SALARE SECURITY™

A White Paper Prepared By: Salare Security LLC
201 East Loop Rd., Ste. 229
Wheaton, IL 60189
http://www.salaresecurity.com
312.994.2336

In Collaboration With: Celenium Corporation
24656 Generation Dr.
Plainfield, IL 60585
http://www.celenium.com
630.865.6861

QIM Analytics, Inc.
417 Lauder Lane
Inverness, IL 60067
http://www.qimanalytics.com
847.530.0435

Information and Communication Infrastructure

Improving Cyber Security Posture

Executive Summary

Defense of the Nation's cyber infrastructure is the most challenging area of the National Infrastructure Protection Plan (NIPP). Cyber security supports many of the critical infrastructures and key resources (CI/KRs) covered by the NIPP such as: Defense Industrial Base, Energy, Public Health and Healthcare, Banking and Finance, Emergency Services, Nuclear Reactors-Material-Waste, Information Technology, Communications, and Transportation. However, despite the best efforts of both the public and private sectors, our cyber security defenses are routinely defeated by internal and external agents. Identifying and then addressing the impediments to the best practice of cyber security can reduce the risk of attack on a broad variety of CI/KRs and can greatly enhance the security of the Nation.

The most critical impediment to the best practice of cyber security is the immense amount of human effort that must be invested each and every day just to maintain current cyber security posture. As are result, because humans are involved, mistakes are made and because of the enormity of the task, little effort can be expended to further enhance cyber security posture. Reduction of the human effort to implement, monitor, maintain, and operate best practice cyber security controls is imperative to breaking the industry's current cycle of being "too busy to get better." Reducing this enormous human effort must be achieved through automation and improved tools to better leverage the time, the knowledge and the expertise of the Nation's cyber security professionals to better defend the Nation from cyber attacks. Industry has begun to address some opportunity for automation but, successful, near real-time automation of the analysis of event information to identify incidents and attack pre-cursors has yet to occur. The analysis of event information is a complex and difficult opportunity that must occur in near real-time to provide the labor savings desired. A scientific breakthrough is required to bring a viable solution to bear.

A solution is not likely to immerge in the market place without government intervention and investment. Solving the problem likely requires a combination of tools, techniques and expertise that are disbursed among a large number of private concerns that are not pre-disposed or well-positioned to cooperate. A viable solution will require drawing upon a multitude of academic disciplines and require the infusion of strong subject matter expertise to proceed towards a solution. The right combination of talent is not likely to come together on its own but only through governmental stimulation. Finally, near real-time analytics technology simply does not exist today to support the anticipated solution.

A government funded breakthrough in automation of near real-time analysis and interpretation of event information will: 1) enable an immediate increase in the security posture of the Nation; 2) attenuate the severe, unmet demand for additional cyber security professionals; and 3) allow cyber security professionals to invest significant time in forward looking work to further reduce risk and enhance security of the Nation's NIPP sectors. This investment would correct a short-term market inhibitor and allow industry to sustain future innovation on its own.

The Area of Critical National Need

The National Infrastructure Protection Plan (NIPP)[1] clearly defines the Information Technology and Communication infrastructures as critical infrastructures and as key resources (CI/KR) to defend. But, the challenge of cyber security is much broader than just these two sectors. The scope of cyber security spans many of the other NIPP defined sectors such as Defense Industrial Base, Energy, Public Health and Healthcare, Banking and Finance, Emergency Services, Nuclear Reactors-Material-Waste, and Transportation because of their necessary reliance on information technology to support efficient operation of those sectors. Strong cyber security defenses are necessary to defend very broad and very substantial portions of the Nation's CI/KR.

Dr. Massoud Amin, Professor of Electrical and Computer Engineering and Director of Graduate Studies for the Security Technologies Program at the University of Minnesota explains the potential consequences of a successful cyber attack[2], "If one part of the nation's infrastructure goes unprotected, that vulnerability quickly cascades into the other networks, putting every individual at risk." He also goes on to say, "The number of cyber attacks has increased, the speed has increased and the severity of the successful ones has increased."

