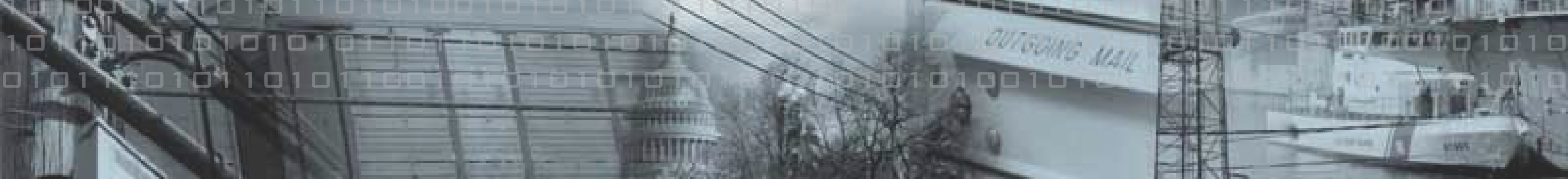

THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

JUNE 2014
PRIVATE SECTOR

VOLUME 12 NUMBER 12

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

Follow us on Twitter here
Like us on Facebook here

GEORGE MASON UNIVERSITY
School of Law
CENTER
for
INFRASTRUCTURE PROTECTION
and
HOMELAND SECURITY

This month *The CIP Report* focuses on the **Private Sector**. Recognizing the essential role industry plays as primary critical infrastructure owners and operators, our authors examine key private sector stakeholders, as well as several important cybersecurity and information sharing initiatives.

First, Rick Saunders highlights the unique way small business can contribute to the infrastructure security and resilience mission space. Our next two articles focus on cybersecurity, with Business Executives for National Security's Alfred R. Berkeley III and General Norton A. Schwartz first looking at the role of C-Suite executives. Thad Odderstol, Director of Industry Engagement and Resilience in the U.S. Department of Homeland Security's (DHS) Office of Cybersecurity and Communications, follows with a discussion of the NIST Cybersecurity Framework and the Critical Infrastructure Cyber Community (C³) Voluntary Program. Jeff Gaynor, Founder and Managing Member of American Resilience Consulting, LLC next argues for Requirements-Based Information Sharing to engage the private sector and enhance resilience. Finally, David Willey, DHS Protected Critical Infrastructure Information (PCII) analyst, explains that program and examines its success in the courts.

We would like to take this opportunity to thank this month's contributors. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Small Business and Infrastructure Security and Resilience

by Rick Saunders*

Small business contributions to the national economy are well known. According to the Small Business Administration (SBA), twenty-three million small businesses in the United States account for 54 percent of U.S. sales and 55 percent of jobs. Small businesses provide economic and social benefits both to business partners and their communities. The best small businesses offer innovative, tailored services and solutions; flexibility and agility; and often attractive price points. In addition to their importance for communities and the economy in general, small businesses are part of every critical infrastructure sector. Small businesses are infrastructure owners and operators and essential components of private-sector networks that support operations within and across sectors.

Unfortunately, small businesses also encounter distinct challenges when trying to strengthen preparedness and resilience because of their size and market positions. Infrastructure security and resilience efforts, both within and across sectors, must recognize the important roles that small businesses play in critical infrastructure, while taking into account the difficulties that small businesses face when preparing for and recovering from disasters and other disruptions.

Small business owners and operators are prevalent in certain infrastructure sectors. For example, large numbers of small businesses engage in food production, distribution, and service. As the Food and Agriculture Sector-Specific Plan (SSP) points out, differences in farm size is an important, complicating factor for prevention and protection efforts by both individual operators and across the sector.[1]

Small businesses play important, if less direct, roles in virtually every critical infrastructure sector because of the interconnected nature of the economy. To maximize efficiency and cost savings, enterprises seek to focus on core competencies while often outsourcing many direct and indirect support functions to small businesses when they can offer specialized capabilities and cost advantages. As a result, all infrastructure providers rely on highly complex networks of both large and small businesses for inputs and services. These include direct inputs such as raw materials and key components; services and goods from other infrastructure sectors such as water and power; inputs that may not be direct parts of the value chain but are essential to the workforce and environment, such as food services, local transportation, and healthcare; and services that sustain work processes, such as transportation and supply chain services, finance, and communication. The National Infrastructure Advisory Council explored the extent and complexity of these interdependencies in a study that also noted that operators in large and diverse sectors generally lack access to information about partners within their own sectors and across sectors, "especially those potentially critical medium- and small-sized businesses."[2]

Unfortunately both for these operators and for the infrastructure sectors in which they participate, small businesses face business imperatives that make it extremely difficult for them to achieve the level of resilience necessary to cope with major disruptions. In the typical small business, all resources—intellectual and human capital, production capacity, finances, and management attention—are committed to day-to-day business activity. As a result, small businesses lack capacity to implement robust business continuity programs, making them vulnerable to lasting economic

(Continued on Page 3)

[1] U.S. Department of Homeland Security, *Food and Agriculture Sector-Specific Plan*, (2010), 1.

[2] National Infrastructure Advisory Council, *Chemical, Biological, and Radiological Events and the Critical Infrastructure Workforce: Final Report and Recommendations by the Council,* (2008), 47, 51-52.

