National Cybersecurity Institute Journal

Volume 1, No. 3

ISSN 2375-592X

National Cybersecurity Institute | 2000 M Street, Suite 500 | Washington, D.C. 20036
Excelsior College | 7 Columbia Circle | Albany, NY 12203-5159

National Cybersecurity Institute Journal

Volume 1, No. 3

NATIONAL CYBERSECURITY INSTITUTE JOURNAL

The National Cybersecurity Institute at Excelsior College is a research center based in Washington, DC, dedicated to increasing knowledge of the cybersecurity discipline and its workforce demands. Published three times a year, the peer-reviewed *National Cybersecurity Institute Journal* covers topics that appeal to a broad readership within the cybersecurity discipline, with a particular focus on education, training, and workforce development. The manuscripts submitted to the journal are reviewed for their contribution to the advancement of applied research in the area of cybersecurity.

Submission guidelines for authors can be found at www.nationalcybersecurityinstitute.org/journal/.

FROM THE EDITOR

Welcome to the third issue of the National Cybersecurity Institute Journal (NCIJ). As the growing cybersecurity community is well aware, the mission of National Cybersecurity Institute is to broaden awareness and knowledge of the cybersecurity discipline and assist the government, industry, military, and academic sectors to better understand and meet the challenges in cybersecurity policy, technology, and education. In previous issues of this journal we provided timely and informative articles that were well-received by the cyber community. The NCIJ will continue to publish three times a year relevant and noteworthy articles that serve to enlighten those with a vested interest in the cybersecurity field.

In this issue, you will find articles from notable authors with a variety of perspectives in the field. Jane LeClair and Randy Sylvertooth review the Cyber Warfare Symposium held at the National Cybersecurity Institute, which examined a topic highly visible in recent headlines. This synopsis is followed by Kevin Newmeyer's article on the elements of national cybersecurity strategy for developing nations. The cyber systems in developing nations are at great risk, and this piece takes a close look at some critical elements that should be considered when developing strategies for those countries. A.H. Kabir presents an interesting article on data-centric security that is sure to intrigue many of our readers. Gerald Beuchelt, Cory Casanave, and Vijay Mehra provide an article that examines the advances in threat and risk modeling and provides some interesting insights. Roland Taylor provides us with a thought-provoking piece on the need for a paradigm shift in cybersecurity in the field of journalism. And finally, Sean Murphy offers his thoughts on the importance of cybersecurity in the health care field.

Each of these articles provides our readers with knowledgeable insight and, I hope, instills a desire for further thought and research on the topics discussed.

As always, a publication such as this is never the work of one individual, but rather the result of collaboration by dedicated people at NCI who work tirelessly to produce a quality product. Many thanks go to all the contributors, administration, and staff for their great efforts to continue the tradition of bringing the National Cybersecurity Institute Journal to our readers. I hope you in the cyber community find this journal informative as you work within your respective cyber areas. I look forward to your comments, suggestions, and future submissions to our journal.

Dr. Jane A. LeClair

Editor in Chief

NCI Symposium on the Nature of Cyber Warfare

Jane LeClair, EdD | Randall Sylvertooth

ABSTRACT

The escalating threat of cyber warfare between nation states continues to be an important topic of conversation in the cyber community. Recently, a symposium was held at the National Cybersecurity Institute in Washington, DC, to discuss the issues involved with this serious concern. Notable guest speakers from both business and government spoke to the audience gathered for the event. The highlights are presented in this piece.

INTRODUCTION

Cyber war takes place largely in secret, unknown to the general public on both sides.

Noah Feldman (Feldman)

The National Cybersecurity Institute (NCI) hosted its premier symposium on September 16, 2014, at its headquarters in Washington, DC, with participants representing the government, industrial leaders, military personnel, and the private sector. The first in a planned series dealing with major cybersecurity matters, the symposium was titled "The Nature of Cyber Warfare" and a number of issues related to the developing crisis in cyber space were discussed. The National Cybersecurity Institute symposium featured leading cyber policy and doctrine experts in the cyber domain.

SYMPOSIUM HIGHLIGHTS

Jane LeClair, chief operating officer of the National Cybersecurity Institute, hosted the symposium and presented the expert panel of speakers. The distinguished panel consisted of: Ernest McDuffie, director at the National Institute of Standards and Technology (NIST) and head of the NIST National Institute of Cybersecurity Education program (NICE); Matthew Flynn, associate professor of military history at the Marine Corps University; Mark Haggerott, deputy director of the Center for Cyber Studies and distinguished professor at the U.S. Naval Academy; Admiral William Leigher (USN-Ret.), current director of Advanced Solutions — Intelligence, Information Services at the Raytheon Company; and Sean McGurk, vice president for business development and critical infrastructure protection at Centripetal Networks Inc.

Following introductions, McDuffie used the newly revised and developed NISxT cybersecurity framework to establish the cyber warfare panel discussion. He referenced several significant events that have taken place leading to where we are today in the realms of cyber warfare and cybersecurity, including NASA's cyber attack by an unknown actor, Russia's cyber attack on Estonia, the U.S. Post Office cyber attack, the ongoing cyber attacks on Defense Industrial Base government contractors such as Lockheed Martin, the cyber attack on Twitter, the 2010 STUXNET deployed cyber weapon, cyber attacks against the Canadian government, and the cyber espionage operation named Red October. McDuffie concluded his remarks by briefly summarizing the cyber attacks against

the South Korean financial sector as well as many other recent cybersecurity breaches, including Home Depot, Target, and J.P. Morgan.

McDuffie reiterated that all of these events have led us to deploy and spend more resources to combat a persistent cybersecurity threat. More of our military resources are being spent on this newly established domain in cyberspace (McDuffie, 2014). He stated that the North Atlantic Treaty Organizations (NATO) has spent roughly $58 million euros for upgrades of its newly developed cyber force and its equipment. McDuffie stated that this cyber threat is real; the enemy could be secreted anywhere and can attack at any time. He noted that anyone who has access to a computer system could launch a cyber attack and that it is the ultimate base of asymmetric warfare (McDuffie, 2014). The basis of asymmetric warfare involves opposing groups who have differing and unequal resources for engaging in battle. Cyberterrorists do not have the resources equal to the United States, but utilize unconventional methods to exploit vulnerabilities and weaknesses that exist in our cyber infrastructure.

Flynn, associate professor of military history at the Marine Corps University, suggested that there are categories in the new cyber warfare domain which are both evolutionary and revolutionary and speculated that perhaps this is a new state of being for the United States (Flynn, 2014). Flynn shared a strong ideological belief that in order to battle this new future in the cyberspace domain, people and personnel should form relationships, talk in forums, and share related cyber threat intelligence with the goal of becoming more effective and vigilant against these threats.

Haggerott, deputy director of the Center for Cyber Studies and distinguished professor at the U.S. Naval Academy, expressed concerns regarding the science of artificial intelligence and the rise of the machines, as depicted in the film "The Terminator." Artificial intelligence attempts to enable a machine to mimic human decision making and learning via clever software. He discussed the evolution from kinetic warfare to cyberwarfare based on machine evolution, and noted how mankind transitioned from manned air power platforms in the 1930s to the recently deployed unmanned platforms such as in weaponized drones. Haggerott stated that, much like the technological advances of manned to unmanned platforms, cyber warfare has become significant in the U.S. war planning efforts (Haggerrott, 2014).

Leigher, current director of Advanced Solutions — Intelligence, Information Services at the Raytheon Company, continued the cyber conversation by describing how the evolution of cyber is rapidly developing and how we are in many ways living in a time of exponential change. He primarily focused on the Defense Industrial Base (DIB), corporate America, and how cyber warfare is seen as a threat to economic-based industries. He advanced his belief that military cyberspace and the attacks on industry are intertwined (Leigher, 2014). Leigher felt that the U.S. must come to understand and develop new alliances because of the asymmetric base of cyberwarfare. It is his firm belief that the U.S. Navy and its contracting industrial base will now have to evolve and acquire new targets and new systems to better thrive and dominate in the new cyberspace domain if America is to remain a global superpower (Leigher, 2014).

The symposium concluded with remarks by McGurk, vice president for business development and critical infrastructure protection at Centripetal Networks Inc., who focused on the kinetic aspects of cyber warfare and the implications for the protection of America's critical infrastructure. McGurk discussed the development and evolution of the STUXNET weaponized malware that wreaked havoc on Iran's newly created nuclear site and explained how STUXNET was a soft weapon that gathered cyber intelligence first on the program logic controllers (PLCs) and the SCADA system architecture before becoming weaponized and kinetically damaging Iranian centrifuges (McGurk, 2014). He is concerned with the potential for such weapons to be unleashed on our infrastructures. McGurk also felt that too many industry professionals are

focused on physical perimeter security and not the cyber domain security. He stated, "We have to better protect that domain by using layered defense in depth and deploying the best technology in order to survive and protect our interests with the use of dedicated computer systems" (McGurk, 2014).

SUMMARY

Following the panel remarks and presentations, there was a lively question and answer period during which the various details about cyber warfare and its numerous components were discussed. There was a general consensus among the panelists and members of the audience that greater attention needs to be paid to the evolution of cyber-related technology, and how the U.S. needs to better prepare our defenses in order to prevent a cyber "Pearl Harbor."

This premier symposium will be followed in the months ahead by an ongoing series of events which will highlight various aspects of cybersecurity and the relationship to our nation's well-being, the security of our businesses, and our critical infrastructure.

REFERENCES CITED

Feldman, N. Brainy Quote. Retrieved from http://www.brainyquote.com/quotes/quotes/n/noahfeldma630545.html

Flynn, M. (2014, September 16). NCI Symposium on the Nature of Cyber Warfare. Washington, DC

McDuffie, E. (2014, September 16). NCI Symposium on the Nature of Cyber Warfare. Washington, DC

McGurk, S. (2014, September 16). NCI Symposium on the Nature of Cyber Warfare. Washington, DC

Leigher, W. (2014, September 16). NCI Symposium on the Nature of Cyber Warfare. Washington, DC

AUTHORS

Jane A. LeClair (jleclair@excelsior.edu) is the chief operating officer at the National Cybersecurity Institute (NCI) at Excelsior College in Washington, DC, whose mission is to serve as an academic and research center dedicated to increasing knowledge of the cybersecurity discipline. LeClair served as dean of Excelsior's School of Business & Technology prior to assuming her current position. Before joining Excelsior College, LeClair held positions in education and in the nuclear industry, bringing her teaching energies to other colleges while having a full-time career in the nuclear industry. Her work in the industry brought her to the attention of the International Atomic Energy Agency (IAEA) with whom she continues to collaborate. LeClair has also been actively involved in a variety of professional organizations. She is well known for being a vocal advocate for attracting and retaining more women in technology fields. Her areas of interest include social engineering, women in cybersecurity, and cybersecurity training.

Randall Sylvertooth (rsylver@gmail.com) is a career industry cybersecurity subject matter expert (SME), and works as a contractor for the U.S. government in various management and leadership capacities. Sylvertooth serves academia in many ways; he contributes as an adjunct professor and advisor for the University of Virginia's School of Continuing and Professional Studies (SCPS), Cyber Security Management Program and as an assistant professor teaching at The University of Maryland University College (UMUC) Cybersecurity Program. Sylvertooth holds two master's degrees, one in The Management of Information Technology from the University of Virginia's McIntire School of Commerce and the second master's degree in Information Security and Insurance (Cybersecurity) from George Mason University's Volgenau School of Engineering. Sylvertooth is currently working on his Doctorate of Science at Capitol Technology University (formerly Capitol College). He serves as a National Cybersecurity Institute Fellow.

Elements of National Cybersecurity Strategy for Developing Nations

Kevin P. Newmeyer, PhD

ABSTRACT

Over the past several years, many nations have published national cybersecurity strategies in an effort to achieve or improve their nation's position relative to threats emanating from cyberspace. Research centers, international organizations, and even private companies have published recommendations on elements to include in these cyber strategies. The current recommendations are a significant improvement over the original guidance of the early- to mid-2000s, which argued for one of two courses of action: either establishing a Computer Security Incident Response Team (CSIRT) or establishing a legal structure to combat cybercrime. Earlier research revealed these two approaches to be inadequate, particularly for emerging countries with limited technical and administrative capability. This paper reviews the newer, more comprehensive recommendations and recently published strategies from emerging countries to identify 15 critical elements for nations to include when developing a comprehensive national cybersecurity strategy. The elements cover the key public policy issues of legal frameworks, public education programs, and political coordination along with the practical, technical recommendations on the establishment of public-private forums and CSIRTS. The paper recommends a practical checklist of policy issues to include in developing national cybersecurity strategies.

INTRODUCTION

The constantly evolving Internet and the increasing extension of connected information systems into nearly all aspects of commerce and governance poses significant challenges to governments, private sector organizations, and individuals around the world. Newspapers and television news announce the latest cyber breeches of major corporations on nearly a daily basis in the developed economies of the United States, Europe, and Asia. The challenges are even greater in the developing world where fewer cybersecurity professionals and technical resources can be brought to bear (Ellefsen & von Solms, 2010; Sund, 2007; Tagert, 2010). This new cyber domain has yet to develop the full range of internationally accepted rules and norms to ensure its safe use as a global commons like its counterparts of land, sea, and air. Today, information and communication systems are involved in nearly all aspects of daily life (Wegener, 2007). Seizing the opportunity for illicit gains, cyber crime emerged to adapt old scams for the digital age and to create new crimes that leverage human gullibility, technical flaws in software, or vulnerable hardware. The Internet security firm Norton estimated cybercrime's direct and indirect costs exceeded $338 billion in 2010 (Whittaker, 2011) with McAfee (2014) placing the losses in Germany at up to 1.6% of gross domestic product (GDP). United States government officials have expressed a fear of a potential "cyber Pearl Harbor" (Bumiller & Shanker, 2012). In the face of these growing challenges, policymakers failed to keep pace with both the technology and the threat. This policy-governance gap is particularly acute in many developing nations which have yet to recognize the risk (Lock-Teng Low, Fook Ong, & Aun Law, 2011).

Cybersecurity is now a national security issue that can impact the lives of individual citizens every day (Klimberg, 2012).

This paper provides recommendations for policymakers to consider as they draft national cybersecurity strategies to respond to this growing threat. The paper also explores the competing paradigms for viewing the problem of cybersecurity, the recommendations of various international advisory organizations, and some of the strategies already implemented to identify best practices in national cybersecurity strategy.

PARADIGMS FOR CYBERSECURITY

There are competing paradigms for viewing the cybersecurity problem. The three most commonly encountered have origins in national security theory, economic theory, or public health theory (Mulligan & Schneider, 2012). The paradigm determines the conceptual framework of the strategy, the approach to relations between the public and private sector, and the means to monitor implementation.

The national security paradigm reflects the traditional role of the state in securing the country's borders and enforcing the rule of law. Harknett and Stever (2009) outlined the unique nature of the cybersecurity problem as one that encounters the interface of the public-private and economic-defense in a previously unseen manner. Cybersecurity is considered fundamental to the military and economic security of the nation and requires an approach rooted in traditional national security arguments on protection of the homeland (Harknett & Stever, 2009; the White House, 2009). Agresti (2010) attributed the emphasis placed on national security in cybersecurity strategy and doctrine to the need to protect critical infrastructure and the importance of those public and private systems to the operation of government.

Kramer (2011), in an argument for an integrated government strategy on cybersecurity, emphasized that the national security risks to military systems, critical infrastructure vital to defense, and espionage targeted at defense plans and technology should be the primary responsibility and focus of the government's cybersecurity strategy. Agresti (2010) and Vacca (2011) argued that the lack of structure in cyberspace allowed for the easy importation of military cultural legacies into the policy debate on cybersecurity.

National security-focused cybersecurity strategies most often approach the problem from the top down and may lack the necessary buy in of civil society and the private sector necessary for successful implementation in a complex economy (Barnard-Wills & Ashenden, 2012; Klimberg, 2012). If security is overemphasized, the policy debate tends to shift behind closed doors (Barnard-Wills & Ashenden, 2012; Mulligan & Schneider, 2011). Excessive securitization gives rise to the potential for over-regulation of cyberspace (Betz & Stevens, 2011), which could hamper economic growth and the freedom of information flow. Overall, the national security focus tends to increase military influence on cyberspace policy (Dunn Cavelty, 2013). The potential danger in this approach is that other sectors may be excluded from the policy formation process and therefore diminish the acceptance and applicability of the final product.

The economic paradigm reflects the growing importance of the Internet and information flow to the economic well-being of the nation. Moore (2010) proposed an economic theory approach to cybersecurity highlighting the current misalignment of incentives, asymmetries, and externalities of the traditional security-based approaches. If the costs of insecurity are borne by others in the network, there is limited incentive to increase security. Moore (2010) recommended two policy changes applicable to a national cybersecurity strategy: (a) make the Internet service providers (ISPs) responsible and accountable for eliminating malware-infected computers on their systems; and (b) require companies and others to disclose data breeches and control system intrusions. Rishikof and Lunda (2011) sought to globalize this concept and argued that global standards are needed in a connected economy where malware can spread unchecked across ungoverned network interconnections.

As a more recent development, other authors advanced a public health model approach to cybersecurity (Charney, 2012; Mulligan & Schneider, 2012; Rosenzweig, 2011). This paradigm views cybersecurity as a public good and that improvement in any area benefits all participants in the network. Conceptually analogous to public health where immunizations and quarantines serve to protect the population from contagious disease, Charney (2012), Mulligan and Schneider (2012), and Rosenzweig (2011) argued for the public health model as a means of shifting from purely defensive measures to detect and stop malware attacks to an alternative approach that seeks to improve the security of each system connected to the global network. By securing the devices connected to the network and requiring "vaccinations" of antivirus software and system patches, the overall hygiene of the network is improved and everyone is more secure. When systems become infected, they must be isolated and cleaned not unlike the medical equivalent of quarantine and treatment. In this approach, a burden is placed on the individual and the service providers to take measures to protect the system as a whole.

The public health model also addresses information sharing on threats to the system (Charney, 2012; Mulligan & Schneider, 2012; Rosenzweig, 2011). This can present challenges on several levels similar to the information sharing externalities in the economic approach (Rosenzweig, 2012). The barriers for government-to-private industry sharing often occur when the security classification of the information becomes involved or questions of fairness are raised if not all firms get the information. Similarly, private industry sharing of information with the government may become problematic when protection of proprietary information, customer privacy, and corporate liability concerns are considered (Rosenzweig, 2012; Ruth & Stone, 2012). Private-private sharing of information faces similar legal restrictions as well as competitive pressures.

RESPONSES TO THREAT

To respond to the cyber threat, several industrialized nations — and a few still developing nations — published national cybersecurity strategies in recent years (European Network and Information Security Agency [ENISA], 2012; Luiijf, Besseling, & de Graff, 2013). Industrialized nations such as the United States, the United Kingdom, Australia, New Zealand, and several European Union member states published national cybersecurity strategies to establish government priorities and policies as a response to potential threats to national and individual security (ENISA, 2012). These strategies respond to unique national interests involving a globalized cyber environment. Luiijf et al. (2013) highlighted the variety of approaches and motivations of nations developing national cybersecurity strategies. Some strategies stressed national security concerns while others focused on predominately economic interests.

The goal of a national cybersecurity strategy is the alignment of the whole of government efforts to achieve or improve cybersecurity. Effective strategies establish the parameters for public and private sector cooperation and coordination in cybersecurity, and provide clear indication of the nation's intent to other nations and interested parties (Luiijf et al., 2013). The original Organization of American States (OAS) (2004) call for member states to develop national cybersecurity strategies was multi-sectorial with specific actions for the legal, security, and telecommunication sectors in the Secretariat and the member states. The European Union (EU) cybersecurity strategy also called for a multi-sector, coordinated approach (European Commission, 2013). Similar to the OAS strategy, the EU called for improvement of legal frameworks for responding to cybercrime issues and the establishment of national cyber incident response centers (European Commission, 2013; Organization of American States, 2004). The EU strategy went further than the OAS and added recommendations for mandatory disclosure of cyber incidents by private sector actors, military cyber defense coordination with NATO, and greater coordination in

external relations (European Commission, 2013). Both documents take a liberal democratic approach to the importance of free speech and human rights in cyberspace.

Wamala's (2011) International Telecommunications Union (ITU) *National Cybersecurity Strategy Guide* provided guidance to developing states on what a national cybersecurity strategy should contain. Wamala (2011) listed fourteen key elements for a national cybersecurity security. Several of the recommendations parallel the suggestions made in the European Union and OAS strategies—specifically the need to adopt new legal measures, the establishment of national-level cyber incident response teams, coordination with the private sector, and the necessity of international cooperation (Wamala, 2011). Using the common strategy construct of ends-ways-means, the strategy included recommendations for establishing high-level government accountability for cybersecurity, establishing a national cybersecurity coordinator, and the development of training programs for the general public and the cybersecurity workforce (Wamala, 2011).

Wamala's (2011) publication provided a significant advance over the earlier ITU Cybersecurity Guide for Developing Nations by Ghernaouti-Hélie. The 2009 document served as a background paper for individuals with little or no knowledge of cybersecurity issues. However, the guide reflects Ghernaouti-Hélie's preference for legal frameworks and is not a true strategy guide.

The ENISA guide provided a European approach along the lines of Wamala's ITU guide (Falessi, Gavrila, Kjenstrup, & Moulinos, 2012). ENISA sought to compile the best practices of European and non-European nations and targeted policymakers rather than technicians. Falessi et al. (2012) called for an eighteen-step process that included the common themes of establishing clear governance and leadership structures, international cooperation, stakeholder engagement, cybersecurity education, and incident response capability. Falessi et al. (2012) also called for organized cybersecurity exercises and the need to establish a balance between security and privacy.

