CYBERNANCE
First In Cybergovernance

Commission on Enhancing National Cybersecurity

RFI Response

Submitted by Charles F. Leonard – September 9, 2016

Introduction / About Us

In the summer of 2014, SEC Commissioner Luis Aguilar stated that *"boards who choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril."* This statement came shortly after the initial publication of NIST's *Framework for Improving Cybersecurity Infrastructure*, and foretold the ascendance of cybersecurity from the server room to the boardroom. Two years later, we operate in an environment where statements like "cybersecurity is more than a technology problem" are met with knowing agreement. This environment reflects the growing recognition that cybersecurity is only one piece of a larger issue – cyber risk. Effective management requires engagement, oversight, and leadership from the highest levels of the organization.

The spirit of the NIST Framework is reflected in our mission as a company – that **cyber risk must be addressed using risk management principles that are led by top executives.** Cybernance was formed to address the growing recognition that cyber risk is an issue that spans the entire economy – not just a few sectors – and that effective management of this growing threat will require adoption of standards such as those developed by NIST. When we are able to apply standards to the cyber risk equation, then we will be capable of building quantitative models that create a common language for addressing risk. These models will help us adapt to our risk environment – collectively and as individual firms – using financial incentives and pricing mechanisms like cyber insurance.

Reflecting this spirit, Cybernance developed a software platform that programmatically implements the NIST Framework for Improving Critical Infrastructure Cybersecurity. NIST encourages organizations of all types and sizes to implement control structures that help them to "Identify, Protect, Detect, Respond and Recover" from cyber incidents. Our software will systematically assess, measure, report, and prioritize the risk management and security controls an organization has in place, and benchmark them against the NIST standard. In doing so, our customers are able to monitor their cyber risk posture over time, track improvement, and compare their results against a relevant set of aggregated data. The benefits accrue not just to one organization, but to the entire ecosystem as we identify common markers of excellence or deficiency. This standards-based collection of data is vital for cyber insurance brokers and underwriters whose business success is tightly coupled with their ability to quantify risk.

Our mission is to create a standards-based environment for risk quantification, so that diverse stakeholders can talk in a common language and create economic incentives for effective risk management. The following report will explain our view of the world in which this mission will unfold.

Structure

This report builds on the recorded wisdom of the expert panelists who convened to speak to this Commission. In many cases, those panelists concisely and eloquently articulated our sentiments better than we could ourselves. Rather than paraphrase or rephrase, we have included relevant quotations and citations from those panelists. These comments illuminate and support our overall view of cyber risk, which is refined through three lenses: Cyber Insurance, Federal Governance, and Organizational Management.

Review of Panelist Statements

We began preparing for this report by conducting a thorough review of statements made by the panelists who sat for this Commission from May – August 2016. From a variety of disciplines, perspectives, and backgrounds, the panelists offered a view of cyber risk and security that aligned remarkably well with our own. In particular, many panelists identified areas that we consider critically important to effectively address this challenge: **Cyber Insurance, Federal Governance, and Organizational Management.** We will use these broad topics to frame our views in this report.

Cyber Insurance plays a critical role as the connective tissue between those who set the rules and those who must implement them. Comments on this topic tend to cluster around issues like policy development and the creation of standards, and around the use of both in search of methods by which companies can be judged against a common yardstick. Cyber Insurance serves to create tight connections between Federal Governance and Organizational Management.

Federal Governance is fairly self-explanatory. Within this category we find discussions of public-private partnerships, regulation and policy, standards creation and enforcement, responsibility for critical infrastructure, and geopolitical concerns connected with all of the above.

Organizational Management contains anything related to the treatment of cyber risk and security within modern organizations. It begins with recognition that cyber risk is borne of security and privacy issues that extend beyond technology. Comments about Organizational Management often focus on corporate governance, organization structure, and company culture.