(Continued from Page 2)

damage from a single event. They usually operate on very thin margins and do not generate the overhead, or indirects, necessary to develop or exercise resilience plans. Leaders do not have the time to participate in sector or community-based collaborative forums. Small businesses are often based in a single location or occupy a very limited number of facilities, making them susceptible to localized calamities. They have few customers and suppliers, and have limited alternatives in the face of supply or distribution chain disruptions. Perhaps most important, they lack financial reserves or alternative lines of business making it difficult to retain their workforce or meet obligations if their core business is interrupted. The impact is telling: between 25 percent and 30 percent of small businesses do not reopen after a major disaster.[3]

National critical infrastructure strategy—set forth in Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience*; the 2013 edition of the National Infrastructure Protection Plan (NIPP 2013); and the supporting SSPs—recognizes both the central role of the private sector and the significance of dependencies, interdependencies, and cascading effects within and across sectors. With 85 percent of critical infrastructure in private hands, NIPP 2013 correctly stipulates that "[i] ndustry does a great deal to secure its own infrastructure and the welfare of the communities it serves."[4] Government's role is to encourage industry "to go beyond what is in their commercial interest and invest in the national interest through active engagement in partnership efforts."[5] NIPP 2013 points out that increasing reliance on information technology and communications systems and other factors are deepening interdependencies across critical infrastructure systems, with significant implications for critical infrastructure security and resilience planning and action.

The national strategy is founded on the importance of private industry and how interconnections shape the environment for infrastructure security and resilience. Within this framework, however, relatively little attention is paid to the consequences of small business participation in infrastructure sectors or to the challenges that make it hard for small businesses to enhance their own security and resilience or collaborate effectively with their larger partners. As it is, PPD-21, NIPP 2013, and the SSPs mostly talk of "industry" without differentiation or indication of how size might matter. There is occasional mention that extensive small business presence complicates sector planning and that special efforts are needed to involve small companies in collaborative efforts. But the nature of those complications and how to address them remains largely undeveloped. For their part, SBA and DHS provide useful advice and resources on business preparedness and resilience best practices, often tailored specifically to small business needs. These focus on steps small businesses can take to protect their own viability and speed recovery after an incident—valuable resources for business continuity planning, but less helpful for assessing small business's place in the larger infrastructure environment.

NIPP 2013's goal of encouraging industry to go beyond what is in its commercial interest and invest in the national interest must be applied to small business as well, within the obvious constraints of size and resources. This requires knowing more about the nature and extent of small business participation in critical infrastructures, greater appreciation for the challenges and vulnerabilities small businesses face and their impact on infrastructure interdependencies and potential cascading effects, and collaborative tools and incentives for addressing these challenges.

A starting point is developing a more thorough understanding of how business relationships—the network of commercial partnerships whereby inputs and services are traded—affect interdependencies. This must include all significant inputs, not just those directly linked to production and distribution. After all, even if power is back on and raw materials are available, a factory will not operate at capacity if the workers have not returned to their homes because they cannot buy gasoline or the local groceries are still closed. This understanding

(Continued on Page 4)

[3] See, for example, American Sustainable Business Council, "Climate Change Preparedness and the Small Business Sector," July 26, 2013.
[4] U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, (2013), 1-2.

(Continued from Page 3)

must include the nature, capabilities, and resilience of business partners, especially when small businesses are involved. Who are the key direct, indirect, and supporting suppliers, large and small? What are their capabilities and vulnerabilities? How resilient are they? What steps can be taken within the sector collectively to mitigate against disruptions and facilitate recovery? The goal here is to develop a realistic, shared picture of small business contributions to sector operations as well as small business readiness and vulnerabilities. Problems can be identified in advance and mitigated if small businesses are brought into the dialogue early.

For their part, small businesses involved in critical infrastructure sectors must do everything they reasonably can to enhance their own resilience and preparedness. At a minimum they need to establish sensible business continuity programs which will reduce their overall risk profile, even in situations that do not threaten infrastructure integrity. Further, they need to appreciate their own role in the larger infrastructure sector. This includes understanding their customers' and suppliers' needs and how their respective continuity plans mesh. It also involves participating in collaborative planning efforts and being ready to consult when a crisis occurs. Small business operators should ensure that their workers and key backers also appreciate how the enterprise contributes to larger community interests as well as what may be expected and provided during and after an event. Knowing that their work is important to overall recovery and that their employer is taking steps to increase the prospect that they will have jobs when it is all over will encourage employees to support the enterprise through the crisis.

There is an internal business case for taking these steps. Large business partners in the infrastructure sector that are addressing their own business continuity needs and thinking about the overall resilience of their sector will also see the benefit of working with small businesses who are apt to remain reliable through difficult circumstances.

Large businesses reinforce this business case with practical steps. At a minimum, they should offer advice, lessons learned, best practices, and other information to ease the planning burden faced by small businesses. Contracts could contain incentives for participation in response and recovery planning as well as surge provisions for continuing services under adverse conditions or similar contingencies.

Similarly, public-private partnerships at the community and sector level should involve small businesses wherever possible. The process should be as inclusive as practicable, not only representing first-tier subcontractors and direct suppliers, but also those small businesses providing essential services to the workforce. Small businesses should be part of sector and community planning processes, either as individual enterprises or through group representation.

A potential dilemma arises from the inherent difference between large- and small-business resilience, which must be anticipated. In a highly networked environment, large businesses will try to shift rapidly to new suppliers and service providers if something disrupts their existing channels. Indeed, their business continuity plans will anticipate such moves. On the other hand, small businesses in the affected area, for the reasons just described, may be unable to meet immediate demands and as a result lose long-term business opportunities. Thus a highly adaptive sector-level strategy that aims at rapid recovery through shifting supply chains and finding alternate providers could have an unintended effect of disadvantaging local small businesses and thus hampering economic recovery. Recovery plans should seek to avoid this dilemma by considering both the near- and long-term consequences for both the health of the infrastructure and the local economy.

Cybersecurity presents special challenges for small businesses and their partners. When one company provides materials, products, or services to another, they gain access to each other's IT networks so they can share technical, scheduling, and financial information and carry out essential administrative functions such as time charging and billing. As a result, the combined network becomes only as safe from cyber attack as the most poorly defended member. This may be the small business partner who, again for reasons stated previously, is unable to afford adequate cybersecurity staff and tools. The Information Technology SSP recognizes this problem and calls for special efforts

(Continued on Page 5)

(Continued from Page 4)

to train small businesses about the importance and impact of cybersecurity. Similarly, all sectors should promote sharing of cybersecurity capabilities among large and small business partners engaged in critical activities.