In assessing nineteen individual national cybersecurity strategies, Luiijf et al. (2013) found three general goals for national cybersecurity strategy: (a) align the whole of government, (b) provide focus for public and private planning with established roles and responsibilities for all stakeholders, and (c) signal a nation's intent to external parties. This study was particularly useful in that it offers the first side-by-side comparison of strategies among nation states of different sizes and levels of development. The study additionally pointed out that there is no consensus regarding the definition of cybersecurity across nations, and the ten states that explicitly defined cybersecurity in their strategy documents varied significantly in their explanations (Luiijf et al., 2013). While the majority of the strategies considered robust cybersecurity essential to the economic strength of the nation, there was no consensus as to which agency should lead the response to a major cyber incident (Luiijf et al., 2013). Reflecting the strategic goals outlined in the European Union strategy and the ITU 2009 guide, there is significant interest across nations in the protection of critical infrastructure both as a security and economic concern (ENISA, 2012; European Commission, 2013; Ghernaouti-Hélie, 2009; Luiijf et al., 2013; Obama, 2013; Thomas, 2009). Luiijf et al. (2013) provided a recommended structure for a national cybersecurity strategy consisting of ten elements. Luiijf et al. (2013) paralleled the other organizational suggestions regarding establishment of legal frameworks, designation of responsible parties, and lines of action.

The strategy guidance provided by Wamala (2011), Luiijf et al. (2013), and Falessi et al. (2012) addressed several of the deficiencies in applicability for developing nations in earlier international cybersecurity strategy guidance noted by Tagert (2010). Tagert (2010) found the earlier international guidance provided by the ITU and others focused too heavily on the establishment of complex legal structures or the development of computer security incident response teams (CSIRT) as the means to achieve cybersecurity. Neither option reflected the realities of the technical and law enforcement capabilities of the African nations he studied. The more

recent strategy guides have begun to break down the abstract guidance of 2000 – 2009 into more practical and policy-oriented steps which may be applied more easily in emerging nations.

SELECTED NATIONAL CYBERSECURITY STRATEGIES

A number of individual nations have published national cybersecurity strategies (Falessi et al., 2012; Luiijf et al. 2013). Some of the lesser developed nations' strategies provide useful insights on cybersecurity policy approaches in order to provide a better context for small island developing states and other emerging economies. The traditional protections of small size and remote geography do not extend to cyber threats (Ragnarsson & Bailes, 2010).

The Republic of South Africa published its national cybersecurity strategy in 2010 (Department of Communications, 2010; Luiijf et al., 2013). The policy is relatively brief at only twelve pages, but it provided for the establishment of the National Cybersecurity Advisory Council to coordinate policy and interventions by the government (Department of Communications, 2010). The new body was interagency but did not specify one agency or ministry as lead. The strategy's objectives included the reduction of cyber threats, the establishment of international cooperation, capacity building, and public private cooperation (Phahamohkla, van Vuuren, & Coetzee, 2011). The strategy meets the barest essentials recommended by international guidelines. However, the strategy succeeded in promoting an explicit national vision of establishing confidence in a secure information and communications technology environment (Luiijf et al., 2013).

The leading English-speaking allies — the United States (Bush, 2003), the United Kingdom (Cabinet Office, 2009), New Zealand (New Zealand Government, 2011), and Canada (Public Safety Canada, 2010) — published comprehensive national cybersecurity strategies. While each reflected their unique national circumstances, they are decidedly more complex than the one published by the Republic of South Africa. Reflecting the close intelligence, military, and political cooperation among the five English-speaking powers, the national cybersecurity strategies reflected common concerns with national defense and critical infrastructure protection (Luiijf et al., 2013). The five countries viewed the private sector and individual citizens as key stakeholders in cybersecurity strategy (Luiijf et al., 2013). Of particular note, the United States published an international strategy for cyberspace security (Obama, 2011). This document outlined the U.S. international approach to cyberspace security built on accepted international norms of behavior but is beyond the scope of what a Caribbean nation would need to produce.

Similar to South Africa, the New Zealand National Cybersecurity Strategy is relatively short and concise. The New Zealand strategy followed the precepts of strategy guides and included specific guidance on the role of government in meeting the increased risk of an evolving cyber threat. The strategy focused on three key objectives: (a) raise awareness among individuals and small businesses, (b) improve government cybersecurity, and (c) build strategic relationships to secure critical infrastructure (Government of New Zealand, 2011). The strategy provided short- and longer-term objectives and established clear roles and responsibilities within government for cybersecurity activities. It was a strategy designed to communicate to the public.

The designation of responsibility for cybersecurity within government varies. In contrast to the strategy of Canada (Public Safety Canada, 2010), which placed the homeland security agency in charge of cybersecurity efforts, the United States divided responsibility between defense and homeland security (Newmeyer, 2012). New Zealand assigned the responsibility to Ministry of Communications and Technology (Government of New Zealand, 2011). Placing the responsibility outside of the national security apparatus offered an alternative approach that supports economic and public health model approaches to cybersecurity.

The United Kingdom cybersecurity strategy established a new Office of Cyber Security within the Cabinet Office along with a multi-agency Cyber Security Operations Centre located in the military headquarters (Cabinet Office, 2009). The United Kingdom strategy leaned toward national security motivations. The United States' approach divided government cybersecurity between the Department of Homeland Security and the Department of Defense with oversight in the Executive Office of the President (Bush, 2003; Newmeyer, 2012). Similar to the United Kingdom strategy, U.S. cybersecurity strategy was more weighted toward national security models (Harknett & Stever, 2009, 2011; Harknett et al., 2010; Newmeyer, 2012). The failure of national cybersecurity strategies to place one agency or ministry in charge may lead to inefficient and ineffective policy coordination (Luiijf et al., 2013; Newmeyer, 2012).

The Colombian national cybersecurity strategy is clearly aligned with the national security approach. The strategy's stated central objective is to "fortify the capability of the state to meet the threats that attack its security and defense in cyberspace" (Consejo Nacional de Política Económica y Social (Conpes), 2011, p. 20). The strategy placed the national CSIRT, colCERT in the Ministry of Defense and defined clear lines of coordination between the National Police and the military Joint Cyber Command with colCERT (Conpes, 2011). This strategy was even more national security-focused than the U.S. approach. The strategy addressed issues of human capital development, international cooperation, legal reform, and the need for multi-sector collaboration but placed the initial emphasis on the development of police and military capabilities (Conpes, 2011). Interestingly, the Colombian strategy provided timelines and allocated funding for the key elements (Conpes, 2011). This defense-focused strategy may well be a reflection of a culture heavily affected by long-term violence and insurgency.

The Panamanian national cybersecurity strategy emphasized a different cultural focus, namely the protection of critical infrastructure. The Panamanian strategy focused on building confidence in the use of cyberspace in order to derive the benefits of connectivity with minimal risk. Panama focused on six pillars in its strategy: protecting privacy and human rights, prevention and punishment of cybercrime, fortifying national critical infrastructure, building a national cybersecurity industrial base, developing a culture of cybersecurity, and improving the security and response capability of public entities (Republica de Panamá, 2013). The strategy adopted the common elements of international cooperation and development of legal and organizational mechanisms for responding to cyber threats. The explicit emphasis on developing an indigenous commercial cybersecurity industry was somewhat unique. While international recommendations often mention human and technological capacity development (Falessi et al., 2012; Wamala, 2011), Panama's text exceeded those encouragements.

The Trinidad and Tobago cybersecurity strategy recognized the need for improved cybersecurity strategy as a key component of economic development (Inter-Ministerial Committee for Cyber Security, 2012). While Trinidad and Tobago controls significant hydrocarbon resources, cyber-enabled commerce is seen to offer growth and employment opportunities in a number of Caribbean states (Erickson & Lawrence, 2009; Hamilton, 2010; Moore-Miggins, 2012; Mullings, 2011).

Trinidad focused on five pillars common in national cybersecurity strategies: governance, incident management, public-private and international collaboration, cybersecurity culture development, and enactment of required legislation (Inter-Ministerial Committee for Cyber Security, 2012). These themes reflected the suggestions made in Wamala (2011) and Falessi et al. (2012). The strategy incorporated ideas from each of the three primary approaches but the actions directed are primarily related to economic and national security. The strategy provided

a clear series of operational goals coupled with the implementing actions required to meet those goals (Inter-Ministerial Committee for Cyber Security, 2012). To ensure clear lines of accountability and responsibility, the drafters included the establishment of the Trinidad and Tobago Cyber Security Agency (TTCSA) to oversee and implement the plan (Inter-Ministerial Committee for Cyber Security, 2012).

EMERGING BEST PRACTICES

Tagert (2010) found two basic and competing approaches to national cybersecurity policy put forward by the international community for developing African nations: one school of thought argued for the establishment of a CERT as an essential component of cybersecurity whereas the other approach championed the development of a legal structure on cybercrime as the solution. Tagert (2010) found these approaches to be inadequate for Rwanda and Tunisia due to the limited technical capacity and lack of human capital. He found the problems required more multifaceted and tailored approaches aimed at improving the technical capability and policy implementation skills of both government and the private sector in the countries he studied. Since that study, the ITU, Organization for Economic Cooperation and Development (OECD), European Union, and others published material that represents a newly emerging set of international recommendations on the development of national cybersecurity strategy that are more comprehensive and, as a result, more applicable to emerging nations. Building upon Stone's (2008) concept of the global agora, policy recommendations from international organizations, individual nations, and even the private sector are included in this analysis to provide a more robust picture that includes non-official points of view.

International and regional organizations including the ITU (Wamala, 2012), ENISA (Falessi et al., 2012), the European Union (European Commission, 2013), OAS (2004), and the OECD (Smith, Pedrosa, Bernat, Ford, & Mansfield, 2012) have published recommendations for national cybersecurity strategy development. The private sector role in national cybersecurity strategy has begun to emerge. Microsoft published its own recommendations on developing a national strategy. In that paper, Goodwin and Nicholas (2013) encouraged governments to establish priorities for understanding and managing risk to ICT systems that reflect the culture and principles of their nation. The authors also referenced the majority of the items discussed earlier, including establishing CERTs, public information campaigns, workforce development, and international engagement.

Table 1 presents a side by side comparison of the recommended elements of national cybersecurity strategies offered by the various international bodies and Microsoft. Many of these characteristics are highlighted in the earlier discussion of the published national security strategies. Taken as a whole, this comprises the core of the emerging international best practices in the field.

Recommendation	ITU	ENISA	European Union	OAS	OECD	Microsoft
Top-level government support	•	•	•	Implied	•	•
National Cybersecurity Coordinator	•	•	•			•
National Focal Point Organization	•	•				•
Legal framework	•	•	•	•		•
National cybersecurity framework	•	•	•	Implied		•
CSIRT/CERT	•	•	•	•	•	•
Cybersecurity education and awareness program	•	•	•		•	•
Public-Private Partnership/Cooperation	•	•	•	Implied	•	•
Multi-stakeholder approach					•	•
Cybersecurity workforce skills training	•	•			•	•
International cooperation	•	•	•	•	•	•
Technical guidelines/security baselines				•		•
Risk assessment process						•
Identify critical infrastructure		•			•	•
Cyber exercise and contingency plan		•	•		•	•
Civil liberties protections			•	•	•	•

TABLE 1: RECOMMENDED ELEMENTS OF A NATIONAL CYBERSECURITY STRATEGY

The six documents summarized in Table 1 either explicitly or implicitly stressed the need for top-level government support, establishment of CSIRT/CERT, the necessity of public-private cooperation, and a requirement for international cooperation for an effective national cybersecurity strategy. Of the sixteen items identified, recommendations regarding the use of a multi-stakeholder approach, the establishment of a risk assessment process, and the establishment of technical guidelines appeared in less than half of the overall set of recommendations. Cybersecurity public education programs, workforce skills development, establishment of legal frameworks, and civil liberties protections were very common across the recommendations.

RECOMMENDATIONS

Since national cybersecurity strategies are statements of political will, the support of senior political leadership is essential to effective implementation. Without the political will to provide

resources, the strategy remains little more than a nice talking paper. Since cybersecurity is a whole of government (if not a whole of society) problem, the establishment of a national focal point organization is critical. Establishing an interagency, public-private group capable of bringing a multi-stakeholder group capable of dealing with issues at the seams of ministries and the public-private interface is essential. Resolution of the complex problems in developing and implementing a strategy requires trust among all parties.

While an organization is necessary for policy development, one individual must be given the authority to direct the resources and apparatus of the political system to implement that policy. A National Cybersecurity Coordinator, properly empowered by top-level political leadership, will be able to focus on the cybersecurity problem and apply resources where most needed. Divided responsibility inserts added challenges into strategy execution (Newmeyer, 2012).

As indicated earlier, effective cybersecurity policy requires a legal framework to establish responsibilities of all actors. For example, without legislation how can government require data breech disclosure or protect private industry from liability for sharing information with the government or competitors about a cyber threat? Legal frameworks also provide for the prosecution of cybercrimes, gathering and preservation of digital evidence, and privacy protections. Legal frameworks are one element of international cooperation.

Although Tagert (2010) found CERTs alone insufficient to establish cybersecurity, CERTs remain a vital element in a national cybersecurity framework. The CERT/CSIRT serves as a repository of information on threats and incidents. The CERT provides additional technical expertise and is a means of national and international information exchange. The CERT will play a key role in information exchange with the private sector. With the majority of the cyber infrastructure in the private sector, cooperation is essential. Additionally, most of the expertise needed in response to a cyber attack will come from outside of government in developing nations.

The education sector must also play a substantial role in the execution of a national cybersecurity strategy. As in public health, it is necessary to inform all users about proper cyber hygiene and what actions to take in a cyber incident. Public information campaigns should be a key part of the national cybersecurity strategy. Developing nations at present have limited cyber workforce skills. As more systems become interconnected and reliance on the Internet for delivery of services increases, it is necessary to build domestic capacity to protect, operate, maintain, and develop the infrastructure.

Critical infrastructure protection should be a key aim of the national cybersecurity strategy. Establishment of minimal standards is necessary in an economic or public health model of cybersecurity. Some countries have adopted ISO 27000 and the U.S. is adopting the NIST framework in an effort to improve the resilience and reliability of critical systems. All countries face resource limitations; however it is necessary for the government and private sector to identify those installations and systems necessary for the maintenance of security and stability. It is impractical to expect that all risks in critical infrastructure can be eliminated. A risk evaluation framework is needed to guide investments toward areas of greatest effect.

An exercise program that tests the validity of contingency plans is essential. The first responder axiom that it is best not to exchange business cards at the scene of a disaster applies equally to cyber issues. The first time government and corporate leaders decide how to respond to a cyber threat should not be after the power grid has been shut down.

Finally, it is necessary to establish protections for civil liberties in the national cybersecurity strategy. The Internet has flourished as a means of free expression and open collaboration. Recent incidents have demonstrated the vulnerability of personal communications and data systems to intrusions on

privacy. A cybersecurity policy that inhibits free expression in the name of security is inconsistent with human rights.

Developing nations want to use the Internet and globalization to grow their economies and create opportunity for their people. Implementation of effective national cybersecurity strategies should improve the odds for success.

REFERENCES CITED

Agresti, W.W. (2010). The four forces shaping cybersecurity. *Computer*, 43(2), 101–104. doi: 10.1109/MC.2010.53

Barnard-Wills, D., & Ashenden, D. (2012). Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture*, 15(2), 110–123. doi: 10.1177/1206331211430016

Bellovin, S. M. (2009). The government and cybersecurity. *Security & Privacy, IEEE*, 7(2), 96–96. doi: 10.1109/MSP.2009.55

Betz, D. J., & Stevens, T. (2011). Chapter Two: Cyberspace and sovereignty. *Adelphi Series*, 51(424), 55–74. doi:10.1080/19445571.2011.636955

Bumiller, E., & Shanker, T. (2012, October 11). Panetta warns of dire threat of cyberattack on U.S. *The New York Times*. Retrieved from www.nytimes.com

Bush, G.W. (2003). *The national strategy to secure cyberspace*. Retrieved from www.whitehouse.gov

Cabinet Office (2009). *Cybersecurity strategy of the United Kingdom: safety, security and resilience in cyber space*. Retrieved from www.cabinetoffice.gov.uk/media/216620/css0906.pdf

Charney, S. (2012). Collective defense: Applying the Public-Health Model to the Internet. *IEEE Security & Privacy* 10 (2), 54–59. doi:10.1109/MSP.2011.152.

Consejo Nacional de Politíca Económica y Social (Conpes)(2011, July 14). *Linamientos de la política para ciberseguridad y ciberdefensa* (Documento Conpes No. 3701). Bogota, DC: Government of Colombia. Department of Communications, Republic of South Africa (2010, February 19). Draft cybersecurity policy. Government Gazette No. 32963. Retrieved from http://www.pmg.org.za/files/docs/100219cybersecurity.pdf

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, 15(1), 105–122. doi: 10.1111/misr.12023

Ellefsen, I., & von Solms, S. (2010). Critical information infrastructure protection in the developing world. In T. Moore & S. Shenoi (Eds.), *Critical infrastructure protection IV* (pp. 29–40). Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-16806-2_3

European Commission. High Representative of the European Union for Foreign Affairs and Security Policy. (2013). Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity strategy of the European Union: An open, safe and security cyberspace. Available at http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

European Network and Information Security Agency [ENISA] (2012, May 8). National cyber security strategies: Setting the course for national efforts to strengthen security in cyberspace. Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

Falessi, N., Gavrila, R., Klenstrup, M.R., & Moulinos, K. (2012). National cyber security strategies: Practical guide on development and execution. Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

Ghernaouti-Hélie, S. (2009). *Cybersecurity Guide for developing countries* (Enlarged Ed.). Geneva, Switzerland: International Telecommunication Union. Available at http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf

Harknett, R. J., Callaghan, J. P., & Kauffman, R. (2010). Leaving deterrence behind: War-fighting and national cybersecurity. *Journal of Homeland Security & Emergency Management*, 7(1), 1–24

Harknett, R J., & Stever, J. (2009). The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen, *Journal of Homeland Security and Emergency Management*, 6 (1), Article 79. doi: 10.2202/1547–7355.1649

Harknett, R. J., & Stever, J. A. (2011). The new policy world of cybersecurity. *Public Administration Review*, 71(3), 455–460. doi: 10.1111/j.1540-6210.2011.02366.x

Inter-Ministerial Committee for Cyber Security (2012, December). *Government of the Republic of Trinidad and Tobago: National cyber security strategy*. Retrieved from http://www.nationalsecurity.gov.tt/Portals/0/Pdf%20Files/National_Cyber_Security%20Strategy_Final.pdf

Klieiner, A., Nicholas, P., & Sullivan, K. (2013). Linking cybersecurity policy and performance. Seattle, WA: Microsoft Trustworthy Computing. Retrieved from http://www.gwumc.edu/hspi/events/Microsoft_whitepaper.pdf

Klimberg, A. (ed.) (2012). National cybersecurity framework manual. Tallinn, Estonia: NATO CCD COE Publication

Kramer, F.D. (2011) Cyber security: An integrated governmental strategy for progress. [Special issue] *Georgetown Journal of International Affairs* 124, 136–150

Lock-Teng Low, K., Fook Ong, S., & Aun Law, K. (2011). Sustainable ICT development: A perspective from ICT loops in developing nations. *International Journal of Academic Research*, 3(6), 92–97

Luiijf, E., Besseling, K., & Graaf, P. D. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, 9(1), 3–31. doi: 10.1504/IJCIS.2013.051608

McAfee (June, 2014). Net losses: Estimating the global cost of cybercrime. Retrieved from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Moore, T. (2010). The economics of cybersecurity: principles and policy options. *International Journal of Critical Infrastructure Protection* 3 (3–4), 103–117

Mulligan, D. K., & Schneider, F.B. (2011). Doctrine for cybersecurity. *Daedalus* 140 (4), 70–92. doi: 10.1162/DAED_a_00116

Newmeyer, K. (2012). Who should lead U.S. cybersecurity efforts? *Prism*, 3(2), 99–120. Retrieved from http://www.ndu.edu/press/lib/pdf/prism3-2/prism115-126_newmeyer.pdf

New Zealand Government, (2011). *New Zealand's cyber security strategy*. Retrieved from www.med.govt.nz/cyberstrategy

Obama, B. (2011). International strategy for cyberspace: Prosperity, security, and openness in a networked world. The White House. Available at http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Obama, B. (2013, February 12). Executive Order 13636 – Improving critical infrastructure cybersecurity. Retrieved February 14, 2013, from http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Organization of American States (2004). A comprehensive Inter-American cybersecurity strategy: A multidimensional and multidisciplinary approach to creating a culture of cybersecurity. AG/RES. 2004 (XXXIV-O/04). Retrieved from http://www.cicte.oas.org/Rev/En/Documents/OAS_GA/AG-RES.%202004%20%28XXXIV-O-04%29_EN.pdf

Phahamohlaka, L., Jansen van Vuuren, J., & Coetzee, C. (2011). Cybersecurity awareness toolkit for national security: An approach to South Africa's cyber security policy implementation. *Proceedings of the South African Cyber Security Awareness Workshop (SACSAW 2011)*. Retrieved from http://www.csir.co.za/dpss/docs/SACSAWFinal_16Aug.pdf

Public Safety Canada (2010). Canada's cyber security strategy: For a stronger and more prosperous Canada. Canada: Government of Canada. Catalog Number PS4-102/2010E-PDF. Retrieved from http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf

Ragnarsson, J. K., & Bailes, A. J. (2010). Iceland and cyber-threats. *RANNSÓKNIR Í FÉLAGSVÍSINDUM XI*, 60–65. Retrieved from http://skemman.is/stream/get/1946/7179/19284/1/STJbok-ritstyrt-heild.pdf#page=69

Republica de Panamá (2013, May 17). *Elementos de la estrategia nacional de seguridad cibernética y protección de infraestructura crítica* (Gaceta Oficial Digital No. 27289 Resolución No. 21). 34–43. Panamá, Panamá: Consejo Nacional para la Innovación Gubernamental, Republica de Panamá

Rishikof, H., & Lunda, K. E. (2011). Corporate responsibility in cybersecurity. *Georgetown Journal of International Affairs*, 12(1), 17–24.