Expansion of Statements

Cyber Insurance

We believe strongly in aligning incentives with desired outcomes. Historically, questions about how to create incentives that reduce risk have found their answer in the use of insurance. The insurance industry's intellectual capital is an accumulation of over a century of research about risk modeling and pricing. So if insurance is a critical component in enhancing security, then the question to answer is, *"How can we clear the way for insurers to perform their work?"*

Several panelists keyed in on this issue:

> *"Insurers have a long history of gathering large amounts of risk and loss data for the very purpose of lowering insureds' risks and the potential for insurance payouts."*
> *– Randall Milch (Distinguished Fellow, NYU Law School, May panel)*

> *"Naturally, the market will differentiate sharply among applicants depending on how the company approaches the **people, processes and technology that affect cybersecurity.** That differentiation comes in the form of premium dollars. Pricing pressures drive insureds to adopt best practices."*
>
> *– Peter Beshar (EVP & General Counsel, Marsh & McLennan Companies; May panel)*

These statements paraphrase and echo the consensus of the insurance industry at large, and they hint at the optimal conditions of an effective cyber risk pricing environment. Generally speaking, actuarial models improve with large quantities of data. But those models gain value more quickly when the data is specific, structured, and standardized.

> *"The underwriting process, by identifying a set of best practices across industries, creates important incentives that drive behavioral change in the marketplace."*
>
> *– Peter Beshar*

Although these panelist statements describe the ideal functions in theory, in practice the environment for cyber insurance is not yet optimized for data collection and risk modeling.

> *"For long-standing risks, actuaries rely on decades of claim data to set premium rates and reserves. For emerging risks like cyber, insurers need to develop new approaches and techniques to guide their underwriting practices."*
>
> *– Peter Beshar*

> *"Insurers complain of too little time with an insured to gain a comprehensive understanding of the company's risk profile. The three-way relationship [insured / broker / insurance company] … places significant time limitations on precise risk assessment … Thus **the mechanics of selling***

> ***commercial insurance today seem incompatible with getting full cyber risk information** about an insured."*
>
> *– Randall Milch [emphasis added]*

Panelists spoke at length on the need for standards that will guide the definition of best practices, which in turn will give rise to an understanding of what data are relevant and how they should be collected. Older forms of insurance eventually settle into a clearly defined understanding of what drives risk. Once identified and defined, those risk drivers can be quantified and subsequently managed, mitigated or otherwise controlled. This is already happening.

> *"The Framework is increasingly being utilized as a basis for an expanding cyber insurance market; and, regulating agencies are harmonizing their regulatory approaches with the NIST Framework."*
>
> *– Robert "Bob" Kolasky (Deputy Assistant Secretary for Infrastructure Protection, DHS, July panel)*

The insurance industry exhibits a natural tendency to seek standard measures of risk (or to develop their own). By developing and embracing a standard that is adaptable to industry, academia, and government – as well as internationally – we can move more quickly toward the optimal environment for accurate risk pricing.

> *"An additional approach could be insurance-backed cyber 'safety standards.'… An independent 'rating' institute could be of significant assistance to companies, particularly in assessing risks in the parts of the cyber eco-system where providers often markedly limit their own liability…"*
>
> *– Randall Milch*

Thus, the process of measuring, aggregating, modeling and pricing risk will benefit greatly from the development of standards. There is widespread consensus that the NIST Cybersecurity Framework should be the standard – and indeed already plays that role in an informal sense.

Federal Governance

In the area of Federal Governance we see two major topics. Again, a number of panelists put forth views that align with our own, and in those cases we've simply echoed their succinct phrasing. The main topics, broadly speaking, are:

1) policy development and regulatory regimes,
2) creation and stewardship of standards, and
3) critical infrastructure protection.

1. Policy & Regulation

On the first issue of policy and regulation: we see distinct similarities between the threat of cyber breach in today's environment, and the threats posed by large-scale financial scandals in the late 1990's and early 2000's. Following the high-profile scandals that led to the collapse of Enron, Worldcom, and others, there was a strong push for regulation to govern financial disclosures and reporting. Today, we know these rules as Sarbanes-Oxley, and they've given rise to a massively complex regulatory and compliance regime.

Similarly today, we see and hear widespread discussion about cyber legislation following high-profile breaches at Target, Home Depot, Sony, and others. What form that legislation might take is not yet defined, but it seems clear that we are heading in that direction. Therefore, it is important that we encourage an active debate concerning what type of rules will be most beneficial.

We believe firmly that prescriptive, one-size-fits-all rules are unwieldy and counterproductive. More often with this approach, *one size fits one* – and for that matter, not for very long. The diversity of cyber threats and bad actors combined with their myriad motives and tactics is complex enough. The notion of prescribing universal methods by which varying industries (each with highly variable risks and exposures) should tackle cyber risk is hard to contemplate.