Taking these steps does not require extensive rethinking of infrastructure security or community resilience strategies and principles. The fundamentals are correct. What is needed is greater recognition of the importance of small businesses in both communities and critical infrastructure sectors and better accounting for their vulnerabilities. The objective is to build upon current approaches and resources for small business continuity and resilience while creating opportunities and incentives that enable small businesses to become more effective contributors to sector security and resilience efforts.❖

**Rick Saunders is an independent consultant working with small and large businesses supporting the homeland security sector. For over a decade he was a senior executive with a major strategy and technology firm, where he helped build and manage an extensive homeland security practice. Prior to joining the private sector, Rick held several national security affairs positions, including in the Office of the Vice President and as a member of the National Security Council Staff.*

The Rick Rescorla National Award for Resilience

The Department of Homeland Security (DHS) is seeking nominations for the 2014 Rick Rescorla National Award for Resilience that will recognize leadership in fostering resilience during 2013.

The award is DHS's first national resilience award for superior leadership and innovation by a private sector individual or organization who exemplifies the qualities and achievements of Rick Rescorla. While the award is for individuals and organizations in the private sector, volunteer responders - firefighters, emergency medical providers, and law enforcement personnel - are also eligible. In addition, local government officials, including first responders, are encouraged to nominate individuals or organizations in their communities. In 2014, there will be two separate awards for organizations, one for "for-profit organizations" and one for "not-for-profit organizations."

Candidates may be nominated for the Rick Rescorla National Award for Resilience until July 17, 2014, 11:59 p.m. (EDT). All nominations must be submitted by email to the following DHS email address: rescorlaaward@hq.dhs.gov. For further information, including the nomination form, please visit the web page at www.dhs.gov/rick-rescorla-national-award-resilience.

Questions concerning the award may be sent to bradley.garner@hq.dhs.gov.

Driving Cybersecurity from the Corner Office

by Alfred R. Berkeley III* and General Norton A. Schwartz, USAF (Ret.)**

Occupants of the corner office, or C-Suite, are coming to recognize cyber risk as the twenty-first century corporate raider. The Ponemon Institute surveyed sixty large U.S. companies in 2013, finding the average annualized cost from cybercrime was $11.56 million, a 26 percent increase from 2012.[1] Cyber threats are constantly evolving and are becoming more numerous and sophisticated. In 2013 FireEye analyzed almost 40,000 unique Advanced Persistent Threats against companies, equating to more than one hundred per day.[2] CEOs are taking note because a cyber breach can have real strategic implications for a company and affect its bottom line. The recent massive data breach at retail giant Target highlighted the real damage caused by cyber events, including loss of consumer confidence, a drop in revenue, an S&P downgrade, numerous lawsuits, and the uncomfortable spectacle of C-Suite executives spotlighted for their cyber risk management decisions.[3]

With the cyber threat to companies on the rise, cyber risk must be managed like any other business risk—through existing enterprise risk management and governance processes, including oversight by the Board of Directors. CEOs oversee the steps their company is taking to mitigate critical corporate risks, such as financial risk; thus, CEOs should also be up to speed on the cyber risks facing their company and associated mitigation strategies. CEOs would not accept a simple thumbs-up from their CFO; neither should they be satisfied with a cursory update from their CIO. A business-proven risk management strategy offers the best way for companies to manage, mitigate, and recover from the inevitable cyber event. An activist, CEO-led corporate cyber risk assessment and management plan is essential for doing business in today's internet-connected economy.

Assessing and Managing Cyber Risk from the C-Suite

While perfect cybersecurity is impossible, with strong executive leadership, companies can effectively manage and mitigate cyber risk and recover from cyber incidents.

Getting Started

The CEO is responsible for managing and overseeing enterprise risk management. Senior executives should be involved in identifying and valuing key assets that must be protected to secure the company's business processes and organizational strategy. The C-Suite should provide direct oversight of risk assessments, cybersecurity plans, incident response, and security budgets. But none of this is truly effective unless the CEO personally leads by setting the tone of cybersecurity awareness throughout the organization.

Regardless of company size and sophistication, the CEO should know the answers to the following questions:

- Who is responsible for developing and implementing an enterprise-wide approach to cybersecurity? Are enterprise leaders, and

(Continued on Page 7)

[1] Ponemon Institute, 2013 Cost of Cyber Crime Study: United States, (2013) 1, accessed March 30, 2014, http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf.

[2] FireEye, Advanced Threat Report: 2013, (2014), 2, accessed March 31, 2014, http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2013.pdf.

[3] Paul Ziobro, "Target Earnings Slide 46% After Data Breach," *The Wall Street Journal*, February 26, 2014, accessed April 2, 2014, http://online.wsj.com/news/articles/SB10001424052702304255604579406694182132568; Andria Cheng, "Target Credit Rating Cut by S&P After Data Breach," Market Watch, March 28, 2014, accessed June 9, 2014, http://www.marketwatch.com/story/target-credit-rating-cut-by-sp-after-data-breach-2014-03-28; Joel Schectman, "Banks Heap Suits on Target Over Breach," *The Wall Street Journal*, February 7, 2014, accessed April 2, 2014, http://blogs.wsj.com/riskandcompliance/2014/02/07/banks-heap-suits-on-target-over-data-breach/?mod=wsj_rchome_rcreport.

(Continued from Page 6)

not just IT professionals, involved in cybersecurity?[4]

- How is the C-Suite informed about cyber risk and its impact on the business?[5]

- What is the company's current level of cyber risk and its potential impact on operations? How many incidents does the company typically detect a week? What is the plan to address this risk?[6]

- Does the company have a cyber-incident response and recovery plan? How often is the plan tested and how often are the results assessed?[7]

- How is the Board of Directors informed about cyber risk and the risk management plan?