The burden of underperforming cyber security is significant. Not only does it weaken the Nation's defense posture, it also significantly impacts the Nation's economy. The Ponemon Institute estimates that in 2009 more than $30 billion in losses were incurred by the US economy due to data record breaches[3]. McAfee in a 2009 report placed the theft of intellectual property at the level of $1 trillion.[4]

[1] *National Infrastructure Protection Plan*, 2009, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
[2] *Threat of multi-agent attacks on United States increasing, experts warn, October 6, 2009, mndaily.com,* Tara Bannow
[3] *Fourth Annual US Cost of Data Breach Study*, the Ponemon Institute, January 2009
[4] *Unsecured Economies: Protecting Vital Information*, McAfee, January 2009

The Societal Challenge

Cyber security is simply too labor intensive. Indirect evidence of this fact is evident in that salaries for cyber security professionals are growing at a faster rate than those of IT professionals and that the number of advertized job openings for cyber security professionals in both the private and public sector continue to grow[5]. Additionally, the introduction of new cyber security technology is astonishingly slow. Even though risks exist that can be economically lowered through use of newer technologies, the new technologies are not being deployed. This clearly indicates a shortage of time to analyze, plan, and implement new, valuable security products. So, given our current cyber security resources the Nation simply can not achieve the levels of risk reduction that are possible if these significant human constraints were not in place.

In testimony presented to the US Congress on November 17, 2009, Richard Schaeffer, the NSA's information assurance director has claimed, "If network administrators simply instituted proper configuration policies and conducted good network monitoring, about 80 percent of commonly known cyber attacks could be prevented." He went on to add that "adhering to already known best practices would sufficiently raise the security bar so that attackers would have to take more risks to breach a network, 'thereby raising [their] risk of detection." Yet, even armed with access to these tools our Nation is still constantly successfully attacked. The lack of resulting protection is due in large part to the complex and very human intensive efforts required to stand up and maintain the known best practices and procedures. There just are not enough people to bring us to a position where we are doing the best with what we now know. Reducing the human effort behind good cyber security is absolutely essential in reducing the incidence of successful attacks.

The problem continues to grow in magnitude, because the level of risk continues to grow. Despite the fact that cyber vulnerabilities are showing signs of leveling off[6] (see Figure 2) other risks present themselves via other avenues that dwarf this single improvement. There is an ever-increasing onslaught of cyber attacks that are launched against our Nation around the clock. Looking at cyber attacks just against the Department of Defense (DoD), the attacks have grown from 43,880 in 2007 to 54,640 in 2008 and 43,785 attacks occurred in just the first six months of 2009[7] (see Figure 1). The rate of attacks is growing increasingly and alarmingly.

[5] *IT Salaries on the Rise: Study,* The InternetNews.com, Sean Michael Kerner, March 5, 2010.
[6] *The IBM Security Solutions X-Force 2009 Trend and Risk Report*, February 2010.
[7] *REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION to the ONE HUNDRED ELEVENTH CONGRESS, FIRST SESSION,* NOVEMBER 2009, http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf

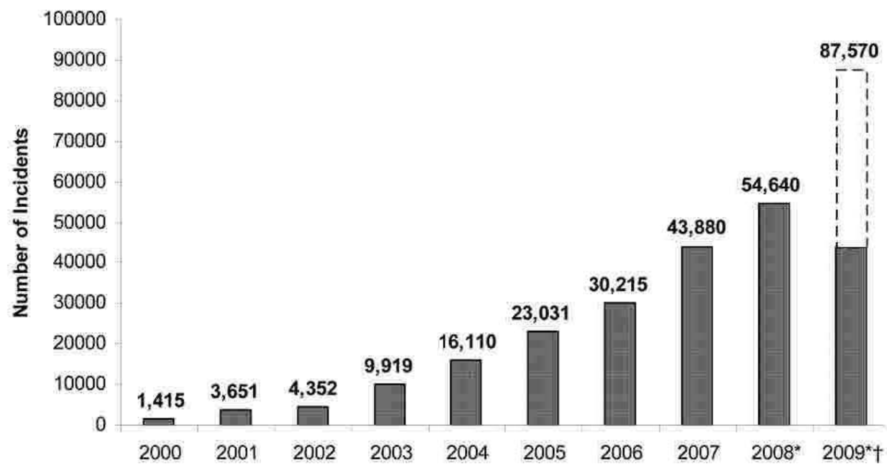

Figure 1 – Trends in Cyber Attacks Against the Department of Defense

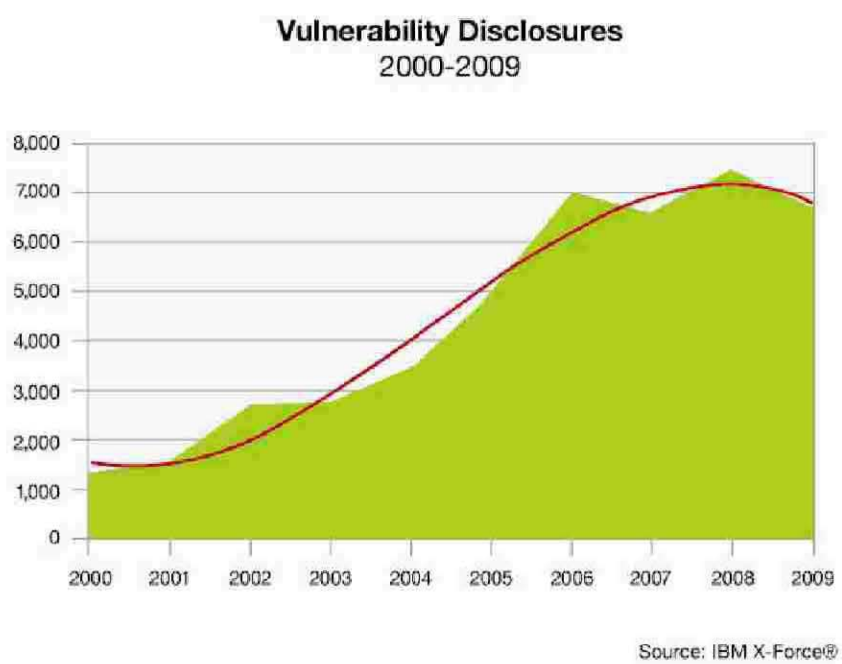

Figure 2 – Trends in Annual Vulnerability Disclosures

Attacks continue to rapidly grow even in the face of a leveling of the rate of new vulnerabilities because the vulnerabilities are changing in their complexion. More of the vulnerabilities can be remotely exploited exposing our Nation to many more threat sources and thus increasing the attack rates (see Figure 3). And, vulnerabilities of web applications are growing rapidly just as our Nation moves toward heavier use of web-based applications and cloud computing (see Figure 4).

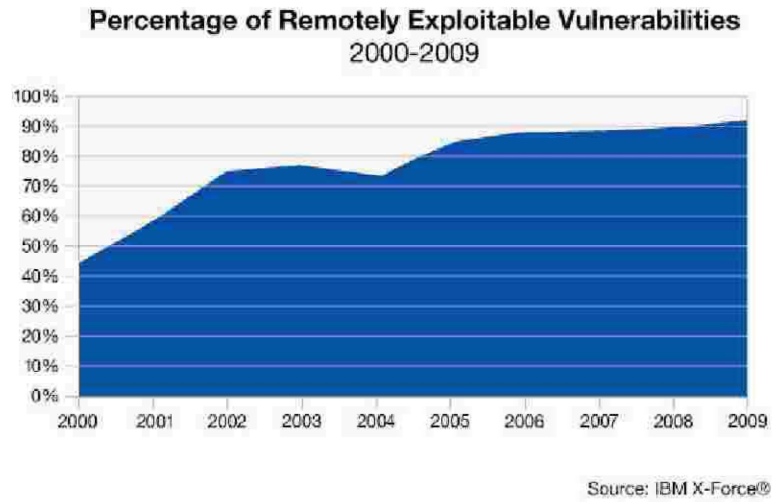

Figure 3 – Trends in Remotely Exploitable Vulnerabilities.