> *"We continue to see an increasing interest among certain agencies in the Federal government on prescriptive regulatory responses to cybersecurity threats … A prescriptive regulatory 'solution' would simply set a lowest common denominator bar that would create a disincentive for the innovation and agility needed to respond to an environment that is characterized by nimble and sophisticated hostile actors and constantly-evolving threats."*
>
> *– Chris Boyer (AVP Global Public Policy, AT&T, July panel)*

As we advance our collective understanding of the cyber issue, we will continue to see a broader acceptance of the idea that *this is not simply an IT and technology problem.* Boiled down to its essence, *cybersecurity poses a risk management and governance problem*. A risk-based approach will be most effective in equipping and empowering leaders, managers, and executives to make informed decisions about operations using a construct that recognizes risk as a driver of business value.

> *"The NIST Cybersecurity Framework has been successful as a mechanism for responding to that environment. It recognizes the diversity of companies and the need for flexible and evolving solutions, and allows companies large and small to tailor the Framework to their specific business needs commensurate to their risks."*
>
> *– Chris Boyer*

2. Stewardship of Standards

From this shared perspective, we enthusiastically embrace the NIST Framework as a standard that should be applied as broadly as possible. Federal Governance, then, should focus on efforts that ease the adoption and application of the Framework – not on regulation that mandates compliance with specific rule sets.

The Cybersecurity Information Sharing Act of 2015 (CISA) was in large part intended to ease impediments to companies sharing threat information with one another. That is, rather than being a punitive regulation, it was designed to help companies engage one another constructively about cyber threats without fear of litigation from parties claiming damages from cyber breach. This is encouraging and it will be more successful when we improve standards that define what "information sharing" really means.

Of course, this can't (and shouldn't) be done overnight. It will require thoughtful discussion about intersecting issues like privacy and liability, two critical issues that lived at the core of the debate over CISA. This debate should continue, and we should embrace a standard for best practices and terminology to act as the rails for the discussion. Panelists offer nearly unanimous support for the adoption of NIST as the national standard. Indeed, it has already become the *de facto* standard among most practitioners and leaders.

> *"I think it's critical that we approach this question with a shared lexicon."*
> *– Mark McLaughlin (CEO, Palo Alto Networks, June panel)*
>
> *"Harmonize rules and guidance. There is a multiplicity of frameworks, standards and guidelines for cyber-security… we would recommend that we continue to emphasize the NIST Cyber Security Framework and in particular the development of associated profiles."*
>
> *– Phil Venables (Managing Director, Goldman Sachs, May panel)*

With that understanding of the need for a common lexicon and a harmonized system for communicating and measuring risks, we return to our discussion of the role played by insurance. The insurance industry creates risk models, pricing mechanisms, and financial incentives to drive behaviors toward desired outcomes. These models serve as the basis for risk pricing and will be greatly enhanced to the extent that they can be built using standards. Federal Governance should focus on easing, facilitating, and accelerating the adoption of NIST as a national standard across industry, academia, and government. To the extent these efforts are successful, we will rapidly strengthen the connective tissue that binds the technology and data infrastructure of the economy.

3. Critical Infrastructure

People often think of critical infrastructure as the physical plants and institutions that provide utilities like power, water and telephone service, and transportation networks. This discussion requires a more expansive definition that includes communications networks, financial institutions and insurers, food manufacturing and delivery… the list goes on and on. It quickly becomes clear 1) how many dependencies exist between them, 2) how tightly they are linked with one another, and 3) how few are government entities.

> “As the vast majority of critical infrastructure in this country is owned and operated by the private sector, it is vital that government and industry lock arms in confronting this risk.”
>
> – Peter Beshar

Prescriptive compliance regimes like NERC-CIP for electric utilities, HIPAA for medical services, and FFIEC for financial institutions are created with the intent of improving security controls, but they complicate matters and prioritize compliance over security. If the goal is to improve national resilience, this approach is counterproductive. A panelist representing the electricity infrastructure re-emphasized the importance of adopting universal standards:

> *“The [electric] industry also is applying the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Department of Energy’s Cybersecurity Capability Maturity Model (C2M2).”*
>
> *– Scott Aaronson (Executive Director, Edison Electric Institute, July panel)*