- If the company is public, is the company following the Securities and Exchange Commission guidance on disclosure of cybersecurity risks and cyber incidents?[8]

- How does the cybersecurity program compare to and apply industry standards and best practices?

Cyber Risk Assessments and Management

In incorporating cybersecurity into enterprise risk management, a company first needs to perform a cyber assessment that determines what information and assets need protection, as well as the likely consequences of a successful cyber-attack on those assets, including the hard and soft costs of service interruption and data leakage. The CEO needs to determine, from a strategic and business perspective, which assets and functions are of the highest priority for the company to protect.

The CEO should also understand what contractual promises the company has with customers or partners that could be affected by a cyber event. Further, the CEO should consider what role customer trust plays in the business model and how a cyber event could undermine that trust. Once corporate assets are classified by importance, the company can determine how to allocate resources to protect the most critical assets. This cyber assessment will enable the CEO or Board to accept an appropriate risk profile. Of special note, as demonstrated by the recent Target breach, companies must also focus on the security of their entire supply chain to include vendors, customers, and anyone with access to their network, not just their internal security alone.

The next step is creating a Cybersecurity Plan that looks at transferring, avoiding, mitigating, or accepting the risk and includes an effective incident response and recovery plan. [9] A regular review of the Plan and a reporting process permits the CEO to evaluate the effectiveness of this Plan and make sure it has been implemented and is protecting the company's key assets and strategic future.

In addition to evaluating the company's cybersecurity assessment and plan and making sure cybersecurity is incorporated into the larger tapestry of enterprise risk management, the CEO must be in the position to work with the Board of Directors on oversight of cybersecurity risk management and investment tradeoffs, and respond to shareholder questions and concerns.

Creating a Culture of Cybersecurity Awareness

To be successful in the quickly changing cyber landscape, a CEO should have ongoing dialogue with staff about cybersecurity. CEOs must ensure that the company culture internalizes the potential for harm to the enterprise posed by

(Continued on Page 8)

[4] James Kaplan, Shantnu Sharma, and Allen Weinberg, "Meeting the Cybersecurity Challenge," *McKinsey & Company*, June 2011, accessed March 31, 2014, http://www.mckinsey.com/insights/business_technology/meeting_the_cybersecurity_challenge.

[5] Department of Homeland Security, "Cybersecurity Questions for CEOs," accessed March 30, 2014, http://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf.

[6] Ibid.

[7] Ibid.

[8] Division of Corporation Finance, Securities and Exchange Commission, "CF Disclosure Guidance: Topic No. 2, Cybersecurity" accessed June 16, 2014, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[9] Jody Westby, "Don't Be a Cyber Target: A Primer for Boards and Senior Management," *Forbes*, January 14, 2014, accessed March 31, 2014, http://www.forbes.com/sites/jodywestby/2014/01/20/dont-be-a-cyber-target-a-primer-for-boards-and-senior-management/.

(Continued from Page 7)

data breaches, compromise, or theft of intellectual property through cyber means. Further, employees must recognize the role of access controls, social media policy, and business partners in maintaining cybersecurity. A CEO should consider what policies, awareness efforts, and training would help the company with its cyber efforts. Employees also need to know that the CEO expects employees to implement and follow the policies and practices in the workplace regarding internet hygiene and safety.

C-Suite Use of the NIST Cybersecurity Framework—A Tool to Manage Cyber Risk

Pursuant to the February 2013 Cybersecurity Executive Order, on February 12, 2014, the National Institute of Standards and Technology (NIST) released a voluntary Cybersecurity Framework that provides guidance on how to manage cybersecurity risk. It is primarily focused on critical infrastructure providers but is adaptable for other companies and is technology-neutral.[10] The NIST Cybersecurity Framework was developed through government and industry collaboration and focuses on using business drivers to address and manage cybersecurity risk as part of an organization's enterprise risk management.[11] Acknowledging that there is not a one-size-fits-all approach to cybersecurity, the Framework provides multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today.

For companies starting out, the Framework can be used as a reference to establish a new cybersecurity program. For those companies with developed cybersecurity programs, the Framework can be used to strengthen existing cybersecurity risk management by determining gaps in a company's current program and developing a roadmap for improvement.[12]

Benefits of Adoption

The Framework is flexible and adaptable to a company's specific risk profile and resources. It can also be used to improve communication of cybersecurity activities from the operational level to the executive level, and provide a way to communicate cybersecurity priorities with outside vendors and business partners. As noted by AT&T CEO Randall Stephenson, AT&T will use the Framework as a baseline requirement for its suppliers and partners because any "large company that isn't imposing cybersecurity standards on their supply chain has a vulnerability that they don't know about."[13] Use of the Framework could also increase customer confidence in a company's security and privacy policies by providing a common method of reference, not unlike public accounting standards.

The Framework is a living document that will continue to be updated and improved as industry provides feedback.[14] Adopting it now may make sense because there is speculation that the Framework will become a de facto industry standard, as well as a factor in plaintiff data breach lawsuits and regulatory actions. Additionally, a broad adoption of the NIST Framework will strengthen the overall cybersecurity posture of critical infrastructure, commercial enterprises, and the broader U.S. economy.

Conclusion

As the cybersecurity landscape rapidly changes, and more prevalent and varied threats are exacting an ever-greater toll on U.S. companies, CEOs must actively include cybersecurity in their enterprise risk management portfolio. Time is of

(Continued on Page 9)

[10] The White House Office of the Press Secretary, "Executive Order—Improving Critical Infrastructure Cybersecurity," February 12, 2013, accessed March 31, 2014, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[11] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, (2014), 2, accessed March 30, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[12] Ibid., 4.