Rosenzweig, P. (2011). Cybersecurity, the public/private 'partnership,' and public goods. Hoover National Security and Law Task Force. Palo Alto, CA. Available at SSRN: http://ssrn.com/abstracts=1923869

Ruth, S., & Stone, S. (2012). A legislator's dilemma. *IEEE Internet Computing*, 16(6), 78–81. doi: 10.1109/MIC.2012.127

Smith, Geoff et al. 2012. *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*. Organization for Economic Cooperation and Development. Retrieved for http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Sund, C. (2007). Towards an international roadmap for cybersecurity. *Online Information Review* 31 (5), 566–582. doi: 10.1108/14684520710832306

Tagert, A. (2010). Cybersecurity Challenges in Developing Nations. Unpublished dissertation, Carnegie Mellon University, Pittsburgh, PA. Retrieved from http://repository.cmu.edu/dissertations/22

The White House. (2009). *Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure*. Washington, DC: The White House

Thomas, N. (2009). Cyber security in East Asia: Governing anarchy. *Asian Security*, 5(1), 3–23. doi: 10.1080/14799850802611446

Vacca, W. A. (2011). Military culture and cyber security. *Survival*, 53(6), 159–176. doi: 10.1080/00396338.2011.636520

Wamala, F. (2011). *The ITU national cybersecurity strategy guide*. Geneva, Switzerland: International Telecommunications Union. Retrieved from www.itu.int

Wegener, H. (2007). Harnessing the perils in cyberspace: Who is in charge? *Disarmament Forum* 3, 45–52. Retrieved from http://www.unidir.org/pdf/articles/pdf-art2646.pdf

Whittaker, Z. (2011, September 7). Cybercrime costs $338 bn to global economy; More lucrative than drugs trade. *ZDNet*. Available at www.zdnet.com

AUTHOR

Kevin Newmeyer (Kevin.newmeyer@gmail.com) is the senior operations director for the CREATE project of the Department of Defense High Performance Computing Modernization Program and a fellow at the National Cybersecurity Institute. A retired United States naval officer, he served on five ships in a combination of command and nuclear engineering assignments. Following the attacks on September 11, 2001, he was detailed to the Organization of American States to establish the Secretariat for the Inter-American Committee against Terrorism (CICTE). His research focuses on international policy issues in cybersecurity. Newmeyer earned a doctorate in public policy from Walden University, and earned a master's degree in international relations from the Instituto Universitario Ortega y Gasset in Madrid, Spain, as an Olmsted Scholar. He holds additional degrees from Escuela Diplomática of Spain, George Mason University, and the U.S. Naval Academy.

Data-Centric Security

A. H. Kabir

ABSTRACT

Gone are the days when endpoints of the organization were confined to desktops and laptops connected to the LAN and somewhat easy to secure. Endpoints now include virtual users, mobile devices, SaaS applications, external consultants and even partner organizations with a need to exchange information. This paper briefly discusses various frameworks, tools, and techniques of data-centric security. It also discusses, in moderate details, some popular data-centric security measures such as Encryption and Data Masking. Finally, emerging platforms such as big data and cloud environments are also part of detailed discussion in this paper. It discusses the impetus of data-centric security, its current strengths, weaknesses, and adoption approaches in Hadoop ecosystem. And for Cloud environments, this paper discusses the mechanisms and trends for securely sharing, verifying, and tracing data as it flows between cloud users.

WHY DATA NEEDS A NEW APPROACH TO PROTECTION

With data access no longer restricted to the four walls of the enterprise and 8-to-5 business hours, enterprises that have traditionally relied on a perimeter-based approach to security are now seeing the benefits of a data-centric approach. Data-centric security focuses on protecting data rather than protecting the network where the data lives. The Nexus of Forces puts data at risk. The rapidly growing significance of Software as a Service (SaaS), bring your own device (BYOD), mobile devices, and changing work patterns increasingly conflict with regulatory requirements for information control. Concurrently, the growing volume of information about sophisticated criminal and nation-state snooping and hacking has forced companies to focus on protecting what they really care about— critical data.

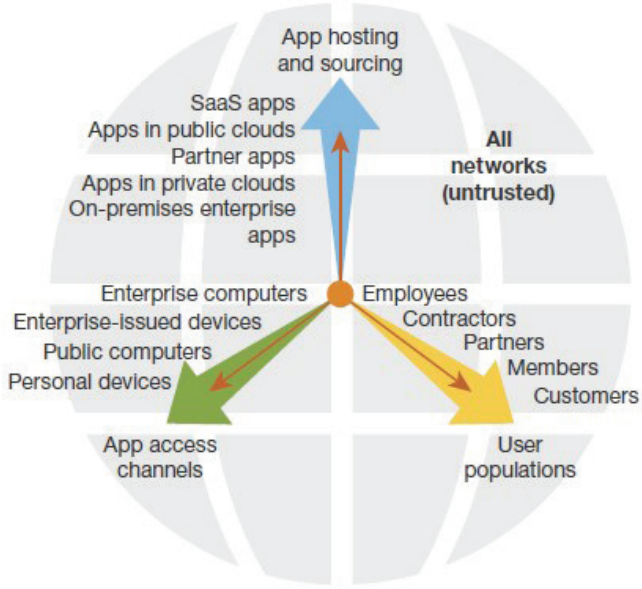

FIGURE 1: DATA-CENTRIC SECURITY FRAMEWORK

(September 12, 2013, "Transform Your Security Architecture And Operations For The Zero Trust Ecosystem", Forrester Report)

DATA-CENTRIC SECURITY FRAMEWORK

Now would be the ideal time to bring together separate silos of security controls such as archiving, access management, and Data Loss Prevention (DLP), and to move these controls closer to the data itself, instead of at the edges (perimeters) of networks. In organizations that are complex, or those with huge amounts of data, cybersecurity personnel may not always know where to start. We are going to break the task down to three main areas: 1) defining the data; 2) dissecting and analyzing the data; and 3) defending and protecting the data.

Defining the Data

Organizations generate data daily, and in many cases, they amass vast amounts of it in "Big Data" storages. Few enterprises have proper data governance in place, and, as a result, they have data strewn across global data centers, computer rooms, remote offices, laptops, desktops, mobile devices, and now, cloud storage. The enterprise cannot protect it all; it is too operationally complex and costly to encrypt everything. Therefore, security and risk (S&R) professionals, together with their counterparts in legal and privacy, should define data classification levels based on toxicity. This allows security to properly protect data based on its classification once they know where that data is located in the enterprise. Discovery and classifications are critical for the following reasons:

- **Data discovery locates and indexes data.** To protect data, the enterprise must first know where users have stored it. S&R professionals, together with legal and privacy teams, must undertake a data discovery project to locate and index existing data and develop a life-cycle approach that continuously discovers data as users create it throughout the extended enterprise network.
- **Data classification catalogs data to make it easier to control.** One of the preliminary steps in the assessment is to classify the data according to risk factors, such as:
  - *Public:* Data whose release would have little or no negative impact on the organization.
  - *Internal Operational:* Data needed by company personnel in the course of their work and not intended for public dissemination.
  - *Confidential:* Data regulated by privacy legislation (or deemed confidential by contractual obligations), which, if released, could cause legal difficulties and/or embarrassment.

Management must also consider the possible loss of reputation or competitive advantage, regulatory and legal sanctions, and breach of contract if data falls into the wrong hands. Even after inherent risks have been identified, residual risks remain. After installing the mitigating controls for the inherent risks, additional compensating controls can reduce the residual risks to an acceptable level.

Dissecting and Analyzing the Data

Data dissection is a continuous process. Cybersecurity personnel need to have continuous visibility into the changing threats to the data. We expect that security network analysis and visibility (NAV) and security information management (SIM) solutions work hand-in-hand with big data to increase decision making for security. More specifically:

- **Data intelligence provides business and other contextual insights about data.** The value of data changes over time. Some data — such as acquisition plans or product road maps — can be confidential one day and unimportant the next (for instance after the completion of a deal or the successful launch of a new product). Classifications can also change because of changes in government or industry regulations. In addition to changing classification, it is important to understand the current state of data. For example, has someone compromised its integrity? Is there an exfiltration in process? How does data normally flow through the organization? By linking SIM and NAV data, companies are able to

determine the state of their network in near real time, thereby finding potential breaches or insider abuse much more quickly.

- **Data analytics identifies changing threats to data and guides decision making.** To gain more insights into the changing threats to data, S&R pros must do a much better job of anticipating threats to their industry and enterprise, targeting efforts where it matters most, and limiting the damage of breaches that have already occurred. The promise of analytics, in some cases, married with big data processing, includes the ability to analyze more data in near real time to proactively protect confidential data. Security pros should anticipate using this data more efficiently to prioritize security initiatives and effectively place the proper security controls. For example, comparing vulnerability data with device configuration and real-time threat data tells the organization where its most vulnerable assets are and helps it create defenses that are more targeted and proactive.

  Additionally, look for more precise threat intelligence offerings as these vendors take advantage of big data. Considering threat intelligence that specifically makes reference to attackers targeting an organization and aligning that data with the organization's internal big data analytics platform provides a powerful defensive advantage against new threats.

Protecting Data and Available Tools

So far we have addressed the need for data-centric security, why it is needed, and which tools fit the model. Now let us take a look at some specific scenarios of how to implement and deploy data-centric security. The following are some concrete examples of how the tools are deployed to support a data-centric model.

- *Gateways:* A gateway is typically an appliance that sits in-line with traffic and applies security as data passes. Data packets are inspected near line speed, and sensitive data is replaced or obfuscated before packets are passed on.

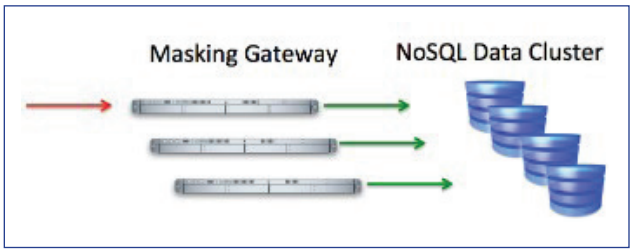

FIGURE 2: GATEWAYS

Gateways are commonly used by enterprises before data is moved off-premise, such as up to the cloud or to another third-party service provider. The gateway sits inside the corporate firewall, at the 'edge' of the infrastructure, discovering and filtering out sensitive data. For example, some firms encrypt data before it is moved into cloud storage for backups. Others filter Web-based transactions in-line, replacing credit card data with tokens without disrupting the Web server or commerce applications. Gateways offer high-performance substitution for data in motion, but they must be able to parse the data stream to encrypt, tokenize, or mask sensitive data.

- *Hub and Spoke:* Extract, Transform, and Load (ETL) has existed for nearly as long as relational databases. It describes a process for extracting data from one database, masking it to remove sensitive data, then loading the desensitized data into another database. Over the last several years, we have seen a huge resurgence of ETL, as firms look to populate test databases with non-sensitive data that still provides a reliable test-bed for quality assurance efforts. A masking or tokenization 'hub' orchestrates data movement and implements security. Modeled on test data management systems, modern systems alter

health care data and PII (Personally Identifiable Information) to support use in multiple locations with inconsistent or inadequate security. The hub and spoke model is typically used to create multiple data sets, rather than securing streams of data. To align with the hub and spoke model, encryption and tokenization are the most common methods of protection. Encryption enables trusted users to decrypt the data as needed, and masking supports analytics without providing the real (sensitive) data.

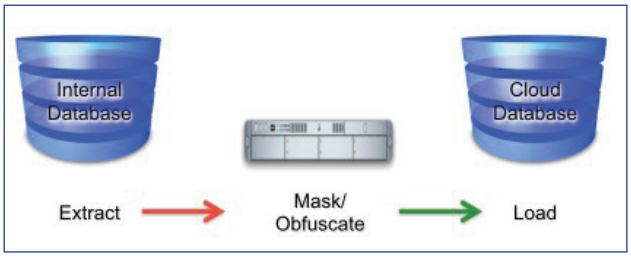

FIGURE 3: HUB AND SPOKE

- *Reverse Proxy:* As with the gateways previously described, in the reverse-proxy model an appliance — whether virtual or physical — is inserted in-line into the data flow. But reverse proxies are used specifically between users and a database. Offering much more than simple positional substitution, proxies can alter what they return to users based on the recipient and the specifics of their request. They work by intercepting and masking query results on the fly, transparently substituting masked results for the user. For example, if a user queries too many credit card numbers, or if a query originates from an unapproved location, the returned data might be redacted. The proxy effectively, intelligently, and dynamically masks data. The proxy may be an application running on the database or an appliance deployed in-line between users and data to force all communications through the proxy. The advantage of proxies is that they enable data protection without needing to alter the database — they avoid additional programming and quality assurance validation processes.

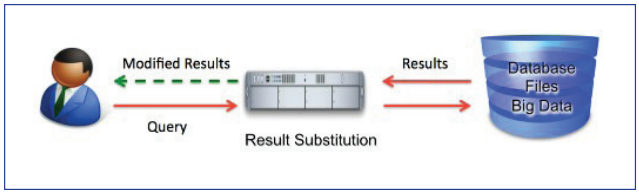

FIGURE 4: REVERSE PROXY

This model is appropriate for PII/PHI data, when data can be managed from a central location but external users may need access. Some firms have implemented tokenization this way, but masking and redaction are more common. The principal use case is to protect data dynamically, based on user identity and the request itself.

- *Other Options:* There are at least two other security platforms worth mentioning. Data Loss Prevention (DLP) systems and Digital Rights Management (DRM) are forms of data-centric security which have been in use for over a decade. DLP systems are designed to detect sensitive data and ensure data usage complies with security policy — on the network, on the desktop, and in storage repositories. DRM embeds ownership and usage rules into the data, with security policy (primarily read and write access) enforced by the applications that use the data. DLP protects at the infrastructure layer, while DRM protects at the application layer.

Both of these platforms use encryption to protect data. Both allow users to view and edit data depending on security policies. DLP can be effectively deployed in existing IT environments, helping organizations gain control over data already in use. DRM typically needs to be built into applications, with security controls (e.g., encryption and ownership rights) applied to data as it is created. These platforms are designed to expose data (making it available to users) on demand. This means that to leverage these security controls users need to deploy these platforms everywhere they want to use data. These data-centric models work for migrating on-premise systems to Infrastructure as a Service (IaaS), but do not lend themselves to some

of the emerging use cases. DLP is not easy to extend beyond corporate IT boundaries into the cloud, and both models tend to compromise the performance and scalability of NoSQL clusters.

ENCRYPTION: A KEY DATA-CENTRIC SECURITY CONTROL

Encryption is a key control in a data-centric system because the data is moving across different systems and is often open to attack from various sources along the way. Encryption is the most effective way to protect data in motion. This does not mean that encryption needs to be applied in all cases, but it does mean that it is normally appropriate to develop an encryption strategy as a subset of the overall control strategy. Therefore, the direct result of the risk analysis is the identification of which data needs to be encrypted. In some cases, it is simply not possible to encrypt data; for example, many mobile devices do not have effective security capabilities. In these cases, alternative controls need to be developed.

The Role of Encryption

The power of encryption to protect data at rest or in motion makes it one of the most powerful controls to consider if strong protection is needed. Wherever possible, a single encryption methodology, such as one based on the Pretty Good Privacy (PGP) standard, should be used throughout the organization so that data can be easily recovered if the encryption keys are lost or corrupted. It is normally not sufficient to make use of the encryption technologies that exist in the various repositories of information, such as laptops, PDAs or cell phones, or technologies such as Wi-Fi or Bluetooth.

A single encryption methodology must be used throughout the organization because:

- files that have been encrypted must remain accessible in future years for business, audit, tax, and other regulatory purposes. Therefore the organization must control the decryption technologies and keep the cryptography keys;
- the systems within which the data may be traveling are likely to be different sizes, and the encryption process must be scalable in order to operate as effectively on a single small computer as it does on several large systems;
- as data moves from platform to platform, the encryption solution must work on any significant platform in the system;
- without a single encryption technology in place, any data will have to be decrypted for use and then re-encrypted after use.

Encryption Standards

Everyone knows how important it is to encrypt private or sensitive data because it transfers over the public Internet. There are several different types of encryption, including symmetric, asymmetric (also known as public key encryption), and hash algorithms. Key lengths of 1,024 bits (each bit of a key increases the difficulty of a brute-force attack exponentially) and a cipher strength of 128 bits are used at minimum.

Symmetric key encryption is most commonly associated with password or passphrase-based encryption.

FIGURE 5: SYMMETRIC KEY ENCRYPTION

Figure 5 illustrates how the same key is used for encryption and decryption. Symmetric key encryption works best for non-persistent data, or static, non-transactional data. Non-persistent data is typically encrypted with a symmetric key (passphrase) and sent to another entity for use. In this way the data is protected while it is at rest before the data is sent, while it is in motion, and when it reaches the data consumer. There is no need for the data to persist.

However, symmetric-based encryption does not scale well particularly when the data needs to persist or when it needs to be shared with multiple recipients.

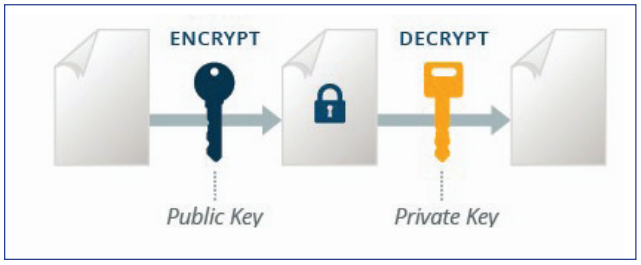

FIGURE 6: ASYMMETRIC KEY ENCRYPTION

When data needs to be protected for longer periods of time for compliance or regulatory purposes, and when it is going to be shared with multiple sets of recipients, the best option is asymmetric keys, otherwise known as public key encryption. Public key encryption uses both a public key and a private key. The public key is used for encryption and authentication while the private key is used for decryption and digital signing. The two keys are mathematically related through the use of cool math including prime integer factorization, discrete logarithm, and elliptic curve relationships. The strength of the encryption is based on the computational intensity that it would take to exhaustively determine the private key. The public key should be easily accessible to any authorized user, and the private key should be kept private and protected.

The key in public key encryption is based on a hash value. This is a value that is computed from a base input number using a hashing algorithm. Essentially, the hash value is a summary of the original value. It is important to note that it is nearly impossible to derive the original input number from a hash value without knowing the data used to create the hash value. The following is a simple example:

Input Number: 10,667
Hashing Algorithm: Input # × 143
Hash Value: 1,525,381

It is clear how difficult it would be to determine that the value 1,525,381 came from the multiplication of 10,667 and 143. But if it was known that the multiplier was 143, then it would be very easy to calculate the value 10,667. Public-key encryption is actually much more complex than this example, but this example depicts the basic idea.

Public keys generally use complex algorithms and very large hash values for encryption, including 40-bit or even 128-bit numbers. A 128-bit number has a possible 2128, or 3,402,823,669,209,384,634,633,746,074,300,000,000,000,000,000,000,000,000,000,000,000,000,000 different combinations — this would be like trying to find one particular grain of sand in the Sahara Desert.

Key Management

The strength of an encryption algorithm is measured by two factors: the effective length of the key and its ability to withstand attack. That ability is ultimately dependent upon its implementation. A critical component of any cryptographic implementation is the key management techniques used. A key management strategy answers the questions: what key is used, and how often? Where is it stored and who has access to it? How is it to be kept secret?

Encryption keys must often be shared or distributed for an effective implementation. In these cases, public/private key pairs can be generated to secure key distribution. As a Data Encryption Standard (DES) encryption key is generated, it can be encrypted by the recipient's public key before it is sent. The private keys used for distribution

and decryption should have restricted access and be changed as often as needed to ensure adequate privacy and security.

A DES symmetric key can also be used to encrypt data to be stored on file systems or in databases. Again the secret key should have limited access and change periodically. One approach is to define a usage pattern for multiple keys, and encrypt all keys with a master key having stronger encryption. Master keys can be changed more often with less effort. The basic concept here is that a moving target is harder to shoot.

Although all organizations need basic key management controls, they vary in rigor and expense from organization to organization. For example, it is usually appropriate for key management to be fully automated and for private keys to be kept confidential; all keys, however, must be encrypted. Keys used to encrypt other keys must be different from the keys used to decrypt data. Short-life keys should, wherever possible, carry activation and deactivation dates. It is important that keys be chosen randomly.

DATA MASKING

Why Data Masking

Data Masking is a method — consisting of one or more transformation techniques — to manipulate data in order to maintain data utility for a specific use case while protecting the secrecy of sensitive information and/or the privacy of individuals as it relates to sensitive information. Data masking aims to balance secrecy and privacy requirements of data with utility requirements of applications and processes. It takes advantage of the fact that not every process and application has to use actual sensitive data and that sensitive data may be transformed to become less sensitive while still useful. Data masking can be applied where encryption is not a suitable control, for example: lower-layer encryption provides little control, higher-layer encryption does not maintain format.

Data masking goes by many names, some of which are specific to the implementation or industry. Data de-identification, data obfuscation, data anonymization, data de-valuation, data scrubbing, and data scrambling are commonly accepted terms to describe the general concept of data masking, often in the context of structured data. Data sanitization and data redaction refer to the technique for "blacking out" sensitive information, often in the context of unstructured data (e.g., documents and photos).

Data Masking Architecture

One aspect of data masking is the architecture that implements the masking operations, which determines how masked data is created and in which locations data can be protected. The three data masking architecture choices are: static, dynamic, and hybrid.

Static Data Masking (SDM)

Static Data Masking (SDM) aims to deter the misuse of data by users of nonproduction (mostly testing, and also training and analytics) databases (typically programmers and testers) through transformation of data items in advance of its use in the database.

SDM offers the most options for masking techniques because it does not operate in real time and can most easily process individual records in the context of the larger dataset that has been extracted for masking. The masking solution can utilize statistical analysis of the data to support substitution, generalization, and shuffling in order to maximize privacy protection. This breadth of masking is useful for non-production environments, and test data management suites often include SDM for that reason. SDM can also implement redaction and substitution for production environments, including for unstructured data.