This speaks back to our core belief that a standards-based approach is essential to creating national resilience in the face of cyber threats. But this does not solve the whole problem. There is another concern about infrastructure providers who are the target of nation-state or terrorist attacks, and whose cyber capabilities could never hope to match those of their adversaries. Could they be held liable for damages from a terrorist attack? Panelist Ted Schlein offers his thoughts:

> *“First, class action lawsuits aimed at a private enterprise for not being able to defend themselves against a cyber attack by a foreign nation state, are unrealistic. Most of our federal networks cannot defend themselves against similar attacks yet the financial burden as well as the public shaming that goes along with such a case, calls out for tort reform in this area to create a safe harbor in certain situations.”*
>
> *– Ted Schlein (General Partner, Kleiner Perkins Caulfield & Byers, June panel)*

There is a mechanism for limiting this liability. We join Peter Beshar again in advocating for broader use of the SAFETY Act:

> *“We recommend that the Commission improve national cyber resilience by facilitating broader use of the SAFETY Act … The SAFETY Act requires DHS to set the limit of liability for each applicant based on the amount of insurance available and the burden to purchase coverage up to that limit. Here again, the insurance industry could potentially play a constructive role…”*
>
> *– Peter Beshar*

The SAFETY Act serves to create incentives for innovation around technologies and other solutions that protect the nation’s critical assets. By reducing potential liability for damages resulting from a cyber crime or a terrorist attack, the SAFETY Act makes it easier for sellers of protective measures to enter into contracts with their customers. Because potential liability is limited by the Federal Government, residual risk of liability can be easily transferred through insurance policies. By effectively underwriting the catastrophic or "black swan" risk, the Federal Government creates incentives for innovation and broad application of new technologies.

Organizational Management

Our discussions of Cyber Insurance and Federal Governance crossed paths several times, and that interweaving of concepts will continue in this section. We believe that stewardship at the Federal level should create constructs in which industry can apply their own competencies to solve problems with incentives and innovation. A standards-based approach combined with programs to limit the liability that derives from "unknowable" catastrophic risk creates an environment where insurers can apply their products to influence good behavior. Within that environment, constrained and structured around those incentives, we enter our final discussion about Organizational Management.

> *"Our views are premised on the firm belief that technology alone cannot protect us from cybersecurity threats."*
>
> *– Eli Sugarman (Program Officer, Hewlett Foundation, June panel)*

> *"It is not always about technology, and I would recommend that governments and companies alike must invest in human capital first, sound policy and procedure second and thirdly with appropriate technology being identified by the capable people that have been put in place to protect the systems."*
>
> *– Marty Edwards (Director, ICS-CERT, NCCIC, DHS, July panel)*

We are only beginning to enter a phase in which people recognize that cyber risk management extends beyond the realm of technology. For years, organizations and their managers have tended to place cyber neatly under the purview of the CIO, with no recognition that the problem is actually one of enterprise risk management. This attitude persists in a majority of companies, and endures through the power of inertia and a fundamental lack of awareness around what cyber risk means at each layer of an organization. In reality, cyber risk is an issue that lives in each level and function of an organization. Put another way, the lack of cyber risk awareness is a problem of organizational culture.

> *"We should recognize that cyber-security risk mitigation is not solely the responsibility of designated cyber-security professionals but is, perhaps more importantly, in the domain of leadership, risk managers and engineers at all levels of organizations."*
>
> *– Phil Venables (Managing Director, Goldman Sachs, May panel)*

Boiled down to its essence cyber risk is about protecting critical assets like sensitive data (personal, medical, financial) and physical controls (dams, power stations, etc.) When something goes wrong, the problem manifests through the technology. But the technology is only *where* the problem occurs – not *why.* Most often, the problem occurs because of some type of human error or the compounded effects of small errors across people, process, and technology. A simple example is an employee who is duped by a phishing email, clicks a link, and quietly initiates the installation of malicious software.

Can technology stop this from happening? Sometimes yes, but not always. Phishing attacks won't stop, but they can be mitigated through a combination of education, testing, benchmarking, incentives, policies, and enforcement that extends to all corners of the organization. These efforts should be prioritized by top managers, and led (with guidance from the CIO) by someone whose role includes training, testing, and compliance. Human resources professionals are key players in this effort. So are auditors, attorneys, and accountants.