[13] Cynthia Brumfield, "NIST Framework Released to Widespread Praise, but What Happens Next?" *CSO Online*, February 13, 2014, accessed April 2, 2014, http://www.csoonline.com/article/2134401/metrics-budgets/nist-framework-released-to-widespread-praise--but-what-happens-next-.html.

[14] National Institute of Standards and Technology, *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, (2014), 1, accessed March 30, 2014, http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

(Continued from Page 8)

the essence and CEOs will need to aproach the cyber threat first with a deep appreciation for what makes their company unique and then apply all available resources, such as industry sector best practices and the NIST Cybersecurity Framework, to ensure the cyber threat is effectively addressed and understood throughout the organization and among external stakeholders. CEOs must lean forward and address a threat that they cannot see, touch, hear, or smell, and learn from the experiences of their peers who were not properly positioned to manage cyber risk and recover from the inevitable breach.❖

**Alfred R. Berkeley III serves as Chairman of Princeton Capital Management, Inc., a registered investment advisor, and has over 40 years of experience in the financial industry, including as President and then Vice-Chairman of the NASDAQ Stock Market, Inc. from June 1996 until August 2003. Mr. Berkeley also serves on the Board of Directors of Business Executives for National Security (BENS).*

*** General Norton A. Schwartz, USAF (Ret.) served as Chief of Staff for the U.S. Air Force from 2008-2012 and is president and CEO of Business Executives for National Security (BENS).*

Founded in 1982, BENS is a nationwide, non-partisan organization which applies best business practices to develop, for government officials, solutions to our nation's most challenging problems in national security, particularly in defense and homeland security. For more information, please visit: www.bens.org.

8TH ANNUAL HOMELAND DEFENSE AND SECURITY EDUCATION SUMMIT

Registration Now Open!

October 9-10, 2014
Colorado Springs, Colorado

This year's theme:
Rethinking Infrastructure Protection:
Innovative Approaches for Education and Research

For additional information, visit:
https://hsedsummit.com/

NIST Cybersecurity Framework and the C^3 Voluntary Program: Improving Cyber Resilience in the Private Sector

by Thad Odderstol, Director, Industry Engagement and Resilience,
Office of Cybersecurity and Communications, National Protection and Programs Directorate,
U.S. Department of Homeland Security

Cybersecurity Threats to the Private Sector

The vast majority of critical infrastructure in the United States is privately owned, and the private sector has increasingly turned to technological solutions to carry out its missions. Businesses are increasingly coming to understand that any disruption to information systems can hamper operations, slow supply chains, damage reputations, and compromise customer data and intellectual property. It is imperative that companies and organizations protect their systems from cyber threats.

Cybersecurity is about managing cyber risks at an acceptable level and in an ongoing manner. Cybersecurity and cyber risk management are also important components of wider enterprise risk management, not simply a checklist of requirements implemented by an IT department. Business leaders too must acknowledge and understand how cyber risks fit into their existing risk management frameworks and governance processes. Cyber risk management discussions must begin with an organization's leadership team and should be communicated regularly with those accountable for managing enterprise-wide risks.

Both the private sector and government have a role to play in strengthening the security and resilience of our nation's critical infrastructure, and it is imperative that we take coordinated actions to achieve this goal. The need for public-private partnerships to combat the increasing number of cyber threats against our nation's critical infrastructure is greater than ever. As technologies evolve, all critical infrastructure sectors will continue to rely heavily on cyber-dependent systems. Taking collective actions with our partners remains a key factor in securing our nation's critical infrastructure, including cybersecurity.

Background on Executive Order 13636: Improving Critical Infrastructure Cybersecurity, Presidential Policy Directive 21, and the NIST Cybersecurity Framework

In 2013, President Obama signed Executive Order (EO) 13636: *Improving Critical Infrastructure Cybersecurity*, changing the way we approach critical infrastructure cybersecurity. The President also released Presidential Policy Directive (PPD)-21, which aims to increase the overall resilience of our nation's critical infrastructure. Together, the EO and PPD drive action toward a "whole of community" approach to cyber resilience, where government and industry across the nation work together to make cybersecurity a priority. The Cybersecurity Framework—developed by the National Institute of Standards and Technology (NIST), in collaboration with industry—consists of standards, guidelines, and best practices to promote critical infrastructure security and resilience through cyber risk management. With physical security and cybersecurity dependent on each other, the extensive work that has been done to enhance both the physical and cybersecurity of critical infrastructure enhances our nation's resilience.

Introducing the Critical Infrastructure Cyber Community (C^3) Voluntary Program

In support of these policies, the Department of Homeland Security (DHS) launched the Critical Infrastructure Cyber Community (C^3) [*pronounced C-Cubed*] Voluntary Program. The C^3 Voluntary Program is an innovative public-private partnership designed to help align critical infrastructure owners and operators with resources that will help them use the Cybersecurity Framework and manage their cyber risks. The C^3 Voluntary Program provides free tools,

(Continued on Page 11)

(Continued from Page 10)

services, best practices, and templates to support implementation. These include the DHS Cyber Resilience Review (CRR), which has been updated to map to the Cybersecurity Framework.

DHS has been working with critical infrastructure sectors for years to increase the awareness of how cyber risks affect all industries and how each company and sector can develop strategies to address these risks head-on. With the recent release of the EO and the Cybersecurity Framework, we are capitalizing on the increased interest in cybersecurity to increase participation in the national effort. Our goal is to turn that increased interest into increased action.

C^3 Voluntary Program Cyber Risk Management Goals

The primary goals of the C^3 Voluntary Program are to support industry in increasing cyber resilience, to increase awareness and use of the Cybersecurity Framework, and to encourage organizations to manage cybersecurity as part of an all-hazards approach to enterprise risk management. The C^3 Voluntary Program's focus in its first year will be engagement with Sector-Specific Agencies (SSAs) and organizations to develop guidance on how to implement the Cybersecurity Framework. Later phases of the C^3 Voluntary Program will broaden the program's reach to all critical infrastructure and businesses of all sizes that are interested in using the Cybersecurity Framework.