Dynamic Data Masking (DDM)

Dynamic Data Masking (DDM) applies masking operations in real time as an application or a person accesses data. The original, sensitive data resides

in the repository and is accessible to an application when authorized by policy. Applications that are not authorized to access the sensitive information are provided with masked data instead. The masking capability may be part of the repository, a mediator between the repository and the application, invoked by the platform or presentation infrastructure, or invoked as part of the application. DDM does not change the data in the underlying repository.

DDM mostly works at the record or file level, provides a subset of masking techniques (i.e., redaction, suppression, and substitution), and is mainly aimed at masking in production environment. Utilizing DDM to feed non-production environments is technically possible, but the absence of other masking techniques reduces the level of privacy control that could be achieved. Incorporating more advanced masking techniques would be possible, but their use generally makes little sense in production environments. DDM should, therefore, be thought of as a type of access control and can, in fact, be used to enhance existing access controls (e.g., DDM can provide fine-grained control for a database even if permissions on the database itself cannot be changed).

Hybrid Data Masking (HDM)

Hybrid Data Masking (HDM) — often referred to as tokenization in products — combines elements of SDM and DDM: A sensitive field in a dataset is replaced with a substitute, and the mapping between the original and the substitute is stored in a different, protected dataset. The unmasking operation can then be applied in real time as an application accesses the data, or the application can be served by the substitute. Like DDM, the masking and unmasking capability may be part of the repository, a mediator between the repository and the application, invoked by the platform or presentation infrastructure, or invoked as part of the application. Because HDM must store the mappings in a secure database and implement an algorithm for unique, consistent substitution, performance is a critical consideration in the architecture.

Like DDM, HDM works at the field level and is most applicable to production environments. Substitution of key identifiers is generally not a good privacy control, which limits non-production use of the masked data. Because the goal of HDM is to replace sensitive identifiers with surrogates in as many applications as possible, the substitute value itself may become a critically important data element. Ensuring its proper protection in production environment, even though certain confidentiality risks are reduced, is an important consideration.

Data Masking Architecture and Security Objectives

Ensuring secrecy and privacy of information is a high-level concept that does not describe when and where information must be protected. In essence, data masking — like other preventative controls — attempts to protect sensitive data from unauthorized access and use. In general, data can exist in three states:

- *Data in use by application or people:* This is the main confidentiality objective of data masking, which is enabled by the fact that sensitive data is required in some, but not all, business processes and applications. The masking architecture is designed so that data is masked by the time it reaches the target user or application. All architectures protect data in use, although HDM creates a new set of possibly critical transaction data that needs its own protection.
- *Data at rest in repositories, systems, and application*: Protection of data at rest is created by the location of the enforcement points that perform the masking and — for HDM — unmasking. DDM does not protect data at rest because masking is applied to outbound data only, but static and HDM do. HDM requires protection of the database containing the substitution tables, which adds to data-at-rest protection concerns.
- *Data in motion in communication channels:* The protection of data in motion is also created by location of the enforcement points, and transmitting at-rest protected data automatically protects

it in motion. As such, all architectures protect data in motion, although the level of protection provided by dynamic and HDM depends on how close to the data source the masking takes place.

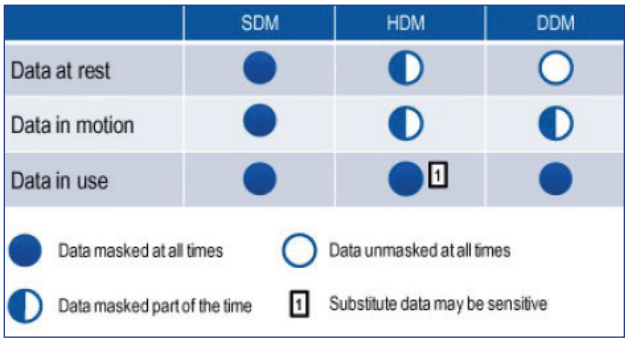

FIGURE 7: PROTECTION CAPABILITIES OF MASKING ARCHITECTURE

DATA-CENTRIC VIEW OF CLOUD SECURITY

The economics of outsourcing data and computation will likely spur a continued migration of applications to the cloud. Just as the Internet is becoming dominated by applications that require data integration and sharing, we similarly expect that applications within the cloud will become increasingly interdependent. The trend toward interoperable cloud applications will require solutions that enable the secure communication and exchange of data between the cloud's users. While cloud security has recently gained traction in the research community, much of this effort has focused on securing the underlying operating systems and virtual machines that host cloud services. A comprehensive solution has to go beyond OS and VM-centric security solutions and, in particular, must provide mechanisms for securely sharing, verifying, and tracing data as they flow between cloud users.

Mutually Verified Attribute Model

The new cybersecurity paradigm must rely on trusted, self-sufficient data packages that provide data consumers a high degrees of assurance that the information is genuine, unaltered, and completely trustworthy while ensuring that only the right people get access to the right information at the right time.

These data packages must carry with them all the attributes and mechanisms to enable this two-way trust relationship between the data and its consumers so that the cloud computing/network environment is essentially taken out of the trust model altogether. The cloud computing environment is simply where the data resides, and the network is just a means of transit from one place to another. Data can safely reside and travel virtually anywhere to support authorized users in any environment.

In this Mutually Verified Attribute Model, the data package and the data consumer continually maintain a set of attributes that can be irrefutably proven by the other as being genuine, unaltered, and verified by a known and trusted third party. Embedded data package attributes might include: unique data package identifier, data classification and authorized data consumer roles, access parameters, etc. On the other hand, embedded data consumer attributes might include: identity, authorization level, organizational affiliation, citizenship, etc.

In this Mutually Verified Attribute Model, the data package and the data consumer must also continually travel with a set of trusted mechanisms that each can rely on to accurately validate and verify the attributes of the other (and their environment) as being genuine, unaltered, and verified by a known and trusted third party.

Bringing Data Packages and Data Consumers Together

To efficiently bring data consumers and data packages together in the cloud environment, one more element may be required: data brokers. Dispatched

by data consumers, data brokers would scour the multitude of network environments, assisting in locating the data packages containing the desired information which is most convenient to the data consumer's situation.

The data broker paradigm could take many forms. Data brokers could simply wander the networks (not unlike taxicabs driving the streets of London) either occupied with a request from a data consumer or free to "pick up" a new request. They could reside at key locations around the globe much like today's Web servers do, awaiting the next data consumer's request. Regardless of the model chosen, the data broker would likely include attributes, abilities, and characteristics such as:

- identity attributes similar to that used for data packages to permit trusted validation of the data broker's identity by data consumers;
- the ability to search and possibly index metadata;
- the ability to cross-reference metadata to data packages and their locations or contact methods;
- integrity/non-repudiation mechanisms (similar to those currently used for digital signature) used to validate data consumer information such as identity, role, and authorization level, before accepting requests.

Verifying Network and Cloud Computing Environment

One final factor in cloud environment may be the need to verify the nature of the cloud computing or network environment inhabited by data packages. The nature of the cloud computing environment might be characterized as public, community, hybrid, or private and include the identity of the cloud provider. The network environment might be characterized as friendly, benign, or hostile; it may simply be characterized as trusted or untrusted. Certain data packages, based on their attributes, might be permitted to reside only in certain cloud computing environments or allowed to traverse only specific network types, whereas others might be permitted in all cloud computing environments and on all networks regardless of their nature.

This environmental validation would require an additional set of mechanisms to either validate a cloud computing environment/network based on its credentials or treat a cloud computing environment/network as untrusted when it cannot supply the required, proven credentials (e.g., in the case of a network that is not equipped to operate in the new paradigm). This verification would also require new technologies and would, in essence, serve as the corollary to emerging Network Access Control models, with the data deciding whether to permit itself to enter the cloud computing environment network based on the degree to which it can be trusted.

DATA-CENTRIC SECURITY FOR BIG DATA

Big data environments enable data to be transposed between structured, unstructured, and semi-structured formats, enabling data to flow among them, and through applications and analytics. The concept of data silos and the application of data security governance, based upon the structure of stored data, are broken. This exposes uncoordinated data security policies and management, and is a recipe for security chaos.

Two challenges in protecting Hadoop have been a lack of security features built into Hadoop 1.0 and the way MapReduce interacts with data that is stored in HDFS, frequently without predetermined structure.

The general availability of many (proprietary) Hadoop security add-ons and features has coincided with the release of Hadoop 2.0 ("YARN"). For example, enhanced enterprise integration and authentication, increasingly granular authorization and transparent data encryption now implement strong controls. In recently released Cloudera CDH 5.1, cell-level access control in HBase was added for securing sensitive data.

Externalized Data Security: Data Services, Discovery, Masking, Redaction, and Tokenization

Externalization of data security means that data security controls are placed outside of Hadoop. Data security controls outside Hadoop can be applied to:

- *Data inbound to Hadoop:* For example, data masking, data redaction, or tokenization before load de-identifies personally identifiable information (PII) data before load. Therefore, no sensitive data is stored in Hadoop, keeping the Hadoop Cluster out of (audit) scope. This may be performed in batch or real time and can be achieved with a variety of designs, including the use of static and dynamic data masking tools, as well as through data services.

- *Data that is retrieved from Hadoop:* For example, use the generic Sqoop Java Database Connectivity (JDBC) connector to export data to a traditional data warehouse that can enforce standard SQL security on the exported data. Depending on the vendor of the traditional database, it may be able to find more efficient connectors than the generic Sqoop JDBC connector. In this example, access to Hadoop is allowed only through a traditional data warehouse; therefore, data in Hadoop is inheriting all data warehouse controls. Abstracting the Hadoop ecosystem behind a data services layer can achieve the same result.

- *Data discovery*: For example, identifying whether sensitive data is present in Hadoop, where it is located and subsequently triggering the appropriate data protection measures, such as data masking, data redaction, tokenization, or encryption. For structured data going into Hadoop, such as relational data from databases, or, for example, comma-separated values (CSV) or JavaScript Object Notation (JSON)-formatted files, the location and classification of sensitive data may already be known. In this case, the protection of those columns or fields can occur programmatically, with, for example, a labeling engine that assigns visibility labels/cell level security to those fields. With unstructured data, the location, count, and classification of sensitive data becomes much more difficult. Data discovery, where sensitive data can be identified and located, becomes an important first step in data protection.

Externalized data security does not need to be expensive. For example, basic data redaction can be performed at extraction, transformation, and loading (ETL) time with a custom user defined function (UDF) that would be executed by applications like Apache Hive, Cloudera Impala, or Apache Pig, and then triggered as a step in the workflow managed by Apache Falcon. But commercial and well-established database audit and protection (DAP) tools, such as IBM InfoSphere Guardium, frequently speak to Hadoop and offer advanced security features such as data discovery.

Strengths and Weaknesses of the Current State of Hadoop Data-Centric Security

Besides being able to externalize security controls, data encryption is becoming a commodity. The Cloudera Hadoop distribution and most of the proprietary security add-ons for Hadoop have recognized that data in Hadoop must be protected both at rest and in transit between Data Nodes and have made data encryption part of their products. Dedicated data encryption solutions for Hadoop, such as Vormetric, are now entering the market and aim to provide authorization in depth in the future.

Hadoop data security currently addresses issues relevant to big data processing. For example, Hadoop allows storage of data whose structure has not yet been discovered. At a later time, layers of transformation can be added to make it viable for various use cases, depending on the tenant. This causes a shift from an ETL paradigm to an extract-load-transform (ELT) paradigm. Data management tools x-ray the ELT process and commonly address data lineage, in addition to log and audit sprawl.

On the other hand, the current approaches of Hadoop data-centric security have these weaknesses:

- Hadoop data security is either fragmented or proprietary. If a customer uses mostly OSS (Open Source Software) for their Hadoop platform, they will find that Hadoop security is fragmented. It improves somewhat when being limited to HBase or going for a proprietary harness (such as Zettaset) or proprietary security add-ons (such as the Protegrity Big Data Protector).
- Hadoop data security is limited to the core components of the Hadoop ecosystem. Hadoop security frequently supports only core components of the Hadoop ecosystem, such as HBase, HIVE and MapReduce. New components need to be followed up with new security (paradigms) that are ideally inside the component, such as HBase or Accumulo, rather than outside, as with Hive and Sentry.

CONCLUSION

The most important use of data-centric security will not likely be deployed as an additional layer of protection against hackers that manage to penetrate a protected network. Instead, it will probably be used to protect data that leaves the network for legitimate purposes.

The big problem with protecting sensitive data is not that hackers get in; it is that data gets out, and data-centric security has the potential to eliminate the problems that can result from data getting out.

Focusing on data is logical, but it is an unusual way for organizations to look at security. More often they ask "How do attackers get in, and how can I stop them?" If the threat du jour is phishing and malware, customers tend to respond with "So let's stop phishing and malware." But if the threat is SQL injection, cross-site scripting, or weak passwords, security deployments follow the threats. It demands a larger awareness and bravery to focus on the data in the heart of the data center, rather than on the perimeter. Securing data first, to provide "security from the inside out," requires a different mind-set than the ever-popular and never-ending threat/patch ping-pong. So for these use cases, firms are beginning to realize that traditional approaches will not work, and they are searching for data protection options that work regardless of environment.

AUTHOR

A. H. Kabir (a.h.kabir.qxya@statefarm.com) is a senior research analyst at State Farm Insurance Company focused on IT security optimization. He focuses on a wide range of security issues, including identity and access management, Web services security, public-key infrastructures, digital rights management, the information security organizations, and information security issues within emerging technologies. Kabir has a Master of Science in Computer Science from Wichita State University and several industry certifications, including PMP, FLMI, CSTE, ACS, ITIL, and AFSI.

Advances in Operational Risk and Threat Modeling

Gerald Beuchelt | Cory Casanave | Vijay Mehra

ABSTRACT

Understanding an adversary and their approach to conducting operations has been considered a necessity since the time of Sun Tzu. Without a basic model that clearly articulates who the adversary is, what their intentions and motivations are, and their methods and actions leading to achieving those objectives, there cannot be an effective strategy to defend oneself. This is true for domains such as traditional warfare, intelligence and counterintelligence operations, or general law enforcement. For those fields there is a significant body of knowledge that combines existing theory, deep operational insight, and frontline knowledge about how to effectively understand the adversary and develop effective countermeasures to evaluate the risk of the overall defensive posture. Recent developments in information security and mission assurance have recognized such comparable approaches for the cyber domain as well. The results are rapidly evolving specifications that model cyber adversaries and their tactics in similar ways: threat intelligence, threat actor tactics techniques and procedures (TTP), and cyber campaigns are now common when discussing information security topics. Similarly, other fields such as emergency management have also adopted some of these concepts for developing effective mitigation strategies and risk models.

While the common ancestry of threat and in traditional warfare suggests a shared conceptual model, close observation shows that there are semantic discrepancies in defining model elements resulting in non-trivial problems to develop shared situational awareness for multi-domain concerns. Without significant explanation, it becomes extremely difficult to share information between different stakeholders without confusing terms and definitions. This paper examines a project undertaken by the member firms of the Object Management Group (OMG) to develop a conceptual model that captures the high-level elements commonly found in explicit or implicit threat and risk models. The goal is to create a specification that enables semantic interoperability between existing models and protocols.

INTRODUCTION

Being able to understand an adversary, their intentions, strategy, tactics, and specific tools is a necessary prerequisite for developing and implementing suitable strategies for countering them. This age-old truism is understood by military strategists from all times and societies, beginning with Sun Tzu, Caesar, and von Clausewitz through the development of a net-centric warfare doctrine. Without a sufficient understanding of the adversary's goals and intentions, as well as their capabilities, any plan for countering the threat they pose has a high risk of failure. The desire of commanders in battle to understand the disposition of enemy, friendly, and allied forces is reflected in the long tradition of utilizing all-sources intelligence to develop a comprehensive mental model of the current situation.

Having the capability to share the situational awareness with allies and friends is a potentially significant force multiplier.

What is true for military applications is starting to become much more pertinent for other applications in today's highly connected world as well: The lack of a comprehensive network of international authorities that can enact and enforce a shared system of policies governing the interactions of entities from different regulatory regimes poses a clear and present danger for governmental agencies chartered to protect the homeland or enforce local regulations.

But it also presents private entities across the world with a mounting challenge. Since there is no regional or global policeman "walking the beat" — i.e., the entire world — corporations and individuals are often in a situation where they cannot rely on governmental support for identifying threats, developing an understanding of their risks, and ultimately for defending themselves against potential adversaries. This has certainly shown in the cyber domain, but is also increasingly true for other threat domains such as epidemics, natural disasters, political unrest, and physical threats, both at home and abroad.

There are numerous tools, protocols, and standards in use today to allow a meaningful representation of this emerging threat landscape. However, these are often deeply rooted in their respective communities where they were developed, leading to the use of specialized vernacular and channels of communication and to a semantic disconnect between stakeholders from different communities. (It is worth noting that a similar problem existed for communications between different law enforcement communities across the United States and abroad. The Department of Justice (DoJ) with substantial support from the Department of Homeland Security (DHS) developed a unified National Information Exchange Model (NIEM), which allows the expression of law enforcement relevant information through a standardized XML framework. NIEM was subsequently expanded to cover non-law enforcement information domains.) In addition, some communities have developed more than one way of expressing threat or risk information; for example, the cyber threat domain has more than 50 different ways of expressing certain types of threats. This proliferation leads to a significant interoperability problem:

A. Currently, terms that are common across different threat domains and implementations are not semantically deconflicted (harmonized); e.g., the word "domain" may be used in a cyber context like an Internet DNS Domain, but also in the sense of Cross Domain Solutions in information assurance. NIEM also defines domains, which are closely aligned with specialized communities of interest. Finally, net-centric warfare differentiates between cognitive, physical, and other domains.

B. Without a common semantic layer, this deconfliction process is actually a non-linear problem. Every time a new stakeholder community or protocol is added, interoperability mappings to all existing participants may need to be created. With a growing number of participating entities, this leads to an ever larger number of mappings going forward.

C. Finally, it is not only the terms which sometimes overlap or are in conflict, but the specific data structures specific to the solutions and technologies in each community are not necessarily compatible — either syntactically, semantically, or both.

With this in mind, we developed a standard specification process at OMG to develop a conceptual model for operational risks and threats. The basic idea behind this initiative is to create a semantic interoperability framework that enables a meaningful exchange between different stakeholders, independent of a specific protocol, vocabulary, or threat domain. Once this is complete, the conceptual model and associated mappings will provide the necessary semantic interoperability layer for a cross-community, cross-stakeholder expression and exchange of information. A Request for Proposal (RFP) has been issued by the OMG for submitting a specification by February 2015 that can address these issues. This specifications calls

for the creation of a conceptual model for expressing threats and risks, and requires documenting this model in machine-readable form with a number of pre-defined mappings. Once complete, it will be possible to generate mappings from one framework to another by creating semantic maps to the conceptual model.

It is important to point out that the conceptual model does not aim to become an "uber model" for everything related to threats and risks. The central idea is to allow community-specific models and protocols to continue developing and be deployed independently, but maintain mappings to the conceptual model. Only major revisions of core concepts will likely require significant changes to the existing mappings.

The remainder of this paper discusses the specific approach that we are taking.

CONCEPTUAL MODELING

The foundation of this effort is a "conceptual model" that will be used as a pivot point between the many risk- and threat-related schema, exchange formats, APIs, products, and technologies. The operational risk and threat model will be informed by and mapped between many established and evolving domain and technology specific data representations — each of which has its own structure, syntax, and vocabulary for the same or related risk and threat concepts. It is not the intent of this effort to create yet another data format, but to federate those that exit. Implementations of this standard will provide for both translation of information between formats as well as federation of information for advanced assessment and analytics. The conceptual model will be expressed in the OMG Unified Modeling Language (UML).

In the OMG model hierarchy (OMG, 2014) conceptual models are not meta-models (models about model), strictly speaking, but instead highly abstracted business domain models that discuss real world entities and their relationship to each other. In this form, they cannot easily be reduced to physical models (e.g., XML schemas or waveforms), but instead need to be specialized by more detailed low-level logical models.

There is an interesting relationship to the DIKW pyramid, depicted in Figure 1, as developed by C. Zins and others:

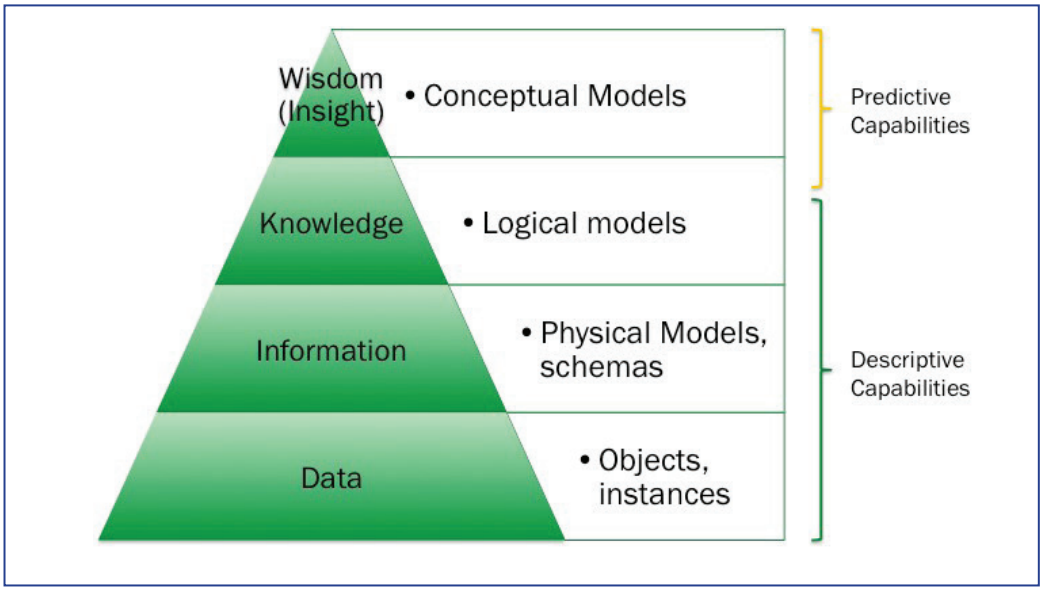

FIGURE 1: DIKW PYRAMID (ZINS, 2008)

Zins differentiates between Data, Information, Knowledge, and Wisdom. Throughout this hierarchy the level of abstraction increases from concrete objects and instances to more abstract representations. This hierarchy maps fairly cleanly to information models in the following sense:

- Data is similar to actual instances.
- Information corresponds to a first level of abstraction found in concrete models such as XML and database schemas, JSON structures, and similar ways of organizing data.
- Higher levels of abstraction such as UML that remove the ties to specific implementation technology can be seen as Knowledge in the Zins context.
- A conceptual model transitions from more tangible attributes and aspects and focuses on the relationships and qualities of the subject or domain it is representing.