Now consider that the cost of a breach has two major components (both tie directly into cyber insurance):

1) the direct cost of remediating damages to internal systems (first party), and
2) the cost of remediating and litigating claims from damaged parties (third party)

The vast majority of breach cost falls into category #2. It is possible to take action against these type of outcomes prior to a breach – it includes creating incident response and business continuity plans, educating employees about reporting and escalation protocols, and establishing clear guidelines to define roles and responsibilities in crisis management. In other words, it has very little to do with firewalls (technology), and everything to do with executive engagement and strategic planning (people). Mr. Venables' imagery of "muscle memory" carries the point home quite effectively:

> *"The first [recommendation] would be to integrate cyber security into the fabric of organizations:*
>
> *It's imperative to ensure that cyber-security risk management is embedded into the main risk management and strategic processes of organizations from the Board, to risk committees, to the wider processes of strategy formulation, product development, investments and acquisitions; both within the organization and across its extended supply chain …*
>
> *It's important to build the muscle memory of effective detection, containment/response, and recovery through continuous scenario planning, drills and exercises."*
>
> *– Phil Venables (Managing Director, Goldman Sachs, May panel)*

Capabilities built around response and recovery are literally the last line of defense – and only the first step in building an effective cyber risk culture. Ideally, our goals should include advanced preventive measures that limit the frequency with which we have to mobilize our response and recovery functions. Expert testimony from the panelists make the point concisely:

> *"Let me first clarify what I mean by prevention. Prevention is about significantly decreasing the likelihood, and increasing the cost required, for an attacker to perform a successful attack. We should assume, and be very diligent in ensuring, that the cost of a successful attack can be dramatically increased to the point where the likelihood of a successful attack declines. This is the outcome we should strive for—not to eliminate all risk, but to reduce and compartmentalize the risk to something acceptable and understood."*
>
> *– Mark McLaughlin (CEO, Palo Alto Networks, June panel)*

For boards, executives, and key stakeholders, this means actively moving toward a posture that prioritizes risk-based decision making around critical assets that are exposed to cyber threats. Leadership is nothing if it doesn't include risk and crisis management – so none of this will be unfamiliar territory – but it might require new stakeholders to help interpret the map. To that end, boards and executives are right to look at the CIO and the CISO, but they are wrong if they don't also look to heads of audit and compliance, risk, procurement, and human resources.

> *"We have a nascent effort to educate Boards of Directors, General Counsels, and other corporate leaders so that they support the work of their internal information risk management team."*
>
> *– Robert "Bob" Kolasky (Deputy Assistant Secretary for Infrastructure Protection, DHS, July panel)*

The mandate is cultural change and the mantle is passed to the board- and executive-level leaders. The guidance, unsurprisingly, is to use the NIST Framework for Improving Critical Infrastructure Cybersecurity. The challenge, then, is to provide the impetus and create the methods through which NIST can be quickly and broadly adopted.

> *The NIST framework's risk-based approach is consistent with the approach used to manage enterprise risk.*
>
> *– Scott Robichaux, Cyber Security Manager, Exxon Mobil*

Trends & Challenges

The emergence of cyber risk is part of the convergence of a number of long-term trends, each of which will continue to shift the landscape of security and privacy for decades to come. We should continue to focus on those long-term trends, difficult as it may be through the fog of near-term challenges. Here again, we invoke the wisdom of the panelists who spoke against the dangers of prescriptive policies and burdensome compliance regimes. An environment for safe collaboration using a common standard, typified by the NIST Framework, will go farthest in helping us adapt to both the present challenges and the shifting economic landscape in which we encounter them.

In the near term, the vast proliferation of technology solutions to address these trends exhibits all the signs of an early-stage marketplace. First of all, what we might call "situational awareness" is low. Most people aren't well informed about the nature of cyber risk, the methods used by hackers, and the specific ways that damage manifests itself. Operating within this under-educated environment we see a thriving diversity of "point solution" providers – technologies that claim to solve one tactical problem or another. In chorus, this massive volume of technologies and competitors makes for a raucous buying environment. Front-line leaders like the CISO are overwhelmed, and those who set budgets have little hope of quantifying an ROI on security spending.