Through the C^3 Voluntary Program, the critical infrastructure cyber community has an opportunity to share resources and lessons learned and to build a sustained community of interest around cyber risk. This community will include a broader range of stakeholders, as more people become interested and want to reduce cyber risk to their organizations. The vision of the community is to offer a place for industry, State and local governments, and many other organizations to convene and discuss the evolving cyber risk management needs and forge solutions.

There are three key activities the C^3 Voluntary Program is supporting to execute these goals, which can be most easily remembered as the "Three Cs":

- *Converging* – The C^3 Voluntary Program is converging critical infrastructure community resources to support cybersecurity risk management and resilience through use of the Cybersecurity Framework. DHS created a website at www.us-cert.gov/ccubedvp, for the first time linking its resources in one place to assist with the Cybersecurity Framework and to support cybersecurity for public and private sector partners.

- *Connecting* – The C^3 Voluntary Program is connecting critical infrastructure stakeholders to the national resilience effort through advocacy, engagement, and awareness. This activity focuses on driving greater participation by stakeholders not previously involved in critical infrastructure security and resilience efforts, as well as re-engaging those that have been involved to ensure awareness of the Cybersecurity Framework and effective communication of available resources to provide assistance.

- *Coordinating* – The C^3 Voluntary Program is coordinating critical infrastructure cross sector efforts to maximize cybersecurity resilience, focusing on socializing cross sector efforts and approaches and lessons learned. DHS is working to ensure that Cybersecurity Framework implementation planning efforts reinforce Sector Specific planning and reporting guidance, to reinforce cybersecurity as part of the all-hazards risk management approach.

Resources for the Private Sector

In addition to providing any organization interested in using the Cybersecurity Framework a way to get started, the program provides access to free and readily available technical assistance, tools and resources to strengthen capabilities to manage cyber risks, and opportunities to influence peers and other partners in the critical infrastructure community. Through participation in the program, organizations can use available resources to meet their fiduciary responsibilities to manage cyber risks in a consistent way with other critical infrastructure stakeholders.

The C^3 Voluntary Program also marks the first time that DHS has converged all of its available resources to support cyber risk and resilience for Federal, State,

(Continued on Page 12)

(Continued from Page 11)

local, tribal and territorial governments, and business partners on one site. Currently, the C^3 Voluntary Program features more than thirty DHS programs and tools, all available online at www.dhs.gov/ccubedvp and www.us-cert.gov/ccubedvp. The C^3 Voluntary Program websites offer a comprehensive overview of the program, downloadable tools, and outreach materials. For example, companies and organizations may download an Outreach and Messaging Kit that includes informational materials for easy printing and/or electronic distribution to help educate stakeholders on the C^3 Voluntary Program. The kit also includes a slick sheet for CEOs and other leaders regarding cyber risk management. Through ongoing engagements with US government and private sector partners, DHS will be increasing the resources and information available to our stakeholders, with additional resources identified and promoted in the near and long term.

As mentioned previously, the C^3 Voluntary Program features the CRR, a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of ten domains, including risk management, incident management, service continuity, and others. To learn more about the CRR and to download tools, visit www.us-cert.gov/ccubedvp/self-service-crr.

Getting Involved with the C^3 Voluntary Program

In order to help protect the economy and national security, the private sector must continue to provide innovative risk reduction and mitigation activities, as well as comprehensive security and communication strategies. These strategies will be most effective if developed through collaboration with stakeholder partners and in accordance with applicable policies, procedures, laws, and directives.

The Cybersecurity Framework is an important step toward raising the bar for cybersecurity across our critical infrastructure. We must all invest in the success of the Cybersecurity Framework because it supports the critical infrastructure upon which we all rely. While the C^3 Voluntary Program was recently launched as a new program within the DHS Office of Cybersecurity and Communications, it is really an extension and refocusing of the DHS's long experience in working with industries across the country to transform their outlook on cybersecurity. The program reinforces DHS's larger risk-reduction mission, as well as the importance of an all hazards enterprise risk management approach. The majority of program activity has been focused on engagement, awareness, and building momentum. Over time, the program will serve as a blueprint for sustaining this elevated interest in cybersecurity and driving changes in behavior across the country.

DHS invites private sector companies and organizations to join the C^3 Voluntary Program and take advantage of technical assistance and tools and resources available to ensure a more resilient critical infrastructure for a more resilient nation. The C^3 Voluntary Program is open to any organization that is interested in using resources and engaging with DHS to develop guidance on how to implement the Cybersecurity Framework. Individuals are also encouraged to opt-in as a C^3 Voluntary Program Community Member to receive free Cybersecurity Framework-related information and communications from the program via email.❖

For more information, to join the C^3 Voluntary Program, or learn more about upcoming events, please visit www.dhs.gov/ccubedvp or www.us-cert.gov/ccubedvp, or email the program at CCubedVP@hq.dhs.gov.

Requirements-Based Information Sharing: Engaging the Private Sector, Building Trust and Resilient Critical Infrastructures

by Jeff Gaynor, Founder and Managing Member, American Resilience Consulting, LLC;
President, InfraGard Atlanta Member's Alliance*

America's aged and increasingly exploited cyber and physical critical infrastructures are both the enablers and disablers of American life. Accordingly, every American has a personal stake not only in their *protection*, but also their operational resilience.

As discussed in an article in the January 2014 edition of *The CIP Report*, titled "Quantifying and Implementing Critical Infrastructure Resilience (CIR)," CIR is an objectively measurable, risk-based, cross-sector infrastructure preparedness standard and operating condition built upon critical infrastructure performance requirements of American communities. Accordingly, it is essential that information sharing with Private Sector-owned and operated infrastructure service providers be extended to high-value and potentially high-consequence producing Private Sector entities/consumers of infrastructure services—to include those providing assistance to communities in the wake of disasters.