While data and lower levels of abstractions are critical for implementing systems, higher-level models, such as logical and conceptual models, have a better capability to not only describe the underlying systems, but also to engage in interpretation and aggregation, and to support predictive activities.

RISK AND THREAT MODELS

Explicit threat and risk models have been available for some time in the software industry: earlier examples include the STRIDE and DREAD models developed by Microsoft in the early 2000s to ensure a secure software development process. Recently, MITRE published the STIX language that builds on earlier capabilities to describe "cyber observable" through the CyBox language. Other organizations such as the Intelligence Community, the military, population health professionals, and law enforcement have used an implicit approach for threat modeling that relies on the experience and knowledge of the respective analysts.

In addition, a number of other communities have implicitly made assumptions about threats and risks when designing standards: the OASIS Common Alerting Protocol (CAP) and more generally the OASIS Emergency Data eXchange Language (EDXL) identifies a number of man-made and natural disasters and general courses of action, and provides mechanisms to identify targets/victims and responders. In another example, NIEM provides a vast library of classes for law enforcement and other government entities, including suspects/threat actors, victims, classes of threats, etc.

Faced with a tactical need to bridge or normalize the information in any two data structures or systems, it is tempting to manually develop a bridge between those specific structures and technologies, resulting in a 1-to-1 mapping. However, when the problem is considered as an interrelated system of systems, 1-to-1 mappings between all endpoints is not scalable, because:

- there are too many, requiring hundreds to thousands of point-point mappings would be required ($N*(N-1) \sim O(N^2)$);
- the cost and time to execute is phenomenal;
- emergency integration of a new schema is impractical;
- different interpretations in each mapping make the end result error prone and unreliable;
- as schema change or are used differently, the set of mappings is not maintainable; and
- the introduction of new technologies becomes impractical and stifles change, significantly reducing the agility expected of our defensive/offensive capabilities to adapt/lead in a rapidly evolving threat landscape.

DEVELOPING A SEMANTIC INTEROPERABILITY FRAMEWORK FOR THREAT AND RISK

To address the concerns for interoperability between different representations of threat and risk, the OMG initiated a project to develop a conceptual threat and risk model. The goal for this project is not to create yet another threat model that would directly compete with the existing successful — albeit insular — solutions, but instead to identify the core concepts needed to bridge these. In order to achieve this goal, the initial focus is not on community-specific needs and requirements (such as the ability to represent MD5 file hashes), but instead to develop the necessary concepts common to most threat and risk models used across different communities. As the model evolves, and more communities become engaged, we intend to work with these communities to further specialize this model to meet their unique requirements, while maintaining the model integrity and core interoperability.

Figure 2 roughly characterizes the current scope for this project:

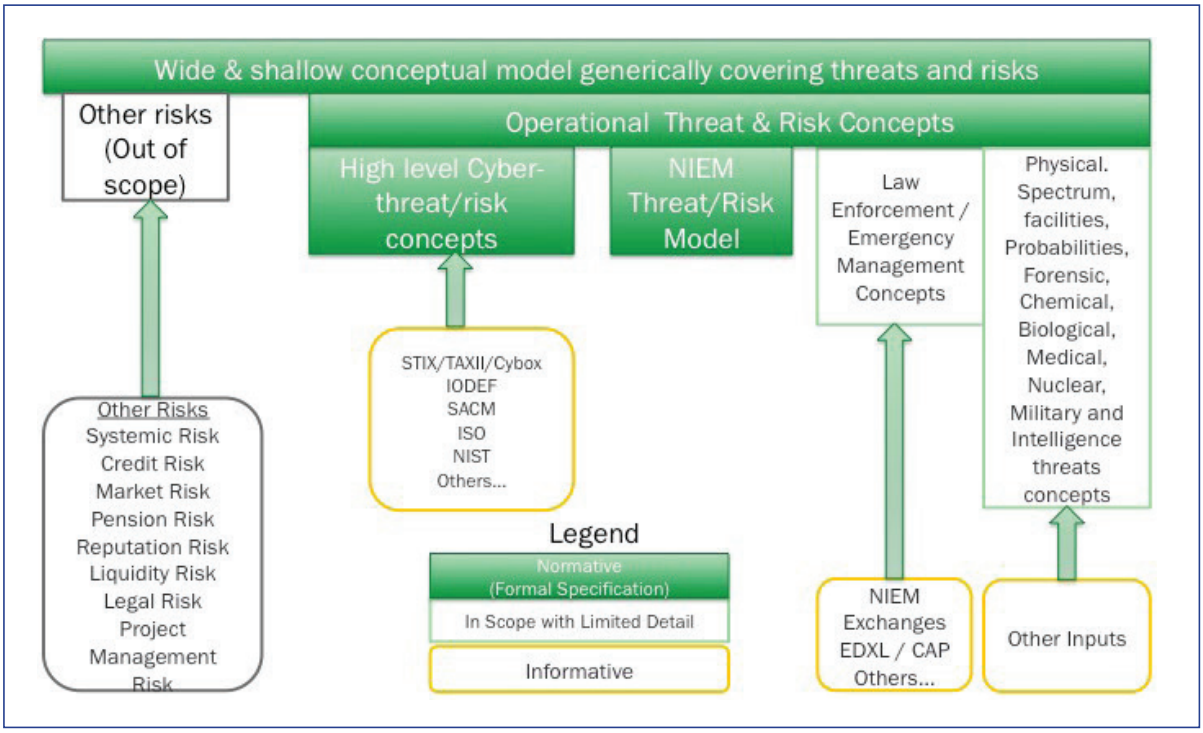

FIGURE 2: CONCEPTUAL THREAT AND RISK MODEL

A. We are building a shallow but broad conceptual model capable of representing threats and risks from a very large variety of threat domains and communities of interest, focusing on operational threats. Non-operational threats (such as systemic, market, credit, etc.) are not in scope.

B. Based on early community interest, we are including a high-level characterization of cyber threats that will integrate with STIX and other cyber threat models.

C. In addition, we will include a mapping process to allow bridging to NIEM, with a special focus on law enforcement.

D. Finally, we will incorporate (to some extent) other threat domains such as physical threats, electromagnetic spectrum, CBRN, military, and other.

Pivoting Through the Conceptual Model

With a conceptual model, it becomes possible to develop mapping mechanisms between different communities of interest and their protocols and standards more quickly and consistently.

For each physical or logical model (whichever is available), a map is generated that allows identifying elements in the more concrete model with their respective counterparts in the conceptual model. This mapping will, in most instances, not be fully faithful: for each specific model, there will be elements that have no counterpart in the conceptual model. This is not a design flaw; rather a feature that allows a semantic interoperability that can focus on the most important aspects of threats that are of interest across communities and domains.

With the ability to map directly and in a semantically consistent manner between the concrete models and the conceptual model, it becomes possible to derive the actual mappings between concrete models from their relationship to the abstract model. Since this work is being performed in a formal modeling framework using UML, the entire process of deriving specific mappings between two protocols can be largely automated and only requires minimal human intervention, primarily to verify the correctness and quality control.

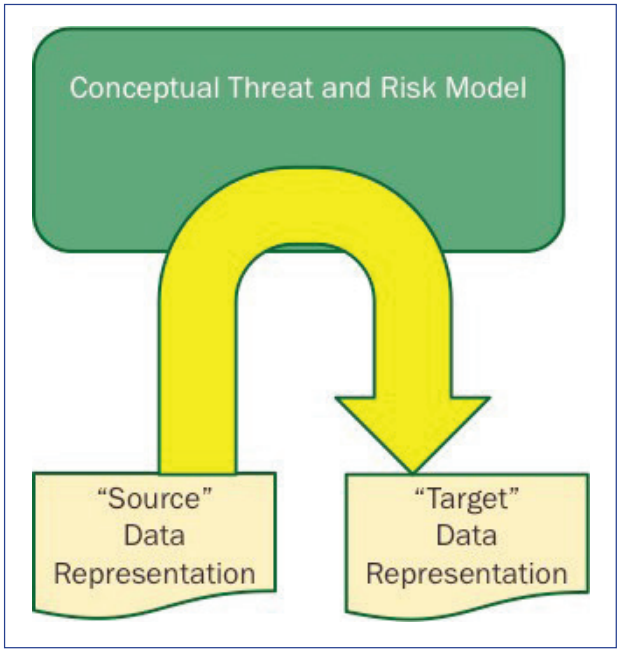

FIGURE 3: SOURCE AND TARGET DATA REPRESENTATIONS

Novel Approaches

While this work is still undergoing research and development, we have already identified a number of relatively new approaches that are worth highlighting:

- **Inclusion of inadvertent actors and natural hazards:** Existing cyber threat models and other communities (such as the Intelligence community) have a somewhat narrow definition of threats. In most cases such threats are seen as originating with a consciously acting threat actor that aims to harm a particular asset. The threat is explicitly or implicitly identified according to its capability and intent. This approach does not account for inadvertent actors (such as careless users or operators), natural disasters, epidemics, system malfunctions, etc. It is critical to include such concepts in a model that aims to address an "all hazards" environment.

- **Goals and desirability of future situations/symmetry of attackers and defenders:** In traditional approaches, the attacker (or the natural disaster) is always a threat to the defenders assets. The assumption is that the attack process aims to exploit vulnerabilities in the asset protection leading to risky situations. This "defender-only" view is too myopic for a comprehensive treatment and assessment of the situation: the threat for the defender is also an opportunity for the attacker to achieve their goals. But — on the other hand — a successful defense is a risk for the attacker and an opportunity for the defender to be successful in their goal to defend the asset. In fact, the defender may even implement an offensive plan to identify the attacker and either eliminate their capabilities or pursue other objective (such as involving law enforcement).

- **Actor capabilities:** When we eliminate the static "threat actor" and defender roles, we introduced the concepts of goals and plans above. As such, any actor may have conscious plans to pursue their objectives. However, in evaluating the chance for success (being a risk or opportunity, depending on your intentions), the general capabilities of each actor are significantly more important than specific tactics or roles.

Components of a Conceptual Modeling Approach

In order to federate information from or map between different existing data structures, we need the following specific set of assets:

- **Precise stakeholder-focused definitions of the concepts in the domain, such as "threat," "incident," or "vulnerability."** These concepts include the properties of and relationships between entities relevant to that domain. When expressed precisely, these definitions become the conceptual model.

- **Definitions of the data structures for the various data structures, schema, and other structured, technology-specific schema.** Examples include XML and SQL schema. In order to bring everything together into a workable form, these schema definitions are also represented as models. The process for bringing a schema into a model can be fully automated.

- **Mappings between each of the schema (represented as models) and the conceptual model — preferably two-way mappings.** Since both the concepts and the schema are models, the mappings can also be models. In many cases these mappings are context specific — so we have to understand the context that is relevant to a domain or problem area.

- **A technology implementation that is able to understand the models, mappings, and map data between formats or combine data from multiple formats.** This is performed by mapping through the conceptual model.

The conceptual model for threats and risks is underway, as are the model representations of existing schema such as STIX and NIEM (NOEM already has a standard UML-based model representation in NIEM-UML). The process is now underway to build out these models and the mappings.

Example Mapping: Incident

Figure 4 depicts an example of how a conceptual incident can be mapped to a NIEM incident and a STIX indicator.

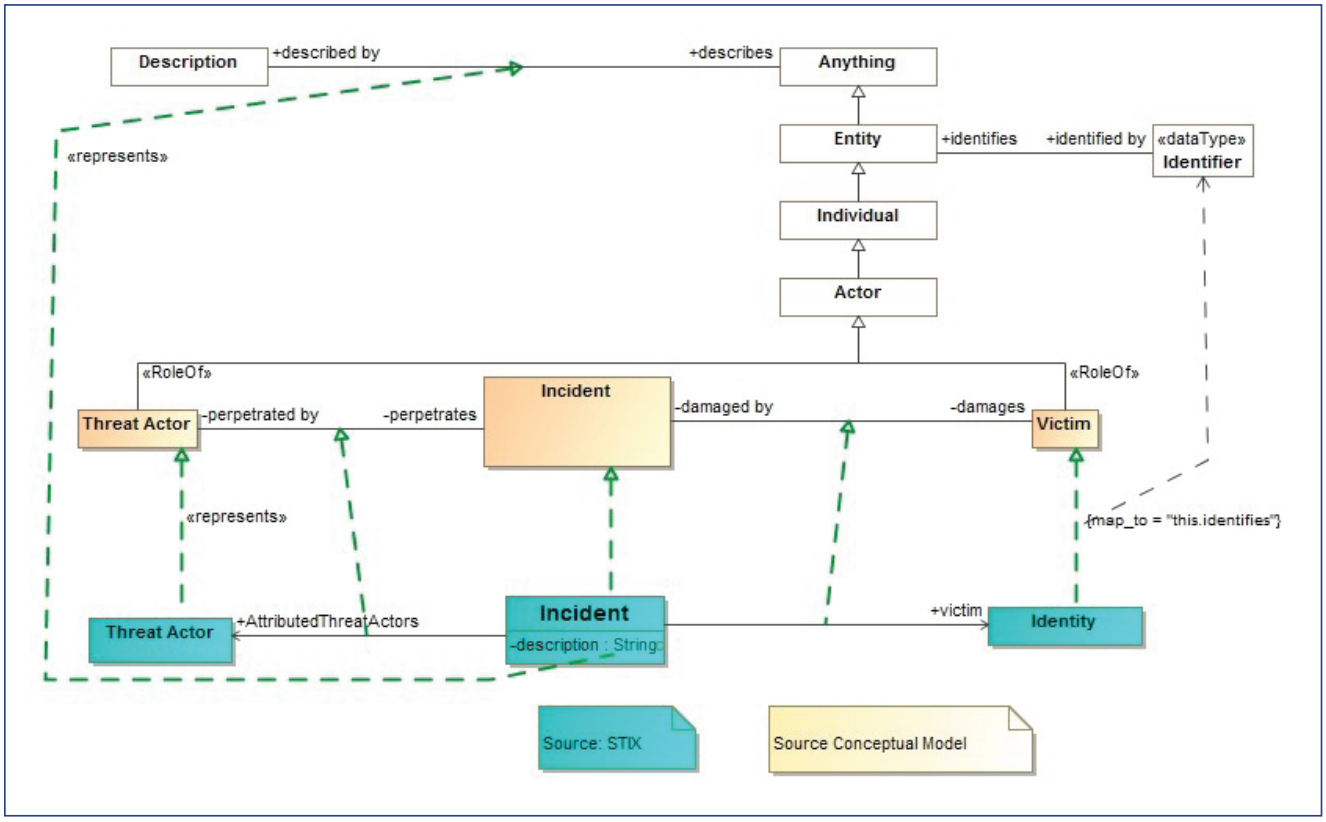

FIGURE 4: STIX INCIDENT MAPPING

The boxes on the top (in white or beige) are defined in the conceptual model using UML. The boxes define classes of items in the domain and the lines relationships between those classes. Both the boxes and lines are "concepts." The boxes on the bottom represent the STIX schema, as a UML representation of the high-level elements in STIX. The green dashed lines show a correspondence between a STIX concept and a concept in the conceptual model.

While Figure 4 depicts how STIX is related to the conceptual model (it does not provide the other end for any federation), in Figure 5 we add a NIEM mapping for a few of the same concepts:

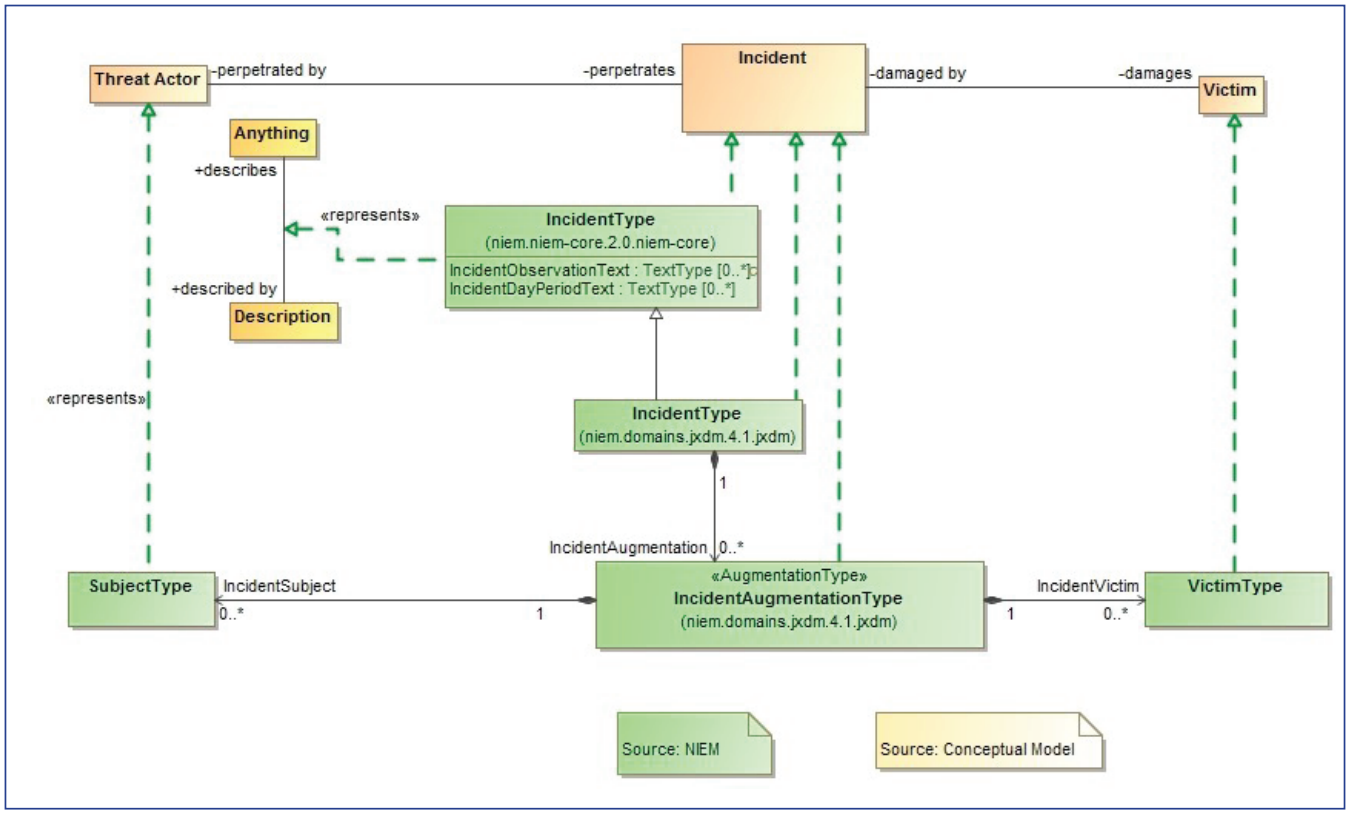

FIGURE 5: NIEM INCIDENT MAPPING

In reviewing both mappings we can then see how information could flow from one to the other.

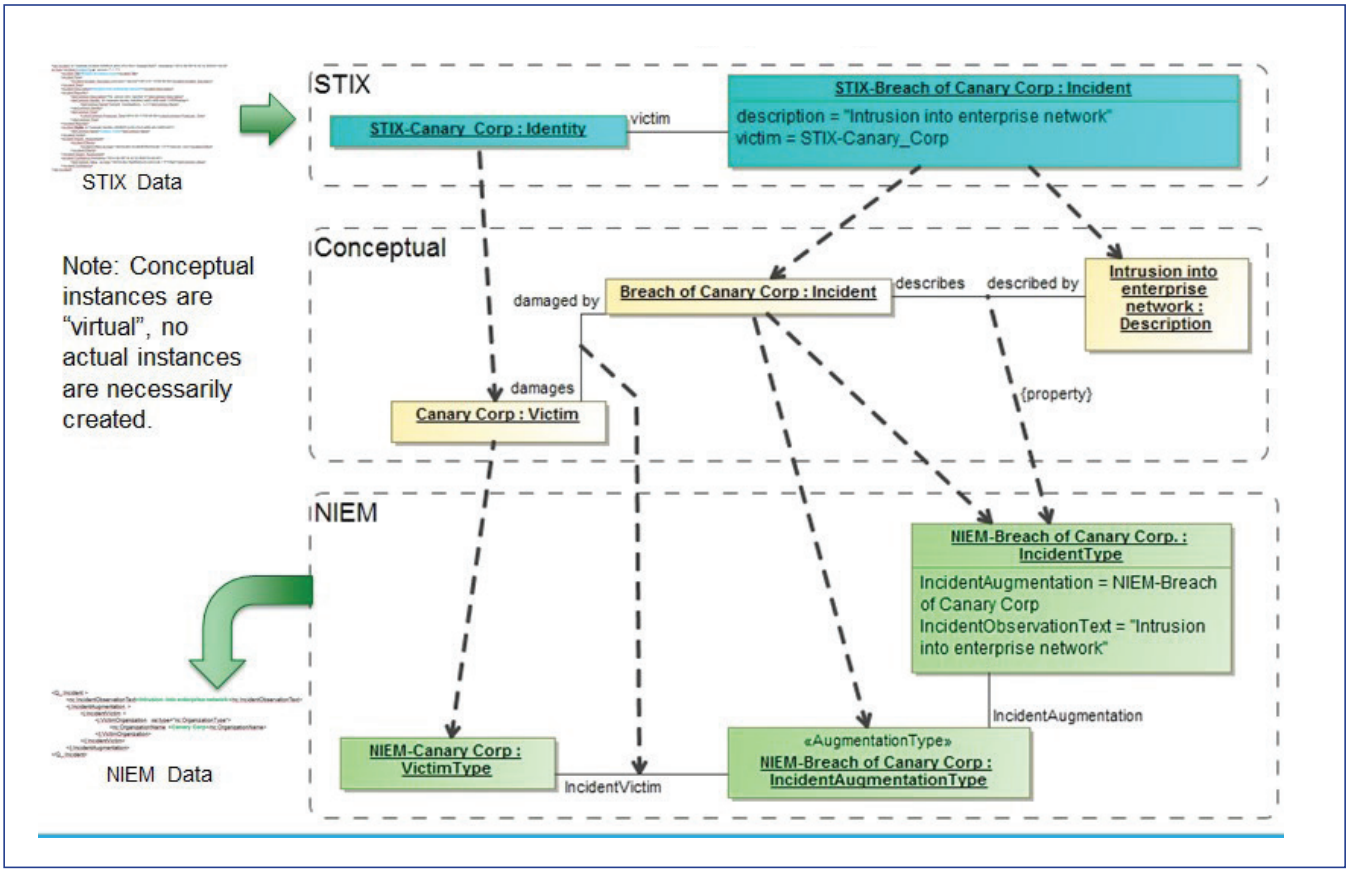

FIGURE 6: SAMPLE INCIDENT — CANARY CORP.

