urgent need for open security assessment programs for critical systems, which we increasingly depend upon for our health and privacy.

To use another recent high-profile example – the hacking of a Jeep by security researchers wherein the automobile's telematics system was breached in order to access and disable critical braking and steering systems - we must define the "right" set of security functional requirements (protections) for a telematics system and then obtain assurance that such hackers (or rather, their blackhat counterparts with similar attack potential) are unable to defeat those protections. In the case of automotive systems, the stakeholders who seek this assurance may include consumers, public sector regulators and standards organizations, manufacturers, second and third tier automotive suppliers, dealers, liability attorneys, insurance companies, independent cybersecurity experts, consumer advocacy organizations, automotive professional organizations, and academic researchers. It is important to note that relying on self-assertion of conformance to good security standards has proven insufficient and dangerous across all industries; assurance through independent evaluation accessible to relevant stakeholders is needed.

Recommendation

Having been involved in a wide range of quality, safety, and cybersecurity standards and assurance programs over two decades, we deduce a common set of characteristics of cybersecurity assessment programs most likely to succeed:

1. Multi-stakeholder ownership and open collaboration to manage the assurance program; not just vendor and government regulator, but independent cyber security experts, customers, applicable industry organizations, etc.
2. Risk-based assessment of threats to deduce an appropriate set of security objectives, requirements, and level of assurance needed for systems
3. Efficient evaluation process (cost and time), with public disclosure of approved systems in order to maximally leverage results
4. Continuous improvement in order to manage the rapidly evolving reality of threats and technology

We propose that NIST, in conjunction with other applicable agencies, be empowered to motivate these kinds of programs across critical infrastructure. This leadership must go beyond issuing guidance and recommendations, although we do not recommend government own and manage new assessment programs. For example, NIST could fund multi-stakeholder non-profit organizations to create or maintain these programs, take leader participatory roles in them to ensure consistent quality, and mandate or provide other economic incentives to achieve adoption and conformance. The latter is perhaps most critical for success: lacking a financial incentive, industry has proven time and again it will fall short of what is required to protect our most critical systems from breach. Even the best technical approaches to conformance assessment will fail without the proper incentives that push industry to utilize these assessment programs. A comparative study of modern security assurance programs, such as DTSec, would be a sensible antecedent to this investment.

The benefits of high quality security assurance programs for industrial developers and suppliers are numerous, including:

- Ability to obtain assistance in determining an appropriate set of security controls that meet the needs of all stakeholders;
- Ensure security efforts are assessed and confirmed by independent cybersecurity experts;
- Provide confidence in security by documenting which systems have been successfully assessed;
- Reduce legal, financial, and brand damage risk by demonstrating systems have been subjected to the commercial best practice of an open, standardized, independent security assessment process;

And of course there are benefits to other stakeholders, including:

- Let insurers (cyber insurers and other) more accurately assess cybersecurity risk and offer optimized insurance plans based on assessment results, reducing financial risk for insurers, manufacturers, critical infrastructures, and consumers;
- Enable consumers and other purchasers to choose products and systems wisely and reduce cybersecurity risk.

Case Study: Connected Medical Device Cybersecurity Assessment Standards

As national critical infrastructure increasingly leverages commercial-off-the-shelf (COTS) technology, we see the confluence of mission critical requirements and demanding, cost-sensitive mass-market consumer product lifecycles and constraints.

In connected medical devices, cybersecurity standards are also nascent. The DTSec cybersecurity assurance standard was first released in May 2016, and the first set of medical device manufacturers are just beginning system evaluations. DTSec uses system-dependent profiles, created using a risk-based approach by a broad multi-stakeholder community, to define security requirements for a system. System-specific vulnerability assessment and penetration testing are required as part of the profile. Multiple profiles can be used for different families of systems (e.g. diabetes devices vs. hospital infusion pumps). While the standard highly encourages re-use of existing lifecycle process standards and associated assurance documentation to assist the system evaluation (as these are often institutionalized in medical device manufacturing organizations), this lifecycle is not strictly required. As part of its mission to remain cost-efficient, DTSec also strives to reuse other standards and regulatory and non-regulatory guidance where applicable and sensible in deriving security functional requirements. Other factors influence this selection. For example, the stakeholder community takes care to ensure that safe clinical use is not adversely impacted in the risk-based specification of security objectives and requirements.

What sets DTSec apart from other earlier cybersecurity assurance programs, in addition to the multi-stakeholder community approach organized by a non-profit, is the steadfast requirement for efficient (in cost and time) evaluation by focusing less on paper-based analysis and organizational lifecycle requirements and more on vulnerability assessment of the system itself. We propose that federal government promulgate this multi-stakeholder approach to all systems and industries critical to national security and safety.