Requirements-Based Information Sharing (RBIS) can be extended to additional Private Sector entities by adapting long-standing U.S. Intelligence Community collection management methodologies. In a nutshell, RBIS enables key Private Sector entities/infrastructure consumers to ask a specific question and receive a specific answer. RBIS brings distinct advantages over the "top-down" flow of sector-focused critical infrastructure related information sharing. Among them:

- RBIS provides homeland security infrastructure analysts far greater insight into the real-time preparedness and continuity issues being addressed by consumers of infrastructure services. That insight translates into timely identification of common infrastructure shortfalls and single points of infrastructure, business, and community failure, and will speed implementation of corrective capacities.

- RBIS will highlight infrastructure capacities and distinctions between American communities. This will reduce assumptions and the temptation to apply less than optimal "cookie-cutter" solutions. A Coast Guard adage is operative: "When you have seen one port—you have seen one port." The same applies to American communities and the deltas between their critical infrastructure capabilities and performance requirements.

- RBIS coherently addresses infrastructure interdependency by both identifying and integrating infrastructure sector performance requirements where they naturally merge—in American communities.

- RBIS, leveraging Year 2000 (Y2K) Transition lessons learned, will build trust in government, promote national unity of effort, provide timely and actionable infrastructure situational awareness, and facilitate performance-based information exchange between infrastructure service providers and those inextricably reliant on them.

- Consistent with the President's June 14, 2014 call for a $1 billion investment in resilient infrastructures, RBIS will help to accurately inform the risk-based triage of, and provide for effective and efficient investment in, critical infrastructure innovation and resilient infrastructure capacity building.

- Because RBIS embraces a greater diversity of private sector entities/customers, there will be "eye-openers" in the questions posed. In the absence of capacities to address them in a timely, accurate, and actionable fashion, the questions will provide justification for program and budget initiatives that will translate into improved information collection and analytical

(Continued on Page 14)

(Continued from Page 13)

and information sharing capacities.

Because the Internet and the threats rapidly growing within it operate at the speed-of-light, cyberspace poses unique information sharing challenges. The successful defense of "America's Nervous System" (its Information Infrastructure) requires technologies that provide an advanced dimension in cybersecurity and resilience—Cyber Indications and Warning (CI&W).

Private sector developed, patented, and operationally proven CI&W technologies that match the pace of Internet operation exist. The technologies are compatible with all current and projected network defense technologies. They identify and neutralize all forms of malware (to include Advanced Persistent Threats) and anomalous Internet activity directed at any network simultaneously on all 56,535 Windows Operating Ports. Because the technology captures inbound Internet traffic "in the wild" (before reaching a network's Internet Point of Presence), it does not jeopardize network accreditation and, at the network owner's option, can provide instantaneous threat warnings and cyber defense system updates to any entity without risk to privacy or proprietary information. When integrated with current cyber information sharing mechanisms, CI&W technologies will dramatically improve the scope, timeliness, and effectiveness of America's cybersecurity and related information sharing efforts.

In sum: in a world where what could be described as an *Opportune Axis* of nations, non-state actors, terrorists, and cyber predators are mapping and planning to use America's infrastructures as a vector for inflicting consequences unprecedented in scope, intensity, and duration. Assuming critical infrastructure availability is a decidedly perilous mindset. RBIS and CI&W technologies provide the means to significantly advance the delivery of timely, accurate, and actionable information to infrastructure providers and their high-value and potentially high-consequence Private Sector customers. In the process of doing so, RBIS and CI&W will:

- Build trust with the Private Sector.
- Provide better understanding of business and community infrastructure performance requirements throughout the nation.
- Accelerate resolution of cross-sector infrastructure interdependency issues.
- Enable coherent investment in resilient cyber and physical critical infrastructures.
- Accelerate correction of the currently perilous preparedness trajectory of America's critical infrastructures.
- Preempt and/or predictably mitigate and accelerate recovery from critical infrastructure-enabled and/or amplified consequences.
- Provide a resilient infrastructure foundation to assure America's security, safety, quality of life, and future.

RBIS, CI&W, and Critical Infrastructure Resilience mindsets, metrics, methodologies, and technologies are readily available. All that is required to achieve the above is a decision to implement them.❖

** Jeff Gaynor is a nationally recognized resilience advocate, innovator, and practitioner having better than four decades of national and homeland security experience. Jeff directed the Homeland Security Advisory Council's (HSAC's) Critical Infrastructure Task Force and was a principal contributor to its Community Resilience Task Force. He is the President of the InfraGard Atlanta Member's Alliance—the FBI's public-private infrastructure preparedness partnership—and is a retired US Army Colonel and Defense Intelligence Agency Senior Executive who directed DoD Year 2000 (Y2K) Operations and served as the Communications Security Officer and as an Alternate Military Aide to Presidents Ronald Reagan and George H. W. Bush.*

Protected Critical Infrastructure Information's Success in the Courts

by David M. Willey*

Suppose your private company operates a large facility providing a critical resource such as water or electricity. You are concerned about protecting your facility from a variety of threats and hazards. You consider reaching out to the U.S. Government but, when you discuss it with your company's general counsel, there are significant issues. Your general counsel informs you that any security information you pass on to the U.S. Government might be disclosed to the public through information access laws such as the Freedom of Information Act or that your information could be passed on to federal regulators who may use it as a basis for new regulation or penalties against your company. Then your general counsel talks about the possibility of civil action litigants acquiring this sensitive information through the legal discovery process.