Figure 6 shows a simple instance of STIX data depicting "Canary Corp." as the victim and "Intrusion into the enterprise network" as the incident. This same data can then map through the conceptual model to a NIEM incident, perhaps one that could be reported to police. Note that on both ends there may be more detail; what we have been concerned with is the data that flows between these communities.

Example Use Case: Large Company Security Operations Center

As an example of how the model may be operationalized, consider a corporate security operations center: for large corporations there are multiple functions that monitor security from a physical and information security perspective, which are often not fully integrated. Using the conceptual model, we can now start to identify data sources that are relevant to both the physical and information security functions. Such data sources can now be normalized and made available for all stakeholders in the formats that are required for their respective systems. In addition, a central dashboard or Governance, Risk Management, and Compliance (GRC) system could aggregate the data and inform executive management of the current security posture and threats to the company.

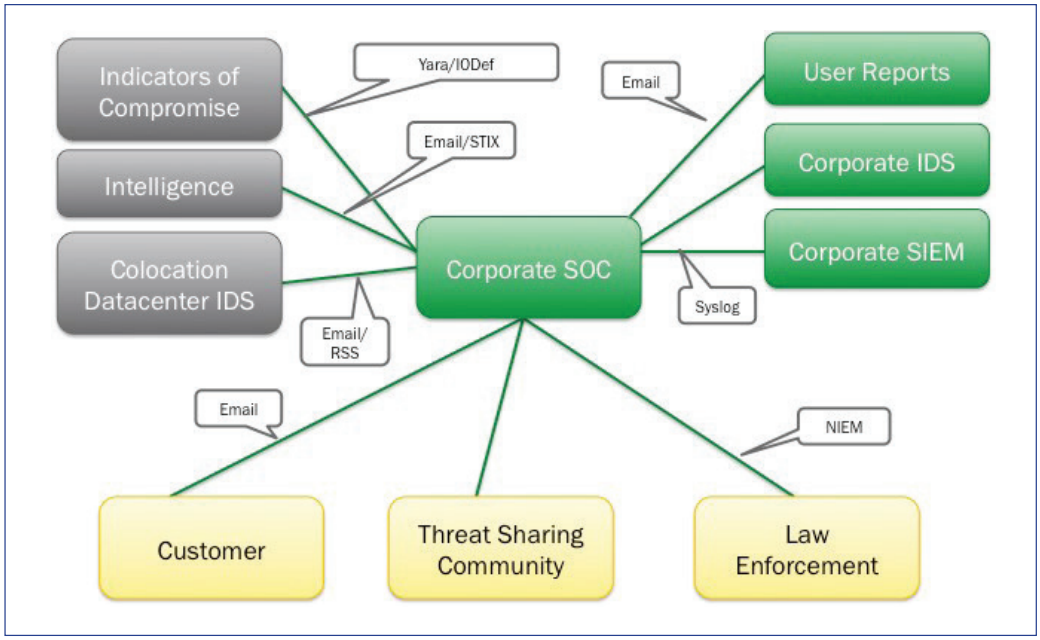

FIGURE 7: SECURITY OPERATIONS CENTER

SUMMARY

The work on developing the conceptual model for threats is currently progressing. The core concepts required to move this effort forward are understood, and the next steps will include a refinement of the mappings to other relevant standards. The submission team has collected a rich set of use cases and is currently in the process of formalizing their release.

Members of the community have also suggested additional use cases beyond the data aggregation, analytics, and exchange: the RFP includes a suggestion to provide the model and its entities with a mechanism to identify parameters for elements in the model and make it suitable for simulation methods such as Monte-Carlo. If this can be achieved the model may be useful to test strategies and plans for their suitability to achieve the stated goals. Another suggestion includes the incorporation of non-operational threats and risks.

REFERENCES CITED

Barnum, S. (2010, September/October). The Balance of secure development and secure operations in the software security equation. *The Journal of Defense Software Engineering*

Barnum, S. (2014, February). Standardizing cyber threat intelligence information with the structured threat information eXpression. *The MITRE Corporation*

Hernan, S. (2006, November). Uncover Security Design Flaws Using The STRIDE Approach. *MSDN Magazine*. Retrieved from http://msdn.microsoft.com/en-us/magazine/cc163519.aspx

MSDN Resource File (2003, November). Threat model your security risks. *MSDN Magazine*. Retrieved from http://msdn.microsoft.com/en-us/magazine/cc164068.aspx

OASIS Standard (2010, July). Common alerting protocol 1.2. Retrieved from http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf

Object Management Group (2014, June). Object management group model driven architecture (MDA) — MDA Guide rev 2.0. Retrieved from http://www.omg.org/cgi-bin/doc?ormsc/14-06-01

Zins, C. (2007). Conceptual approaches for defining data, information, and knowledge. Journal of the American Society for Information Science and Technology 58 (4), doi:10.1002/asi.20508

AUTHORS

Gerald Beuchelt (gbeuchelt@demandware.com) is the chief information officer for Demandware and responsible for leading the development, implementation and management of the corporate information security governance and management framework. Beuchelt is the recipient of many awards, including the 2011 MITRE Program Recognition Award of Distinction of his work on "Enabling Healthcare Transformation," sponsored by the Department of Health and Human Services (HHS). In 2005 he received the Sun Microsystem's Chairman's Award for innovation. In 1997 he received his Master of Science/Diploma in Theoretical Physics from Cologne University, Germany. Beuchelt is also serving as a voluntary member of the Information Systems Advisory Board for the Town of Burlington, MA, and is an elected member of Burlington's Town Meeting.

Cory Casanave (cory-c@modeldriven.com) is a recognized expert and thought leader for actionable agile architectures at all levels — making enterprise, business, process, information, and services architectures meet business needs while directly supporting executable IT solutions using Model Driven Architecture (MDA). Casanave's focus is broad-based information sharing and federation, and he is the chief architect of the community initiative and standards effort to address the sharing and analytics of cross-domain threat and risk information sharing, a crucial capability for government and industry. Casanave is a member of the Object Management Group (OMG) board of directors and chairs the OMG's Open Government Workgroup. In support of government/industry collaboration, Casanave helped the U.S. National Information Exchange Model (NIEM) program office create the new standard for model-driven information exchange data — NIEM-UML. In support of information sharing and enterprise integration, Casanave was also one of the authors of "SoaML" — the modeling standard for SOA.

Vijay Mehra (vijaymehra@gmail.com) is a results-oriented professional with more than 20 years of experience serving in management and technical leadership positions, delivering complex mission solutions. His areas of experience include IT strategy and growth planning, large-scale IT systems development and implementation, standards development, and program/project management, with mission focus on justice and public safety. Over the last 12 years, Mehra has primarily focused on topic areas related to information interoperability. He is active in the standards development community, and has led or supported many initiatives around the development and adoption of technical/functional standards, reference architectures, and information interoperability strategies. Most recently, he has been working closely with the Object Management Group to develop core concepts and standards-based models for the Threat and Risk Information Sharing Initiative. This initiative recognizes the need for focusing on the broader threat spectrum that enables a unified view of different types of threats (cyber, physical, environmental, etc.) leading to better integrated response planning and optimal use of shared resources.

The Need for a Paradigm Shift Toward Cybersecurity in Journalism

Roland Taylor

ABSTRACT

The press is often considered the shining light and voice of the potential fourth branch of our democracy, the people. In this role it is critical the press provides protection and anonymity to those brave enough to come forward and provide information.

In the current virtual global infrastructure of Internet and communications, both journalist communications and data are at risk. The threats range from government to criminal and include both domestic and foreign. This paper addresses the need for a holistic and multidisciplinary approach in journalism and for the supporting academic community to provide journalists with more cybersecurity education and tools.

INTRODUCTION

In the United States freedom of the press plays an important role in shining a public light on crime and corruption within our society and government. One of the fundamentals of freedom of the press is the protection of sources. Without the protection of anonymity, sources would be fearful of reprisals, thereby deterring them from coming forward with vital information of public interest.

Examples and Challenges

The iconic example of protection of a confidential source occurred in 1972 when Bob Woodward and Carl Bernstein of *The Washington Post* reported on the Watergate scandal, which resulted in the resignation of U.S. President Richard Nixon (Woodward, 2005). In another more recent example, reporter Judith Miller, formerly with *The New York Times*, was jailed in 2004 for contempt of court for refusing to testify before a federal grand jury investigating a leak revealing Valerie Plame as a CIA officer (Liptak & Newman, 2005).

As technology has progressed so have the legal methods and tactics used by governmental agencies in obtaining reporters' information and identifying their sources. In 2013, it was revealed in a federal affidavit that a federal judge authorized a search warrant (allegedly approved by U.S. Attorney General Eric Holder) for the personal emails of Fox News reporter James Rosen, and named him as a "co-conspirator" in a leak investigation of classified information about North Korea. That same year the U.S. Justice Department advised the Associated Press (AP) that months prior it had subpoenaed the phone records of several AP journalists, eventually capturing all records of several main phone lines.

The Shift in Media Consumption

The journalism community, over the last decade, has adapted to an overwhelming shift in how society consumes news media via the Internet and personal electronic devices. The consumer shift to electronic and social media has fundamentally transformed the way society gets its information and has financially devastated the print news media. This shift has resulted in the closures of many legacy newspapers nationwide. The academic community has adjusted its journalism curriculum with the addition of electronic multimedia publishing skills focused on graphics, video, and photo editing. Social media and blogs have changed consumer expectation of

reporting; consumers evolved from expecting information on the day following an event, to expecting information within hours and minutes (real time). The news industry's information technology (IT) download speed and security was a lower priority until the more recent foreign cyber attacks on some major news organizations.

The lack of a sound cybersecurity infrastructure within the field of journalism discourages informants from coming forward and raises concerns that secrets may not be safe with journalists, according to Christopher Soghoian, PhD, a principal technologist and a senior policy analyst with the American Civil Liberties Union (ACLU) (Soghoian, 2011). In the future, the focus within journalism should be to create a culture of cybersecurity awareness and information protection. The range of risk of exposure varies greatly from the local big story to national security coverage or assignments in international high-risk locations. The consequences of a weak cybersecurity infrastructure can range from simply losing the scoop on an important story to a high-value source losing his or her life. There is no one-size-fits-all security method or tool. Journalists require education in identifying risk and threat modeling in order to better apply the most appropriate combinations of operational cybersecurity practices and technologies.

Tools and Resources Available to Journalists

Many journalists gain their limited cybersecurity tools and techniques from various online sources connected with other press professional and political activist or "hacktivist" communities requiring anonymity. For example *The Guardian's* Glenn Greenwald, who broke the Edward Snowden story, acknowledged in a 2013 interview with the *Huffington Post* that Snowden had to provide step-by-step instructions and video on how to secure their communications, which delayed the release of the information (Calderone, 2013). Many of the major news media companies provide computers and virtual private networks (VPNs), which by policy could restrict new program installation by reporters to protect their systems from cyber attacks. This approach may force reporters to use personal computers and smart phones to install open source security programs, thereby creating another set of security and personal safety issues.

Many of the open source programs used in the Internet freedom community were not designed to be user-friendly programs, but as tools to be used by experienced IT programmers and professionals. A reporter using one or two of these open-access programs, without a broader understanding of the risks and threats, may not provide the required protection of anonymity/linkage, encryption, or operational stealth to protect the source's identity or information received. In most cases, it is the source who requires the security tools and few reporters are experienced enough to educate the source on how to install or use these programs.

An example of the insufficiency of current journalistic practices is a journalist using only a tool such as a Tor browser — an anonymity tool that routes their Internet traffic over the World Wide Web. The Tor network serves little purpose if users blindly think they are anonymous on their own personal computer while logging into their personal Facebook accounts. Selecting any browser on one's computer, other than Tor, provides no protection. Using encryption tools that only block the body of an email and not the metadata still allows a foreign government service to locate the source's location, which may be all they need to compromise the source. Properly using anonymity tools on a computer while the person's cell phone location traceable Short Message Service (SMS) is enabled also contradicts the methodology of anonymity. Unlike commercial Internet security or commercial, anti-virus for-profit software solutions, most open-source, non-profit tools are single focused in purpose.

Some progress in awareness within the journalism community has begun. A December 2013 press release of the Freedom of the Press Foundation's Executive Director Trevor Timm announced that they planned to make digital security for journalists their major initiative in 2014. Timm stated, "We not only want to support these encryption tools, but train journalists how to use them" (Timm, 2013). The Freedom of Press Foundation has furthered the development of the SecureDrop tool that was

originally the project of the late hacktivist, Aaron Swartz (then called DeadDrop), to allow safe ways to communicate with sources. Both the Freedom of Press Foundation and the National Press Foundation have added cybersecurity-related pages and free webinars on their websites.

SUMMARY

Creating a safe channel of communication is critical. Many information security professionals would argue that downloading the Tor browser's bundle appropriate for a particular browser is the first step to anonymity. Mozilla's Firefox browser and their email application Thunderbird can make emailing safer when the Enigmail add-on is also installed. Enigmail signs and encrypts emails sent from Thunderbird. For instant messaging, journalists should consider using an all-in-one messenger like Pidgin; they may also consider using the Off the Record (OTR) plug-in for Pidgin. Basically, the OTR plug-in provides encryption, authentication, and secrecy to all the services that are used through Pidgin. It is also important not to use personal emails or information to establish an anonymous account nor share data or communicate with your personal accounts.

Until more formal training is provided, journalists should begin to explore and experiment with the open-source encryption and anonymity tools. Learning to strengthen the computer's data security and how to properly delete and overwrite data is an important element in preventing forensic recovery. The typical user's learning curve does not allow waiting until the journalists or their sources need it. First, journalists should explore tools to secure data on their computers with software like TrueCrypt that encodes and password protects files, and file deletion tools such as CCleaner that make it more difficult to recover seized files. CCleaner achieves this protection by overwriting data after file deletion.

The journalism community needs to make a paradigm shift toward cybersecurity technology and education. The key thing to remember is that nothing is 100 percent secure. However, by applying layers of protective tools and becoming personally more aware of potential risks and threats, operational and cybersecurity capabilities grow with practice. Embracing these cybersecurity tools and tactics in addition to pushing for the required "paradigm shift" enhances the safety of journalists in high-risk locations where there is no freedom of the press protection. Additionally, this shift in thinking further increases the comfort level of informants, allowing them to come forward with a reduced fear of reprisal.

REFERENCES CITED

Calderone, M. (2013, June 10). How Glenn Greenwald Began Communicating with NSA Whistleblower Edward Snowden. The HuffingtonPost.com. Retrieved from http://www.huffingtonpost.com/2013/06/10/edward-snowden-glenn-greenwald_n_3416978.html

Liptak, A. & Newman, M. (2005, July 6). New York Times Reporter Jailed for Keeping Source Secret. The New York Times. Retrieved from http://www.nytimes.com/2005/07/06/politics/06cnd-leak.html?pagewanted=print

Soghoian, C. (2011, October 26). When Secrets Aren't Safe With Journalists. The New York Times. Retrieved from http://www.nytimes.com/2011/10/27/opinion/without-computer-security-sources-secrets-arent-safe-with-journalists.html?_r=0

Timm, Trevor. (2013, December 5). Freedom of the Press Foundation Launches Campaign to Support Encryption Tools for Journalists. Freedom of the Press Foundation. Retrieved from http://freedom.press/blog/2013/12/freedom-press-foundation-launches-campaign-support-encryption-tools-journalists

Woodward, B. (2005, June 20). How Mark Felt Became 'Deep Throat.' The Washington Post. Retrieved from http://www.washingtonpost.com/politics/how-mark-felt-became-deep-throat/2012/06/04/gJQAlpARIV_story.html

AUTHOR

Roland Taylor (rolandtaylor_sgt@yahoo.com), PMP, has over 30 years of progressive domestic and international experience in both business and criminal justice management. He is a guest lecturer and subject matter expert in several law enforcement technical areas. Additionally, he served as an instructor in Human Intelligence (HUMINT) tradecraft skills. Taylor has a Master of Science in Criminal Justice/Law Enforcement Administration with dual specialization in Cyber-Forensics Administration from Loyola University, New Orleans.

Is Cybersecurity Possible in Healthcare?

Sean Murphy

ABSTRACT

With the numerous data breaches in healthcare over the past several years, it almost appears unreasonable that a patient have any expectation of the privacy and security of their information. This paper explores possible solutions to the current situation and makes recommendations concerning how to implement and complement cybersecurity in healthcare. Emphasis remains on the quality of healthcare, patient safety, and access to healthcare for patients.

INTRODUCTION

"You already have zero privacy. Get over it!"

Scott McNealy, CEO, Sun Microsystems, 1999

With the numerous data breaches in health care over the last several years, it almost appears that patients having any expectation of privacy and security of their information is unreasonable. In 2012 alone, 780,000 patient records were stolen from the State of Utah Department of Health, Department of Technology server, by an Eastern European hacker. At Saint Joseph's Health System in California, the information of approximately 31,800 patients was made potentially available through basic Internet search engines for about a year because security settings on the system were set incorrectly (McNickle, 2012). Add to these more traditional cybersecurity incidents the numerous workforce (user) mistakes — losing laptops, backup tapes, and sending unencrypted e-mails — and one can legitimately question the expectation of privacy and security. Yet, the expectation is based on a legal and ethical obligation for health providers to do exactly that — protect the privacy of patient information through adequate cybersecurity.

There are several issues that complicate healthcare cybersecurity. To begin with, no healthcare organization exists to provide cybersecurity. They exist to provide healthcare. Information protection goals usually culminate with compliance. Typically, compliance is all that a healthcare organization can dream of affording. Reimbursement or revenue for healthcare is not tied to any cybersecurity efforts. Information protection is completely under relegated to overhead costs. In other industries, cybersecurity cost may be passed on to the consumer. In healthcare, where margins are already tight, cybersecurity costs are absorbed by providers. As compliance is typically the best we can hope for, security professionals shudder because they know compliance is not equal to security. Further, the governing healthcare privacy and security law — the Health Insurance Portability and Accountability Act (HIPAA) — written in 1996 and amended several times since, goes to great lengths to not prescribe solutions and only requires healthcare organizations to take reasonable actions to prevent data loss. Compliance, ineffective as it is for truly protecting information, is at best ripe for being misconstrued and variable among staff and regulators.

Coupled with the seeming vague and uncertain guidance to provide patient confidentiality, integrity, and availability, even the most basic operations in healthcare depend on liberal sharing of patient information. The sharing of this information must almost be unfettered and "need to know" can be highly open to interpretation. In fact, in a world where confidentiality, integrity, and availability are the tenets of cybersecurity, healthcare is different in that these are not equivalent concerns. Availability may be the most important of the three. Stated another way, cybersecurity professionals in

healthcare may find themselves in the uneasy position of flexing on confidentiality controls in favor of increased availability.

A third concern that influences cybersecurity in healthcare is that the value of healthcare information to hackers and unauthorized users is primarily for identity theft. The theft can be for medical identity to obtain health services and prescription medication by assuming someone's identity or health insurance credentials. The theft can also be for purely financial gain, either to sell on the black market or to use to drain or open credit accounts. The problem is that some individually identifiable information is needed in healthcare. That will not change. Financial information is also needed. That will not change. But the abundance of information that is needed currently and how it must be coupled with the patient medical record is troublesome.

The fact remains that cybersecurity in healthcare is, of course, badly needed and possible. To borrow from John F. Kennedy, we must do these things not because they are easy, but because they are hard (and patients have a right to expect it). But, in consideration of the constraints mentioned in the introduction (and others), healthcare cybersecurity must be implemented with particular attention paid to the unique issues. Cybersecurity applied to healthcare without a proper acknowledgement of the clinical environment can cause patient safety issues and, in some cases, unintentional cybersecurity vulnerabilities.

This paper will consider the healthcare environment and offer some potential solutions. As cybersecurity in healthcare can be considered a recent issue with the advent of electronic health records (EHR) over the last 5 years, more research and effort is needed to refine these solutions and develop others that protect sensitive information, yet do not impede the clinical workflow that originates from the doctor-patient relationship.

UNIQUE PATIENT IDENTIFIER

One necessary action for the feasibility of cybersecurity is for U.S. healthcare to establish a national patient identification system. Some would argue we already have one: the social security number, issued by the U.S. government. Currently, there is almost universal adoption of the social security number. So much so, that many other U.S. agencies, like the military and the Internal Revenue Service (IRS) (for individual federal tax identification), use the social security number as a de facto unique identification number. In fact, it is common for banks, colleges and universities, health insurance companies, and employers to rely on the social security number. However, this contributes to the reasons why the social security number is not the solution. The risk of losing it to an adversary (defined as anyone who does not have authorized use of the data) outweighs the reward to be gained by having one more use for a social security number.