This speaks to another piece of the landscape: the severe shortage of technical cybersecurity talent. According to Forbes (Jan 2016), 209,000 cybersecurity jobs will go unfilled in the US this year. Cisco puts the global figure at 1 million job openings, and Symantec expects a total shortage of 1.5 million by 2019.[1] This doesn't include the myriad functions within an organization (e.g., human resources, procurement) whose actors play a key role in cyber risk management. Altogether, we face huge constraints in our ability to build a properly equipped workforce who collectively know how to recognize and act against cyber risk.

> *"Yes, we need more skilled cybersecurity engineers, more secure programmers, more technicians, firewall people, investigators, . . . the list goes on, but this is the easy part. But what about the line of business manager and the project manager? The VP of development, of R&D, of Marketing? These people need to learn about the risks and values of security. Yet, for many of these positions and the people in them, they don't even know they need to know what they don't know – [Donald] Rumsfeld's 'unknown-unknown'."*
>
> *– Dr. Wm. Arthur "Art" Conklin (Director, Center for Information Security, University of Houston, July panel)*

We expect the cybersecurity market to mature along many of the same lines that most young markets do: buyers will become more sophisticated, fragmented competitors will consolidate, and the labor market will adjust to fill what is currently a severe talent shortage. But those evolutions will take place against a larger, less predictable backdrop of structural economic change and the blistering pace of technological advancement.

Moore's Law describes geometric growth in computing power and the concurrent collapse in price-per-unit of computation. Together, these combine to ensure large-scale availability of powerful computers. That availability has led to a proliferation of technology entrepreneurs whose continual innovations bring computational power to ever-broader audiences through products that make computing more accessible. This widespread availability and accessibility has provided fertile ground for the information economy, where so many businesses now pursue efficiencies and new opportunities through big data and analytics. Although there is value in beneficial use, there is value in malicious use as well, and these trends have converged to create massive opportunities for hackers. Thus, as computing becomes easier and cheaper for all, the opportunity space for bad actors grows just as quickly.

One manifest of this trend is the Internet of Things – where ever-smaller computers find their way into every conceivable facet of life. IoT is driven by the desire on the one hand for data collection (*what can sensors in a refrigerator tell us about grocery buying habits?*) and on the other for functionality and convenience (*what if we could automatically re-stock a missing item in a refrigerator, or even an empty refrigerator?*). The result is a world where devices of all types and kinds now observe, collect, and process data about our daily lives.

This trend exists in both the consumer and the industrial economies, and in both it represents an exponentiation of what is known as "attack surface" – the total exposure to bad actors. Until recently, our exposure has been limited to financial damages from the release of health or financial information. Organizations are also suffering damages from lost intellectual property. All of these are serious, but in the end, not life-threatening.

That changes with the expansion of the attack surface into our industrial facilities, critical infrastructure, and everyday lives. As devices become smaller, more powerful, and cheaper, they will become ubiquitous and touch our lives in new ways. The damage from an attack will no longer be limited to financial fallout – it will place people's lives at risk. This trend – away from economic risk and toward physical risk – will likely manifest itself before we are prepared, and will cause tumultuous changes in the security and risk business.

When this happens, it will accelerate citizen and consumer awareness of and engagement in cyber risk mitigation. Today, most citizens are largely complacent about cybersecurity. The burden and the liability tend to fall to the organizations that handle their data. That liability landscape is shifting, and we expect a time when companies will begin to hand some responsibility for data protection back to the consumer. The early sprouts of that trend can be seen in enforcement of password policies (misguided or otherwise) and nudges toward things like 2-factor authentication.

The real awakening will occur when a cyber attack results in physical harm or loss of life. Researchers have conducted multiple demonstrations of their ability to remotely hack the physical control systems of modern automobiles. These demonstrations have been conducted in controlled environments under optimal conditions and so they are difficult to replicate – but the implication is clear. As our dependence on connected devices grows unabated, our risk exposure will grow at least as much.

It is unclear what this means for our economy, our society, and our lives. But we believe that we have a vital tool to manage this massive shift: **a standards-based environment for risk quantification, so that diverse stakeholders can communicate in a common language and create economic incentives for effective risk management.**

Contact

Charles F. Leonard, VP Product Management, Cybernance Corporation – charles.leonard@cybernance.com

Reference

[1] http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#27658f0f7d27