Why would a company voluntarily provide sensitive information about its infrastructure when there are so many concerns? After the terrorist attacks of September 11, 2001, Congress passed the Critical Infrastructure Information Act (CII Act) of 2002[1] which created the Protected Critical Infrastructure Information (PCII) Program and addressed the concerns of private industry sharing critical infrastructure information (CII) with the federal government. Although the CII Act was enacted primarily in response to terrorist threats, it has since evolved to address five hazards: acts of terrorism, cyber threats, accidents and technical failures, extreme weather, and pandemics. The PCII Program allows infrastructure owners and operators to voluntarily provide security and resilience information about their infrastructure through appropriate channels to the Department of Homeland Security (DHS) or other federal entities, enabling effective collaboration. In exchange for voluntary submission, the government guarantees that the submitted information will be used only for appropriate homeland security purposes.[2] The CII Act also explicitly prohibits PCII disclosure to the public through federal or state information access laws,[3] as well as its use in regulatory proceedings[4] or third party litigation.[5]

The real value of the PCII Program is that it facilitates the secure collection of infrastructure information, allowing DHS to build a comprehensive picture of infrastructure systems, identify critical dependencies and nodes, and compare individual facilities against an entire sector. Additionally, without the PCII Program, it would be difficult for the federal government to provide advice and assistance to private industry regarding infrastructure security and resilience. The Program has proven to be a robust mechanism for building partnerships between DHS and the private sector.

In practice, information can become PCII through two mechanisms. First, an owner or operator may submit CII directly to the PCII Program office for validation. Second, and more common, PCII is collected as a part of an approved program such as the Enhanced Critical Infrastructure Protection (ECIP) initiative conducted by DHS Protective Security Advisors. Properly submitted information that meets the definition of CII[6] becomes validated and protected as PCII.

Though the PCII Program has received limited attention in federal and state courts, the attention it has received affirmed the protections of valid PCII for privately owned infrastructure. The PCII Program received its first introduction to

(Continued on Page 16)

[1] Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 – 134 (2002).

[2] Code of Federal Regulations, Disclosure of Protected Critical Infrastructure Information, title 6, sec. 29.8(d).

[3] Homeland Security Act of 2002, 6 U.S.C. §§ 214(a)(1)(A), 214(a)(1)(E)(i) (2002); Code of Federal Regulations, Disclosure of Protected Critical Infrastructure Information, title 6, sec. 29.8(g).

[4] Code of Federal Regulations, Permissive Inspection, title 7, sec. 29.39(b).

[5] Homeland Security Act of 2002, 6 U.S.C. § 214(a)(1)(C) (2002); Code of Federal Regulations, Disclosure of Protected Critical Infrastructure Information, title 6, sec. 29.8(i).

[6] Homeland Security Act of 2002, 6 U.S.C. § 212(3) (2002).

(Continued from Page 15)

the courts in 2005 in the administrative law case *Robert Tombs v. Brick Township Municipal Utilities Authority*, OAL DKT. NO. GRC 06786-04S. The petitioner filed a request under New Jersey's Open Public Records Act, N.J.S.A. 47:1A, et seq., seeking a digital copy format of geospatial information system (GIS) topographic mapping data from the Brick Municipal Utilities Authority (MUA). The Brick MUA used the GIS data primarily for property tax assessment, but digital data had been previously submitted and validated as PCII. In 2006 a New Jersey appellate court upheld the Office of Administrative Law's Initial Decision that the digital copy format of the GIS data was protected from disclosure due to its PCII status.[7]

In contrast to the Tombs case, the 2009 case of *County of Santa Clara v. The Superior Court of Santa Clara County*, No. H031658, 09 C.D.O.S. 1526, 2009 DJDAR 1802, provides an alternative interpretation of the CII Act and PCII. The Court of Appeal in California's Sixth Appellate District upheld the lower court's decision that the County of Santa Clara must provide GIS data to the requestor through the California Public Records Act (CPRA) even though the data had been validated as PCII. In the decision, the appellate court found that the County of Santa Clara was the submitter of PCII, not the recipient, and ruled that the prohibition of PCII disclosure under CPRA applied to government *recipients*, not *submitters*, of PCII. Consequently, the county could not rely upon the data's PCII status to withhold it from disclosure. The court acknowledged that the CII Act preempted the CPRA and, had the county been the recipient of PCII, it would not have been required to disclose the GIS data. Although this ruling creates a wrinkle for California government PCII submitters, the appellate court nonetheless upheld the CII Act's preemption of the CPRA for California government recipients of PCII.

Most recently, in the 2013 case of *Murphy v. Ellman Capital Corporation*, CV 2011-070394, the plaintiff sought to subpoena documents from a municipal government in Arizona to support a negligence case against the owners and operators of a stadium complex. The information had been submitted and validated as PCII and received by the municipality. In the evidentiary hearing, the Superior Court found that the documents were exempt from disclosure pursuant to the CII Act.

Examined as a whole, the courts have upheld the prohibition of disclosure of PCII through information access laws and in third-party litigation. Even considering *County of Santa Clara*, no court has required the disclosure of information that has been submitted by a private entity and validated as PCII. In the context of PCII, critical infrastructure owners and operators will continue to have meaningful partnerships with the federal government and confidence in the ability of the PCII program to protect sensitive critical infrastructure data shared with the federal government.

** David M. Willey is a graduate of the University of Pittsburgh School of Law and has experience analyzing the infrastructure of southern Iraq for United States Forces-Iraq. He is currently an analyst with the Protected Critical Infrastructure Information Program Office within the Office of Infrastructure Protection, Department of Homeland Security.*

Disclaimer: The thoughts, opinions, and conclusions expressed in this article are the author's, and do not necessarily represent those of the United States Government or the Department of Homeland Security.

[7] *Tombs v. Brick Township Municipal Utilities Authority*, Docket No. A-3837-05T5 (N.J. Super. Ct. App. Div. 2006).

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1