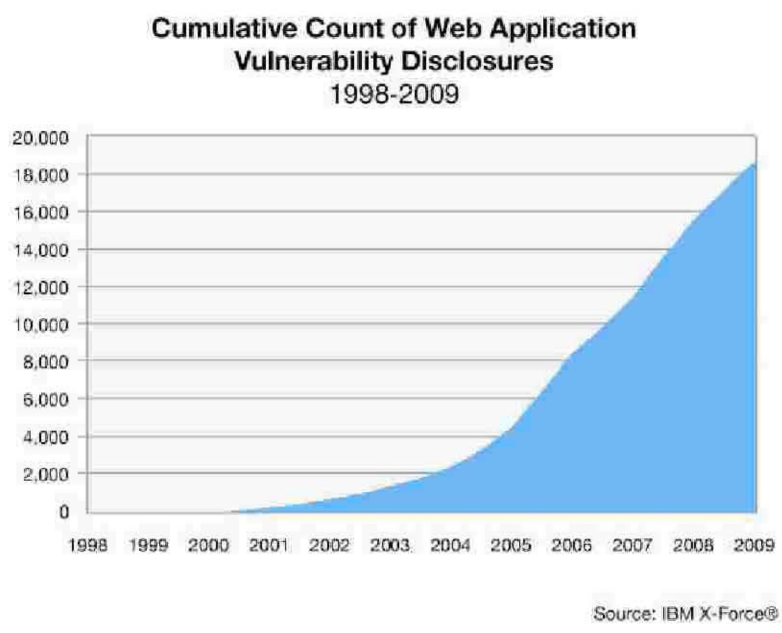

Figure 4 – Trends in Web Application Vulnerability Disclosures

Government support is required to advance the state-of-the-art in cyber security automation because of a number of forces at work in the market place that are producing an inefficient market. First, a solution to the problem likely requires a combination of tools, techniques and expertise that are disbursed among a large number of private concerns that are not pre-disposed nor well-positioned to cooperate. Second, a viable solution will require drawing upon a multitude of academic disciplines and require the infusion of strong subject matter expertise to proceed towards a solution. The right combination of talent is not likely to come together on its own but only through governmental stimulation. Third, near real-time (that will ultimately become real-time) analytics technology simply does not exist today to support a solution. While business intelligence applications have proven valuable in identifying similar (but unrelated) information from static information stored in data warehouses, there are significant challenges in grooming data, loading it, and analyzing it in real time because of the sheer volume of information that must be processed and presented in actionable form. Scientific advances are required to minimize the computational requirements of the loading and transformation of data to deliver a viable system.

It anticipated that the three authors of this white paper, Salare Security LLC, QIM Analytics, Inc., and Celenium Corporation and other potential collaborators such as the Illinois Institute of Technology's Departments of Electrical and Computer Engineering, Applied Mathematics, and Information Technology Management; Carnegie Mellon University; and the Internet Security Alliance and its members would be interested in submitting a joint proposal.

The Transformational Results

The security industry must progress along a roadmap of sustained innovation to provide ever-increasing and effective cyber security protection. These major roadmap stages are: Ad hoc, Proactive, Managed and Optimized as depicted in Figure 5. Presently, the industry is locked-in the Ad Hoc stage despite the best efforts of the leading cyber security companies in the world. There is a strong recognition and desire to move the cyber security industry along this path, such as Cisco's "Self Defending Network" strategy that mapped out similar objectives more than six years ago. However, there has been disappointing progress along this path. The cyber security industry is fixated on older technologies and antiquated thinking that has stifled breakthrough innovation in this area. Small, dynamic entrepreneurial companies are best equipped to put forward truly transformative approaches and technology because they are free to break away from existing technology and methodology. However, because of the stated intentions of the large, established cyber security vendors, investment to bring that innovation to market is simply too high of risk for venture investors despite the poor record of significant innovation by those vendors.