The social security number is not the answer for healthcare, expressly because of the success of the social security number. When the U.S. government enacted the Social Security Act, and the social security number, it was not intended to be an identifier (Puckett, 2009). In fact, the Social Security Act itself does not require a person to have a social security number to live and work in the United States. However, it has become inextricably connected to many significant components and applications concerning an individual's identity. In cybersecurity, we recognize it as a best practice to refrain from having a consolidated, single target for the adversary. The advice to healthcare to also use the social security number as a unique patient identifier is unsound. Having a separate, unique patient identifier for healthcare — not tied to the social security number — would be more secure.

There are other reasons why healthcare has not adopted the social security number, starting with the fact that not every patient that presents for healthcare will have a social security number. Some will be non-citizens; although some non-citizen

residents can get social security numbers. Others will be children who were not issued a number, yet. As small a percentage as this may be, it is not a good idea to issue a social security number for the sole purpose of receiving healthcare. Again, such a social security number becomes more valuable to the adversary as it is not tied to any financial accounts or other government identities (e.g., the IRS). To further complicate matters, oddly enough, a recent study found that more than 20 million Americans (Cheddar Berk, 2010) actually have multiple social security numbers associated with their name in commercial records. In sum, the reliability of the social security number has some problems.

Given this history, it is interesting to note the reason healthcare has not developed another unique patient identifier, despite the fact that they did not favor the social security number. Because there was political opposition based on concerns for privacy, the federal government actually prohibited the U.S. Department of Health and Human Services from funding any research or demonstration projects for a unique patient identifier until "a standard could be agreed upon" by Congress (Carr, 2011). That was the rule in 1998 and it still stands.

So, in the face of very poignant concerns about using an attractive cybersecurity hacker target like the social security number and a government ban on establishing something else, healthcare providers create workarounds. To positively identify patients, they will use at least two or three patient identifiers (one of which may be a full or partial social security number). They will also use name, date of birth, sex, or address in some combination. The need to do this is not only for patient administration or billing. It is also a patient safety measure to ensure the right medicine and procedures are administered to the right patient.

This process has proven benefits in reducing medication errors and adverse events, again, as it relates to patient safety. But as a means of identifying patients from a cybersecurity perspective, the practice is almost as bad as creating a singular cybersecurity target. Instead of one data element — the social security number — there are now multiple valuable pieces of information available in every instance of the patient encounter, and some are not always needed.

A unique patient identifier used specifically for healthcare mitigates repetitive use and disclosure of all the other individual identification data elements under the current practice. It would be relevant for communication inside the organization (patient care, billing, etc.). To this point, most healthcare organizations already create a unique number for each patient called the medical record number (MRN). However, it is only understood within that organization. Patients are typically transient, visiting different healthcare settings over any given period of time. The MRN does not follow them. With the MRN, the additional data elements are still used anyway.

A unique patient identifier at the national level would also work for external communications to other healthcare organizations, health insurance companies, and government agencies like public health or Medicaid and Medicare. What has accelerated the impact (and imperative) for external communication compatibility is the widespread implementation of the electronic health record (EHR) and dozens of categories of networked medical devices enabling advances like teleradiology, telemetry, and body area networks. The American Recovery and Reinvestment Act (ARRA) of 2009 among other initiatives, provided stimulus funds earmarked for healthcare organizations which implemented an EHR before 2014. The EHR had to meet "meaningful use" criteria, which included standards for electronic data exchange and some privacy and security measures. However, the standards did not mandate a unique identifier. But through the implementations, the viability (and again, imperative) for a unique identifier comes to the forefront. Related to the privacy and security standards of the EHR, cybersecurity professionals would welcome the unique identifier so that proper controls to assure confidentiality, integrity, and availability are more feasibly protected through implementation.

The recommendation for a unique patient identifier presented here should not be interpreted as a new recommendation. The issue was raised by professional organizations starting as far back as with the Computer-based Patient Record Institute, in 1993. Since then groups like the American Society for Testing and Materials (ASTM), the American Health Information Management Association, and Health Level 7 (HL7) have generated calls to action and presented as many as 12 solutions that follow the mandate for establishing unique patient identification standards found in HIPAA (Unique Health Identifier, 1998). Rather than propose a recommendation as a new idea or a better recommendation from any previous, the purpose here is to recommend that the unique patient identifier is an idea whose time has come. Cybersecurity, information technology, and clinical processes have aligned to a point where political concerns no longer make much sense and the risk of disclosure to the adversary means harm to the patient and to the healthcare organization.

If the time has come, then there is one more hurdle that must be cleared. For the unique patient identifier to be truly effective beyond access control, patient tracking, clinical work flow, auditing, and information exchange, it must be decoupled from the other valuable identifiers for those who access it. In other words, the unique patient identifier cannot be an access point into the patient's social security number, financial information, or some other identifying data in case the adversary gains unauthorized use. That would defeat the purpose. However, those who can demonstrate a bona fide need to know (e.g., a healthcare insurance company) should be able to match the unique patient identifier with other identifying information they already have. To make this happen, a third-party organization should be established to serve as a proxy with appropriate access to an individual's information to fulfill identification matching requests.

Figure 1 illustrates a simple data flow of healthcare providers, the third-party proxy, clearinghouses, and other healthcare providers. A healthcare clearinghouse is a recognized healthcare organization subject to HIPAA law for handling protected

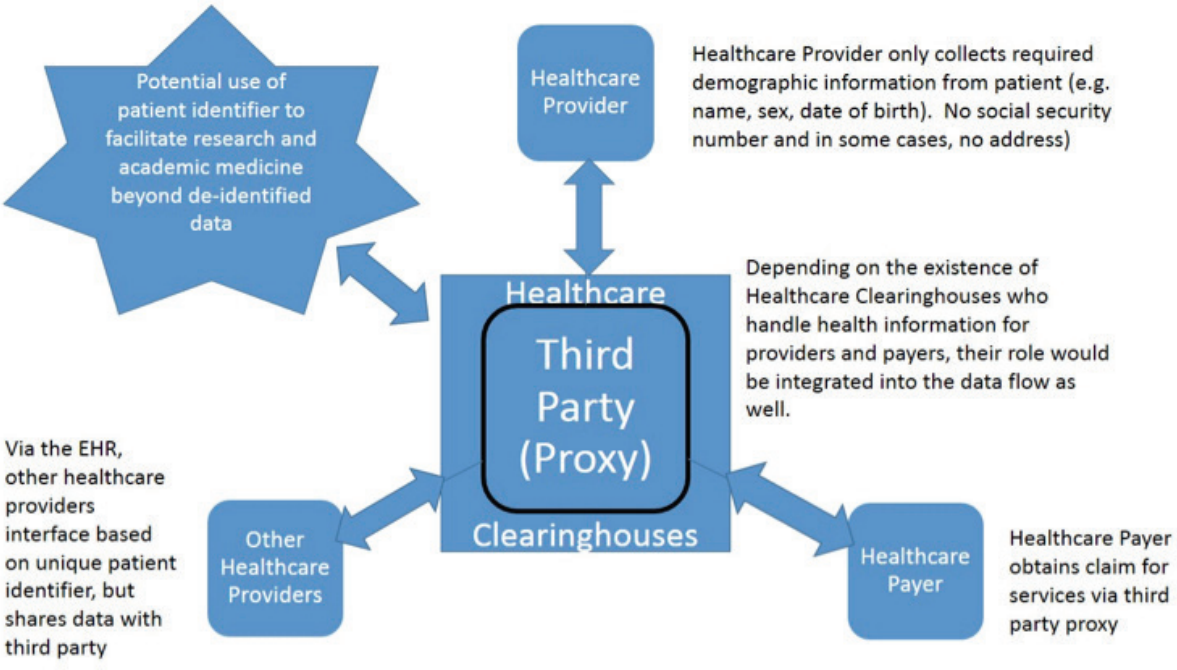

FIGURE 1: SIMPLE DATA FLOW FOR UNIQUE PATIENT IDENTIFIER THIRD-PARTY PROXY

health information. For instance, a utilization management organization that reviews tests and procedures that healthcare organizations request is a healthcare clearinghouse. The overall point of the data flow is that between the organizations that require portions of the individual's information, none of them need both the social security number and a unique patient identifier, where one exists. This would limit the impact of any data loss by any one of the data handlers.

Selecting a third party to be the proxy is a matter for further research and discussion. There are some capabilities that are necessary. First, because the unique patient identifier must be valid nationally and controlled, it is plausible the function should be performed by a federal government agency. That might point to an agency like the Social Security Administration. But since it already administers the social security numbers and the effort is in decoupling the identifiers, the Social Security Administration is probably not the best choice. Another agency that might fit the purpose is the United States Postal Service. By virtue of the agency's current oversight of programs like Medicare and Medicaid (and HIPAA itself), the U.S. Department of Health and Human Services (HHS) may be the proper proxy agency to maintain separation of an individual's identification information and health information. The added benefit of having HHS handle this is its familiarization (e.g. authorship) of the HIPAA-mandated Business Associate Agreement (BAA). The BAA is a special type of contract or obligation into which third parties must enter with the healthcare organization. In brief, the BAA outlines responsibilities each organization has with handling the protected health information.

Whoever could be the best proxy, the main criteria are adequate reach and a nation's trust to ensure availability and integrity of identification without failing to maintain confidentiality and privacy. It may very well be a process that ends up looking like the public key infrastructure process with the private sector playing a major role versus the public sector. In either case, the unique patient identifier is a solution that is needed immediately.

HEALTHCARE-FOCUSED RISK MANAGEMENT

Cybersecurity technology, starting with risk assessment, needs to be developed specific to healthcare to support medical technologies like health information exchanges and medical devices. Without question, the protection of information has introduced and evolved some extremely sophisticated and effective technologies and processes. Everything, from firewalls to anti-virus to encryption tools, has helped both businesses secure their corporate intelligence and individuals protect their home networks.

Additionally, there are dozens of information security risk assessments that exist. Highly respected organizations like the National Institute for Standards (NIST) and International Organization for Standardization (ISO) have the frameworks upon which most publically available risk assessment methodologies are based. This is not in debate. Where cybersecurity in healthcare goes wrong is in trying to apply these standards in healthcare, use the automated scanning tools, and mitigate findings without regard to the clinical workflow. This does not mean the NIST and ISO frameworks or cybersecurity tools are not applicable. It means that tailoring them to healthcare requires some additional work. Here we introduce three tailoring efforts that must be made in healthcare so that information can be protected, but that the crucial requirement of information sharing within healthcare is never impeded.

RISK ASSESSMENT FOR AVAILABILITY

How an information risk assessment is done is a process that is customized, by definition, for each healthcare organization. Even if using the NIST Risk Management Framework (RMF), each organization will prioritize the findings according to management input, for example. But beyond this, healthcare organizations must apply the risk assessment with more of an emphasis on availability than do most other industries apply for cybersecurity. As

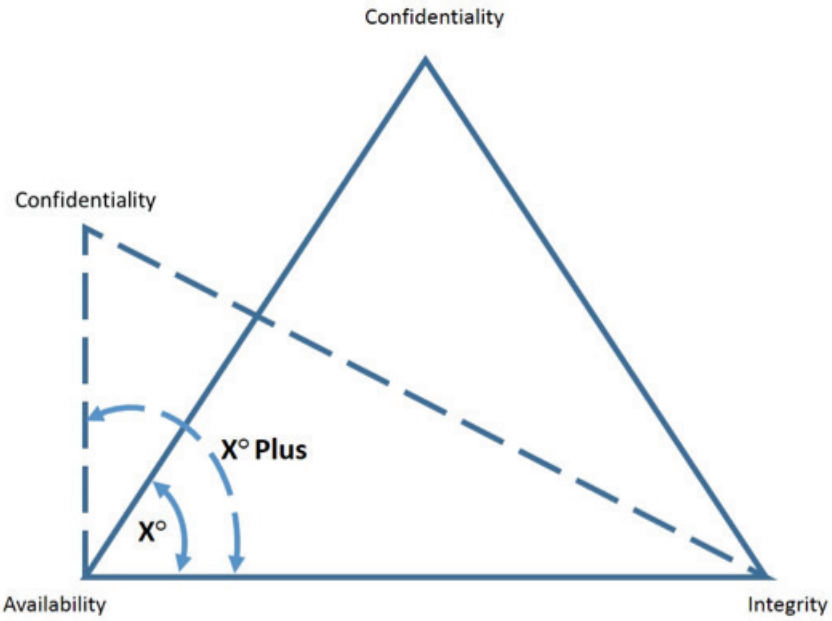

FIGURE 2: THE CIA TRIAD IN HEALTHCARE

far back as 1995, NIST identified the confidentiality, integrity, and availability (CIA) triad as an equilateral triangle. Since then, it has become the standard illustration. While the measurements of the angles were probably never intended literally, the implication is equal value, equal attention. In Figure 2, the measurements are no more precise, but in healthcare the CIA triad is shifted toward availability.

In other industries where contingency plans can withstand days of downtime and manual processes, healthcare cannot. There is emphasis built into the popular risk assessments to guard against unauthorized access (confidentiality). Identity management and authorization are certainly important in healthcare too. The trust between the healthcare system and the patient to keep health information private is central to patient care. Data breaches make the news and financial penalties are widely reported. However, healthcare cybersecurity professionals quickly learn that constant and uninterrupted access to electronic patient information is often more important to daily hospital operation and patient care. Breaches may result in reputational or financial harm but are not likely to impact patient safety. There are specific and required bypasses for authorization and emergency access in HIPAA (break-glass procedures). It is not enough to promise service levels that achieve 24-hour recovery time.

Backup and continuity systems must be robust and responsive. Imagine a scenario where physicians and clinicians rely more and more on digital data and images, but backup and recovery processes lag behind. In this scenario: emergency room physicians and nurses lose access to the medical record and patient histories, patient care is hampered, and financial concerns are magnified as surgeons have to cancel operations. The low tolerance for such lack of availability is understandable. Unlike high-availability systems in other industries, failing to have information in the hands of providers can cause a mistaken diagnosis and kill someone (Christiansen, J., 2012). Healthcare cybersecurity and risk management should strike a different balance within the CIA triad. Not to mention the

fact that billing process are almost prohibited from being done on paper any longer, so electronic system downtime can easily be measured in lost revenue (or at least delayed).

Management of Third-Party Risk

Related to tailoring the information risk assessments to concentrate on the most important concerns, which may be weighted more heavily around availability, is the management of third-party risk. In healthcare, so much of the protected information use is provided by third-party business partners. Data storage, EHR applications management, or managed security services are just a fraction of the types that handle protected health information for the healthcare organization. They may have other clients, but may or may not have any other healthcare clients. Healthcare dictates a compliance scenario for which the third party is not always prepared. Under HIPAA, the same requirements for privacy and security to which the hospital must adhere, must also be met by the third party (Modifications to the HIPAA, 2013). One of the best examples of how this requirement, and the risk assessment that must document it, surfaces is in a data storage company that provides cloud services. Co-mingling health data within environments where non-authorized personnel may have access to it can be unauthorized disclosure. Furthermore, where data is stored at rest, government regulators increasingly mandate that it must be encrypted (HHS announces first HIPAA, 2013). These requirements may not exist outside of healthcare. But if the third party wants to do business with the healthcare organization, they must demonstrate compliance through a documented risk assessment, among other measures. In the final analysis, the key point here is that NIST or ISO risk management processes are important and applicable to healthcare organizations. Third parties who are familiar (in compliance) with these and other information protection standards do not have to retool their business to support healthcare. But they will have to integrate healthcare-specific controls (HIPAA). This is mandatory and may increase cost, alter the third parties' normal business processes and contracts, and increase liability for data loss.

Exception Handling

Cybersecurity professionals have a plethora of tools at their fingertips. Scanning tools like Retina, Nessus, as well as anti-virus applications and perimeter security devices, come to mind. All are extremely powerful and useful, if used appropriately. As cybersecurity has matured and healthcare has become more digitized and connected, the intersection has not always worked for either party. Stated best, the indiscriminant application of even the best cybersecurity tools and practices can result in patient safety issues. This is not meant to be alarmist. But, the assertion is that cybersecurity practices typically do not accommodate the level of exception handling or alternative controls implementation that healthcare often requires (because availability is key). Without a savvy understanding and application of cybersecurity tailored for healthcare, healthcare stops and cybersecurity becomes an organizational pariah.

A major example is that more and more medical devices are networked to each other and the hospital information infrastructure. They not only bring the same vulnerabilities to the network that regular office automation does, they are also susceptible to being impacted when the adversary attacks the hospital network. However, these devices are special purpose computers even as they look and act just like office automation computers on the same network. The key concerns with medical devices — digital x-rays, ultrasounds, and infusion pumps — are that the original manufacturer always remains responsible for in-warranty devices (Quality System Regulation, 2013). They do this because the US Food and Drug Administration (FDA) regulates these devices to ensure patient safety and operational effectiveness. These additional pressures make it difficult, if not impossible, to simply manage them from a cybersecurity perspective like the rest of the information technology inventory. A vulnerability patch added to a

device without manufacturer testing and approval can void the warranty, making future manufacturer support highly problematic. They may consider the device a non-standard configuration. In fact, under some manufacturer warranties, the act of someone else servicing the device voids the warranty. While this might be OK for cybersecurity because the information services personnel can continue to test and apply software, the medical device may become unsafe from a patient care perspective because qualified technicians are no longer accessing the device to maintain it. Developing mitigation strategies around this type of scenario is one example of exception handling.

Another example of exception handing, one of the most prevalent cybersecurity practices that works well with networked information technology, is the automated vulnerability patch management process. It has saved countless hours of cybersecurity professionals' time. Automated end-point management assures a baseline security through tools like [insert favorite tool name here] to identify all the Windows-based computers on the network, load up the prescribed software fixes, and execute.

There is a major problem when the automated patch management process includes medical devices. Some patches can disable processes that regular office automation does not rely on. Medical devices are usually systems with complex dependencies and machine-to-machine communications. They are often vital to the continued existence of a person. Therefore, manufacturers have regression testing processes that help determine the impact of any software changes, including vulnerability patches. At best, the timeline for approval of a patch is usually longer than the timeline for information assurance compliance. At worst, healthcare organizations may be pressured to rely on older versions of the software and develop alternative, mitigating controls. This can create challenges for cybersecurity professionals if these variations to the preferred process are not integrated into the cybersecurity strategy. Even when the vulnerability patch is cleared for implementation on a medical device and the warranty is not voided, care must be taken when the patch is applied. For example, the normal process would be to schedule the update during the weekend, after normal business hours. This might not work for a digital radiology system needed during that time. No one wants to funnel work (revenue) to other healthcare organizations for an emergency radiological interpretation because the in-house system is down for cybersecurity patching.

A third consideration related to exception handling is based on enterprise anti-virus configuration. While the cybersecurity effort must continue to use whatever anti-virus tools are available, one size fits all is not appropriate. The FDA has written several publications to emphasize that medical device manufacturers are not excused from cybersecurity efforts (Cybersecurity for Medical Devices, 2013). Yet, the reality is that many medical devices still operate on older operating systems, run proprietary algorithms, and have complex interdependencies.

For these reasons, cybersecurity professionals have to do their part by ensuring any antivirus is configured with proper exceptions noted. One of the most common exceptions is to configure anti-virus applications to recognize .dcm files in the digital radiology system. If this is not done, each time the anti-virus runs, it may quarantine all .dcm files. The problem is that .dcm is the file extension for Digital Imaging and Communications in Medicine (DICOM) and the protocol for all digital imaging. If those files are quarantined, they become unavailable to the radiologist and that may negatively impact patient care.

EDUCATION AND CERTIFICATION

Education and certification requirements must be established and implemented to develop a professional healthcare cybersecurity workforce that provides a level of assurance to patients and employers alike. Throughout this paper, the

underlying point is that healthcare cybersecurity is unique. To make it possible, cybersecurity professionals must be able to tailor the tools and practices to protect information, yet not impede availability for those who need the information. To impede availability is not just a business contingency issue, or a revenue drain, it can be a patient safety adverse event. These events themselves, under laws like HIPAA can (and do) result in civil and criminal penalties. Therefore, a focused effort to educate, train, and assess competency of healthcare cybersecurity professionals is needed.

To start with, the US National Initiative for Cybersecurity Education (NICE) has been established to build a common set of standards for educators to use in building a cybersecurity workforce. NICE is not focused solely on healthcare, but they draw from the education and credentialing processes already in healthcare for physicians, nurses, and specialized medical practitioners (National Cybersecurity Workforce, 2014). The baseline educational component of NICE follows industry leading frameworks, for example, the 10 domains (CISSP, 2013) in the International Information Systems Security Certification Consortium (ISC)² Certified Information Systems Security Professional (CISSP) curriculum. However, there are additional knowledge domains to cover relative to healthcare information protection. The healthcare cybersecurity professional will need exposure to HIPAA, privacy topics, and the healthcare organization. Again, using the (ISC)² as a guide, one can look at the Healthcare Information Security and Privacy Practitioner for additional (or complementary) domains that the educational curricula should cover (HCISPP, 2013). In fairness, (ISC)² is not the only organization that is championing these areas of study. Other examples exist within AHIMA and the International Association of Privacy Professionals (IAPP), to name just two. The effort here is not to point to one over the other, but as an illustration of how to incorporate educational material into the curriculum that NICE is proposing for educational organizations. While NICE is focused on education from grades Kindergarten through 12, the thought process is found at the collegiate level, too. Many associate and some baccalaureate programs already thinly veil CISSP or the SANS Institute Global Information Assurance Certification (GIAC) credentialing preparation into their academic coursework. It is difficult to criticize such an approach.

The goal is not to simply create degree-granting programs that duplicate credentialing processes. Looking at a few examples of what exist already, one way to address the need to specifically educate (and confer a formal degree) is through the major-minor or concentration process. At Excelsior College, for example, a Bachelor of Science to Master of Business Administration degree path is available. This is unique enough, but they add the opportunity to major in Health Services Management and concentrate on a minor in Cybersecurity Management. Within the Cybersecurity Management minor or concentration, students research and understand the core competencies of cybersecurity; but with their healthcare background, they can apply their knowledge to the unique industry in which they will one day work.

The need for more of these types of specialized programs is growing. There are not a lot of programs in healthcare cybersecurity outside of the major-minor approach. A couple of other examples of formal education leading to graduation from a college or accredited academic institution are the University of River Valley Community College (RVCC), in Claremont, NH, and the Texas State University at San Marcos (TSU-SM), TX. RVCC actually offers an associate degree that (paraphrasing their own words) is unique in that it focuses on the integration of technology with the needs of healthcare. TSU-SM, on the other hand, offers a 16-credit Health Information Privacy and Security Certificate independent of any of their other degrees and coursework. They too, integrate the significant aspects of health information management (e.g. privacy topics) and a familiarization with the

healthcare organization with the core competencies in cybersecurity like data communications and network security fundamentals.

There are not many other programs addressing this need, hence the call for action. As civil and criminal penalties mount in healthcare, the natural inclination might be to get more restrictive in information flow. But that would not enable better, more cost-effective patient care. Locked-down networks with frustrating access control for not-so-technical care providers is not the direction healthcare cybersecurity can afford to go. More educational institutions will see the value in offering degrees in this area, much like NICE sees the value in growing cybersecurity students from their first day at school.

Formal education structures will take time. In the interim, the professional credentialing process is somewhat successful at keeping pace. As introduced earlier, several professional organizations like $(ISC)^2$ and SANS have introduced education and certification programs to offer employers a measure of competency in cybersecurity. To be credible, accompanying any valid certification must be continuing education requirements. Courses and seminars can be held by the accrediting organization or approved for continuing education credit. Either way, once a professional earns the credential through experience and examination, they must maintain it through continual investigation in their education on relevant, current topics.

The credentialing process is more responsive to industry needs, which may be why it is so popular and accepted in information technology, cybersecurity, and now in healthcare. $(ISC)^2$ and SANS have developed several industry and topic-specific credentials already. They see the need to have healthcare-specific credentials as well. From the healthcare side, the growing reliance on information technology and digitization has convinced groups like AHIMA to offer privacy and security certification. To summarize, between formal education and professional certification, cybersecurity in healthcare is only possible if (in part) the healthcare industry can recruit, train, and retain proven, competent, and qualified information protectors based on legitimate standards.

INCENTIVES

Much like the federal government incentivized providers to adopt Electronic Health Records (EHR) under the American Reinvention and Reinvestment Act (ARRA), government incentives are needed to drive quicker adoption of health cybersecurity practices. Follow the money. The technical ability to digitize health records has existed for at least 30 years when the Department of Defense implemented the Composite Healthcare System (CHCS) — now the Armed Forces Health Longitudinal Technology Application (AHLTA) — and the Department of Veterans Affairs had Decentralized Hospital Computer Program (DHCP) — now Veterans Health Information Systems and Technology Architecture (VistA) (Bacon, 2008). But for a variety of reasons well-articulated in any trade publication, commercial healthcare was slow to adopt the EHR. They certainly were slow to adopt anything that would interact with other healthcare organizations, like today's health information exchanges. This is also not a criticism. Margins are very tight in healthcare and capital investment (which an EHR would be) is a competitive process. Revenue is tied to equipment like computed tomography (CT) scanners and additional operating rooms. Channeling investment dollars to digitizing paper records and creating electronic order entry had not proven a return on investment over paper-based records.

However, a few initiatives began to intersect. First, in 1999 the Institute of Medicine published a sentinel report called, "To Err is Human: Building a Safe Health System." This pointed out (among other things) that between 44,000 to 98,000 deaths each year were a result of preventable error (Kohn, 2000). In many cases, EHRs can avoid these errors by digitizing provider notes (eliminating handwriting) and creating alerts (reducing medication prescription errors).

Another initiative at the intersection of EHR adoption is mergers and acquisition of healthcare organizations. As costs rise and external pressures mount, healthcare organizations seem to integrate horizontally. This has both improved communication, as organizational boundaries have fallen, but technical boundaries have arisen because paper-based records cannot physically cover the geographic space between two affiliated healthcare organizations that may now be caring for the same patients collaboratively, not competitively.

There were other initiatives that began to make using EHRs a must around 2009. But, the principal game changer was ARRA. The over $2 billion that the federal government has paid out in reimbursement to healthcare organizations to date spurred healthcare organizations to move away from paper records, since they would see a quick return on investment. Not coincidentally, EHR vendors and implementation consultants proliferated because resources were now available (at minimal risk) for EHR adoption.

Although a brief history lesson, this might sound like a success story. In many ways it is. However, in the effort to move quickly to digitized health information, privacy and security concerns were not adequately addressed. Of the multiple standards a healthcare organization had to attest to regarding "meaningful use" of the EHR (and then receive reimbursement for) only one related to privacy and security and compliance with HIPAA. Meaningful use is a term that indicates that, if a healthcare organization satisfies established objectives, they are not just installing an EHR. They are also using it for certain business and clinical situations. The singular privacy and security standard requires

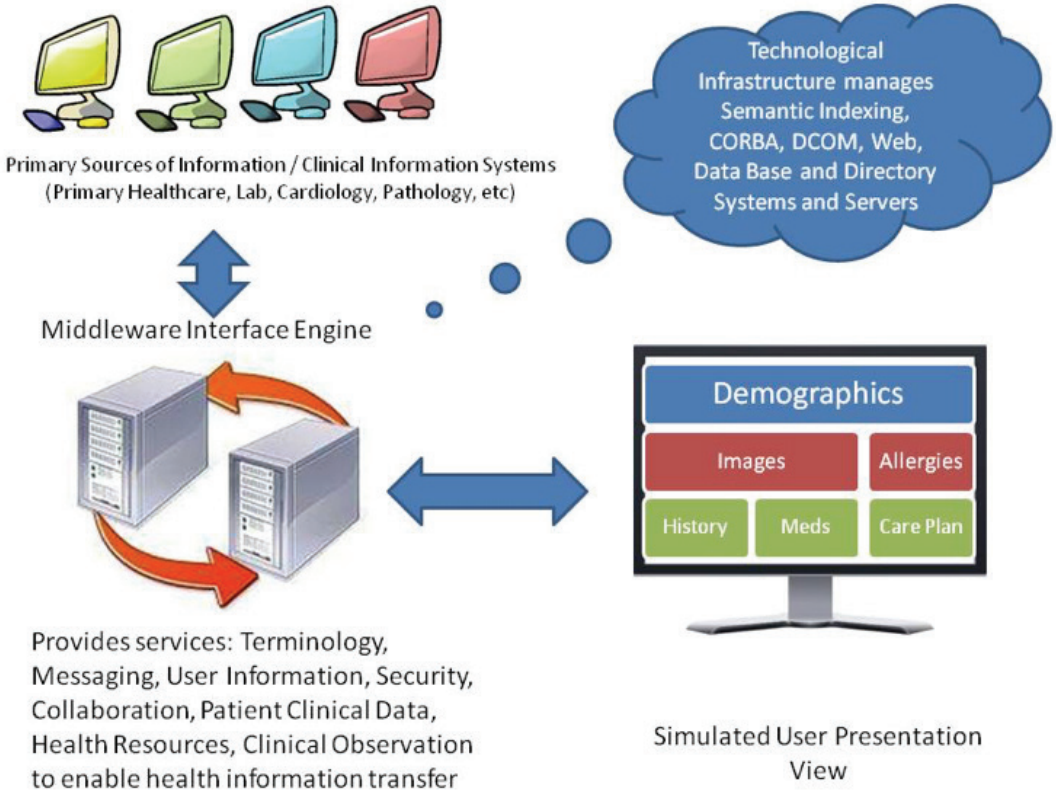

FIGURE 3: THE EHR – A SYSTEM OF SYSTEMS

the submitter to attest that a risk assessment sufficient to HIPAA law was conducted or reviewed annually. No documentation was required to be submitted, just a signature attestation. There was no requirement to demonstrate any investment in perimeter security or network architecture.

A related condition for reimbursement under "meaningful use" was that the EHR had to be certified by the Certification Commission for Healthcare Information Technology (CCHIT), an independent, not-for-profit group that certifies EHRs. Within this requirement were a relatively robust set of privacy and security requirements based in HIPAA authentication, auditing, accounting for disclosures, and least privilege. Important to note, there was no requirement for encryption of data at rest or in transit. That requirement is coming in the next round of certifications. Regardless, the relative attention paid to the EHR privacy and security was a small, albeit positive, step in the direction of what is needed.

Placing a secure (enough) EHR on an insufficiently secure healthcare information network interconnected to numerous third-party business partners and other healthcare organizations is a real vulnerability to the Defense in Depth practices cybersecurity professionals understand. It is important to note that an EHR is not a singular application, but a system of systems with interconnection with legacy clinical and business applications (Figure 3). It is unrealistic to measure security compliance on an EHR product in standalone mode. But, because reimbursement dollars were not dependent upon the architecture or infrastructure in which the EHR was implemented, too little investment was made in the protection of the perimeters of hospitals and the interconnection with legacy systems (not certified by CCHIT).

The solution would be to launch a similar incentive-based program like ARRA to address these discrepancies. The national EHR incentive program has proven successful. But as healthcare operations are rapidly changing, HIPAA compliance and awareness of cybersecurity concerns cannot lag behind (any longer). The definition and standards for demonstrating meaningful use could expand to include more organizational factors for privacy and security. There is no suggestion that the reimbursement should approach an additional $2 billion dollars, but considering how much the healthcare industry already pays (approximately $40 billion) to implement information technology in general, it would be well spent (Lewis, 2011).

Incentives should be tied to measurement of objectives, of course. One standard that relates back to other recommendations made within this paper is to measure healthcare organizations against a workforce competency standard for privacy and security of healthcare information protection. Taking a lead from the Department of Defense Instruction 8570 that requires any workforce member who has information assurance responsibilities to have a requisite competency education and certification, CISSP, e.g. For instance, those cybersecurity workers in a healthcare organization applying for incentives must obtain HCISPP or equivalent.

The organizational cybersecurity readiness can also be measured. Incentives can be applied against an organizational information protection accreditation standard. Much like the Department of Defense has implemented through the Defense Information Assurance Certification and Accreditation Process (DIACAP), commercial organizations can borrow the holistic technical and observational process approach to compile a readiness and maturity level for an organization based on the risk assessment standards. One such assessment unique to healthcare that is gaining acceptance is the HITRUST alliance that provides a comprehensive assessment for healthcare organizations. The state of Texas has gone so far as to require healthcare organizations to receive a "seal of approval" accreditation from HITRUST for its hospitals (HITRUST and THSA, 2013).

The role government plays in commercial healthcare makes these incentives more of an investment than a handout. As the major payer in the U.S., the government is probably the biggest benefactor of advances made in digitizing records. So, too, would they benefit from improving information sharing, protection, and infrastructure modernization now that the EHR stimulus is well underway. The federal government through regulation tends to be more effective in standard setting (like HIPAA). But it also tends to be more effective to apply these standards and require compliance through a reward system for early adopters. The ARRA stimulus plan offered reimbursement rewards until 2014, after which, lack of an EHR resulted in varying levels of fines and penalties. The standards remain (and are expanded), but early adopters are rewarded. Those who took a wait-and-see approach or who procrastinated can only hope to invest in cost avoidance of fines and penalties now. In terms of privacy and security in healthcare, the worry has always been on penalties, fines, and regulatory action from data breaches, at least since the Health Information Technology for Economic and Clinical Health (HITECH) Act amended HIPAA in 2009 with provisions for enforcement. The government can redirect this momentum from compliance to encourage a healthcare system where privacy and security is integrated into the business strategy.

HEALTHCARE CYBERSECURITY LAW ENFORCEMENT

A strategy for having law enforcement specifically attuned to healthcare cybersecurity is also needed. This recommendation borrows from already published suggestions that, in terms of cybersecurity in general, law enforcement must "catch up" with the cyber criminals and their methods and motivations. Looking another step ahead in that pursuit is for law enforcement to recognize how attractive a target healthcare is. The adversary is just starting to see it. A stolen medical identity now has a street value of $50, compared to $14–$18 for a stolen credit card number and just $1 for a stolen Social Security number (Study: Few Aware, 2012). As the adversary finds that healthcare is often a softer target with information stores that are actually more valuable than that of banks, retail, etc., we can expect more hits like these recent ones (Chronology of Data Breaches, 2013):

- On October 15, 2013, the FDA, Center for Biologics Evaluation and Research (CBER) databases were hacked exposing the names, details, phone numbers, email addresses, and passwords of 14,000 accounts (approximately 5,000 of which are active).
- Michigan College of Optometry did not learn until July 23, 2013, that there was potential unauthorized disclosure of protected health information in December of 2011. A server with the names, social security numbers, demographic information, and a limited amount of clinical information for over 3,400 patients was infected with malware.
- Uniontown (PA) Hospital patient information was found posted online for public view and use. Names, encrypted passwords, contact names, email addresses, and usernames may have been exposed. There is no certainty about how long the information had been available.

From the patients' perspectives, they provide healthcare providers sensitive information and they do it with a high level of trust. They trust that the information is needed. They expect it will be used solely for the purpose of treatment, payment, and healthcare operations. And they provide it at a vulnerable time, when they are typically ill or injured. Cybersecurity professionals in healthcare have a big responsibility. However, as pointed out, data breaches do happen. Some are the result of internal activity and some are the result of hackers. This is where law enforcement steps in and can help make cybersecurity possible in healthcare.

It is almost a perfect storm. Healthcare is not as mature in cybersecurity programs as other industries. This is partially because efforts to implement cybersecurity in healthcare, just like other industries, tends to impede healthcare, frustrate providers, and (therefore) seems like only a cost

with little return on investment. Add to this the fact that law enforcement will have to also tailor their new cybersecurity tools and techniques in healthcare. But they must. For instance, where there are provisions to allow disclosure of healthcare information for purposes of law enforcement, it is still tightly controlled. Law enforcement has to be in tune with the request for information procedures of the healthcare organization.

The adversary has realized that currently many healthcare targets are easy prey. Even as cybersecurity attacks can potentially disrupt patient care and business operations immensely, most incidents of hacking have gone unnoticed. One cybersecurity criminals have infiltrated and accessed the target, they can cover their tracks. This means attacks may actually be vastly underreported. There are not adequate mechanisms to detect, report, and investigate them.

Although not the only solution, a proposed direction in which law enforcement should go is to partner with home-grown healthcare intelligence gathering, like the HITRUST Cyber Threat Intelligence and Incident Coordination Center (C^3). The core principle for this organization is to collect and make available industry-relevant cyber threats (HITRUST Cyber Threat Intelligence, 2013). The input comes from the healthcare community and results in proactive alerts to bolster healthcare cybersecurity readiness in the face of potential cyber threats and attacks. With law enforcement connected to these kinds of processes, there can be better detection and mitigation of industry-specific incidents. Where there are many cybersecurity incident alerts services, like the U.S. Computer Emergency Response Team (US-CERT), the HITRUST C^3 can help law enforcement hone in on specific healthcare attacks and coordinate specific healthcare response activities, especially when they involve medical devices and patient safety issues.

CONCLUSION

In the end, cybersecurity in healthcare is more than a possibility. It is an imperative. There is probably no information protection subject with a wider audience and with more at stake. Everyone at some point in their life is a patient and their protected health information, some financial information, and other demographic information is collected, stored, and shared. Clearly, failure to provide adequate cybersecurity is not an option. The right answer is NOT to get used to breaches or to buy credit reporting protection and accept the reality of unauthorized disclosure. However, the right answer is also NOT to apply general, best practice cybersecurity to healthcare. Answers must come from tailoring cybersecurity practices with respect to the business of healthcare and the clinical workflow. The suggestions provided in this paper are a start. The challenge is to discover more ways to tailor cybersecurity to healthcare and refine the initiatives already underway. We must operate with a scalpel instead of a butcher's knife. In the final analysis, this must happen because the adversary is developing new tools and techniques. Healthcare is advancing and constantly changing to make patient care more accessible, affordable, and of higher quality. Healthcare will be more connected, not less. Healthcare cybersecurity will be more valuable, not less.

REFERENCES CITED

Bacon, B. and S. Yoshida. (2008). "Contextual History and Visual Timeline of AHLTA and VistA CPRS Products." PIIM Research. Retrieved on December 20, 2013 from http://www.academia.edu/2995189/Contextual_History_and_Visual_Timeline_of_AHLTA_and_VistA_CPRS_Products

Carr, J. MD. (2011, December 12). "Tenth Report to Congress on the Implementation of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996." National Committee on Vital and Health Statistics. pg 14.

Cheddar Berk, C. (2010, August 12). "How Many Social Security Numbers Do You Have?" *CNBC Consumer Nation*. Retrieved on December 12, 2013 from http://www.cnbc.com/id/38678753

Christiansen, J. (2012, November 1). "The healthcare privacy balance." *The Privacy Advisor.* International Association of Privacy Professionals (IAPP). Retrieved on December 22, 2013 from https://www.privacyassociation.org/publications/2012_11_01_the_healthcare_privacy_balance

"Chronology of Data Breaches." (2013). Privacy Rights Clearinghouse. Retrieved on December 16, 2013 from http://www.privacyrights.org/data-breach-asc?order=field_breach_date_value_1&sort=asc&title=

"CISSP – Certified Information Systems Security Professional." (2013, December). (ISC)². Retrieved on December 30, 2013 from https://www.isc2.org/cissp/default.aspx

"Cybersecurity for Medical Devices and Hospital Networks." (2013, June 13). FDA Safety Communication. Retrieved on December 19, 2013 from http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

"HCISPP—HealthCare Information Security and Privacy Practitioner." (2013, December) (ISC)². Retrieved on December 30, 2013 from https://www.isc2.org/hcispp/default.aspx

"HHS announces first HIPAA breach settlement involving less than 500 patients." (2013, January 2). US Department of Health and Human Services (HHS). Retrieved on December 22, 2013 from http://www.hhs.gov/news/press/2013pres/01/20130102a.html

"HITRUST and THSA Partner to Help Texas Take the Lead in Efforts to Ensure Health Information is Secure." (2013, October 14). Industry Press Release: HIE Answers. Retrieved on December 12, 2013 from http://www.hieanswers.net/hitrust-thsa-partner-help-texas-take-lead-efforts-ensure-health-information-secure/

"HITRUST Cyber Threat Intelligence and Incident Coordination Center." (2013) HITRUST Alliance, LLC. Retrieved on December 18, 2013 from http://www.hitrustalliance.net/c3/

Kohn, L, J. Corrigan, and M. Donaldson. (2000). "To Err Is Human Building a Safer Health System." Institute of Medicine. National Academy Pres. Washington, DC. Page 26. Retrieved on December 3, 2013 from http://www.nap.edu/openbook.php?isbn=0309068371

Lewis, N. "Healthcare IT Spending To Reach $40 Billion." (2011, May 16). Information Week Health Care. Retrieved on January 1, 2014 from http://www.informationweek.com/healthcare/electronic-health-records/healthcare-it-spending-to-reach-$40-billion/d/d-id/1097768

McNickle, M. (2012, June 6). Top 10 data breaches include public health departments. Government Health IT. Retrieved on December 12, 2013 from http://www.govhealthit.com/news/top-10-data-breaches-include-public-health-depts

"Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules." (2013, January 25). Code of Federal Register (CFR) Parts 160 and 164, Vol. 78, No. 17. Section I(A)(ii). pg 5566.

"National Cybersecurity Workforce Framework v2.0." (2014, May) National Initiative for Cybersecurity Careers and Studies. Retrieved on July 24, 2014 from http://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework

Puckett, C. (2009) "The Story of the Social Security Number." Social Security Administration, Office of Retirement and Disability Policy. Social Security Bulletin, Vol. 69 No. 2 Retrieved on December 3, 2013 from http://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html

"Quality System Regulation." (2013, April 1). Food and Drug Administration (FDA). CFR 21 Part 820 Subchapter H. Retrieved on December 17, 2013 from http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=820&showFR=1

"Study: Few Aware of Medical Identity Theft." (2012, July 13). Nationwide. Retrieved on December 11, 2013 from http://www.nationwide.com/about-us/061312-few-aware-of-medical-id-theft.jsp

"Unique Health Identifier for Individuals: A White Paper." (1998, July 2). U.S. Department of Health and Human Services (HHS). Retrieved on December 11, 2013 from http://epic.org/privacy/medical/hhs-id-798.html

AUTHOR

Sean Murphy (sean.p.murphy@leidos.com), CISSP, ISSMP, HCISPP, FACHE, CPHIMS, CIPP/IT, is a vice president in Leidos Health Solutions Group and serves as the organization's health information privacy and security officer. He is a healthcare information security expert, with nearly 20 years of experience in the field, serving at all levels of health care from the hospital to an international integrated delivery system. Before joining Leidos, Murphy was a lieutenant colonel in the U.S. Air Force Medical Service Corps. He has served as CIO and CISO, but his proudest professional accomplishment was his service as senior mentor in 2008 – 2009 to the Afghan National Police Surgeon General's Office in support of Operation Enduring Freedom. He has a master's degree in business administration (advanced IT concentration) from the University of South Florida, a master's degree in health services administration from Central Michigan University, and a bachelor's degree in human resource management from the University of Maryland. He is also an adjunct professor at St. Leo University, a fellow with the American College of Healthcare Executives, board certified by the Healthcare Information & Management Systems Society (HIMSS) and the International Association of Privacy Professionals (IAPP), and holds three certifications from the International Information Systems Security Certification Consortium (ISC)². He is a past chairman of the HIMSS Privacy and Security Committee and serves on the Excelsior College Industry Advisory Councils for Information Technology and General Technology.


EXCELSIOR COLLEGE
FOUNDED IN 1971