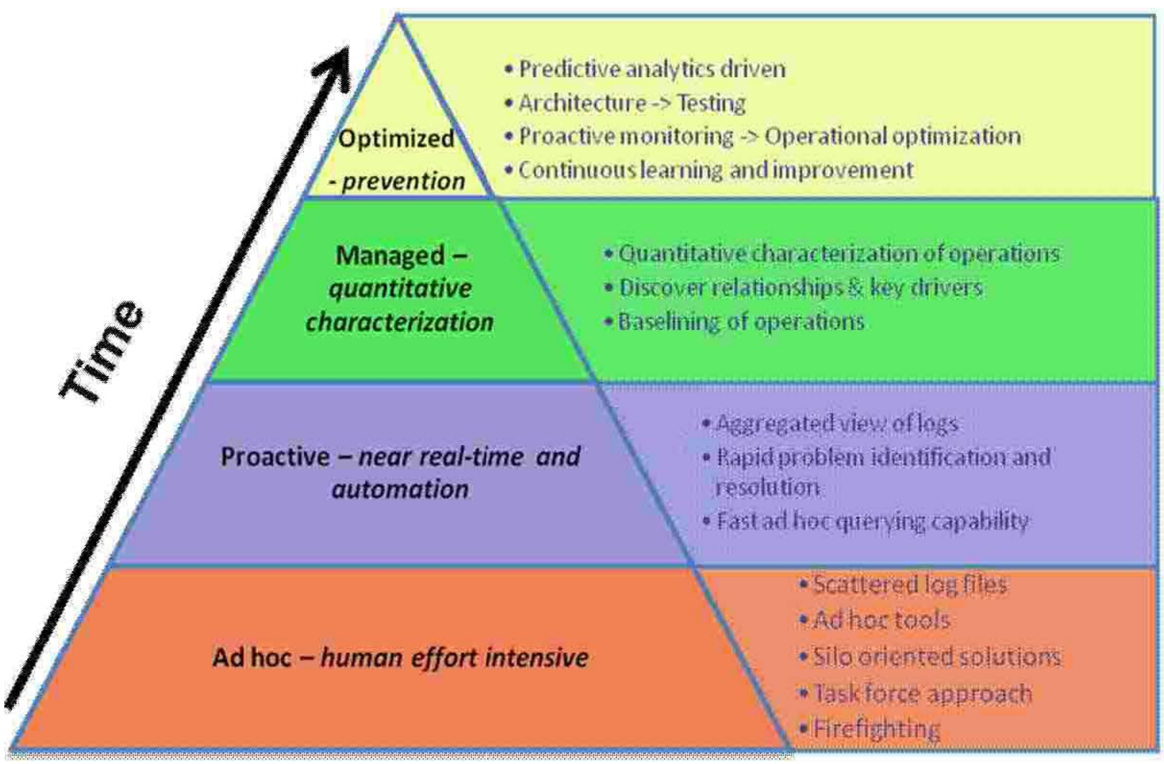

Figure 5 – Security Automation Transformation Roadmap.

Once government investment is made to move the industry from the Ad hoc to Proactive stage of the roadmap, the industry will be able to self-sustain further evolution along this roadmap of security automation transformation. The technological advances and the resulting economic opportunity will stimulate further private sector investment to address what has been viewed as an attractive market but a market without viable technology and methodology to extract value.

The results of successfully moving the cyber security industry from Ad hoc to Proactive will result in significant short and long term gains. In the short-term, improved automation will enable better execution on existing cyber security controls and an enhanced security posture for the Nation. Longer term, there will be reduced pressure for adding additional cyber security staff. The existing cyber security subject matter experts will be able to devote time to mentoring, teaching and training the evolving workforce. They will also be able to devote time to addressing the ever increasing number of cyber risks that the Nation faces. At last, the cyber industry will be able to better understand, plan and prepare to provide better and better cyber risk management. In short the "too busy to get better" cycle will be broken. Once this cycle is broken, the need for future government support will be eliminated and industry will be able to sustain future innovation on its own.

