

2014 IDGA Homeland Security Conference after-action report

Using new tools to respond to evolving threats



Contents

3	Note from the authors
4	Executive Summary
5	The changing threat landscape
6	Driving solutions into the field
8	Navigating the data stream
9	Partnering with the Private Sector
10	Conclusion
11	Works cited
12	Authors



Note from the authors

This After-Action Report serves as a summary of the key takeaways from the Institute for Defense and Government Advancement (IDGA) 2014 Homeland Security Week Conference. Now in its fourth year, the Homeland Security Conference took place in Washington, D.C. on October 6-9, 2014 and brought together hundreds of homeland security stakeholders from across government, the private sector, academia and non-profits.


This report includes quotations and statistics from speakers at the Conference and key themes across their presentations. The authors would like to thank IDGA for hosting the Conference and putting together a valuable and collaborative event that informs discussion on the homeland security mission.



Executive Summary

Since its creation in November 2002, The Department of Homeland Security (DHS) has navigated evolving mission requirements, changing regulatory oversight and constant public scrutiny across its components. As the world's largest law enforcement organization, DHS is responsible for protecting the United States and its territories from a broad array of threats.

At the 2014 IDGA Homeland Security Conference, stakeholders from the public and private sector highlighted four key takeaways on where the Department is headed and the challenges it will need to tackle in the coming years:





Today, the Department faces increasingly sophisticated and complex threats.

Drug cartels and terrorist organizations are coordinated multinational enterprises. Cybersecurity actors are more patient and can conduct "Zero Day" encrypted attacks that are hard to trace and harder to predict. Insider threats can wittingly or unwittingly leak proprietary data or government classified information. These individuals and groups operate across multiple borders and jurisdictions, challenging the way that law enforcement organizations traditionally operate.

Yet, DHS must concurrently handle both funding uncertainties and greater Congressional oversight.

In this threat environment, DHS is also facing constrained budgets due to current political pressures. At the same time, due to the legacy oversight relationships of DHS components, over 120 committees, sub-committees and other congressional bodies have some jurisdiction over DHS.¹




As a result, DHS must innovate to address the evolving threat environment.

As Customs and Border Protection Chief Technology Officer Wolf Tombe has said, "If we don't stay innovative, we could lose so much ground in one year that it would be hard to catch up." Agencies are using tools such as sensor technology, biometric recognition, and predictive data analysis in the field to drive mission performance and combat threats.

And in an environment of "do more with less," DHS cannot do it alone.

The Department is relying on the private sector to provide technology solutions, industry leading practices and information sharing to address its most pressing mission needs. In some cases, the government is entering Public-Private Partnerships (PPPs) with industry organizations, particularly in order to protect critical infrastructure and mitigate insider threats. However, concerns still remain on both sides on how to best share information that is in the public interest while maintaining companies' proprietary data.



The changing threat landscape

DHS is confronting evolving, sophisticated threats that have continued to grow in complexity since the Department's inception.

Ebola. ISIS. Unaccompanied migrant children. Wikileaks. Today's national security threats are fluid, cross-border and diverse. Accordingly, these threats fundamentally challenge our existing emergency response and preparedness systems and understanding of the responsibilities of national security agencies. In its 2012–2016 Strategic Plan, the U.S. Department of Homeland Security (DHS) outlines five mission goals that seek to address these challenges across the homeland security enterprise.² These mission goals provide both tactical objectives and investment priorities for DHS in the near-term and are increasingly relevant in light of emerging threats. National security agencies — DHS among others — should alter their traditional way of doing business to proactively address the changing threat landscape and continue to fulfill their mission. As DHS faces new mission challenges across the enterprise, the Department is looking at technological solutions that can enhance capabilities and respond proactively to secure the homeland.

If we don't stay innovative, we could lose so much ground in one year that it would be hard to catch up.

Wolf Tombe, CBP Chief Technology Officer

Five Mission Goals of the U.S. Department of Homeland Security Strategic Plan for Fiscal Years 2012–2016

- 1 Preventing Terrorism and Enhancing Security
- 2 Securing and Managing Our Borders
- 3 Enforcing and Administering Our Immigration Laws
- 4 Safeguarding and Securing Cyberspace
- 5 Ensuring Resilience to Disasters

As described at the Homeland Security Conference, by **Wolf Tombe**, Chief Technology Officer of U.S. Customs and Border Protection (CBP), the shift from traditional to emerging threats “requires DHS to be more agile and to take a proactive rather than reactive approach” to national security.³ One example of these emerging threats is the recent increase in targeted one-off attacks led by well-organized and well-funded adversaries such as ISIS who are motivated by their nation-state identity. Previously, threats were assumed to be widespread and global, with identifiable signatures that allowed national security agencies to effectively track and prevent these attacks (See Figure 1).

This rapidly changing threat landscape directly challenges the current capabilities of national security agencies. In addition, growing Congressional oversight and declining budgets have imposed the imperative of doing more with less across the federal government. The resulting imbalance of rising threats and fewer resources compel national security agencies to reimagine their traditional approach and seek out innovative solutions. “If we don't stay innovative,” explains Mr. Tombe, “We could lose so much ground in one year that it would be hard to catch up.”⁴

Figure 1: Changing Landscape of National Security Threats

Traditional threat	Emerging threat
Widespread and global	Targeted threats, as increased knowledge informs our adversaries
Repeatable	“One of a kind, zero day” attacks are targeted towards one specific industry or market
Financially-motivated	Nation-state actors or national identity driven espionage have increased the scale and complexities of attacks
Malware	Sophisticated, well-funded attackers, malware SDKs
Organized crime	Highly innovative drug cartels demonstrate how organized crime is now acting like a business
Physical threats	Sophisticated engineering of new chemical, biological weapons, as new designer drugs to avoid laws and circumvent scanners
Unencrypted threats	Encrypted threats disadvantage border security agencies as they aren't readily detectable by existing technology

Driving solutions into the field

DHS is evolving to gather data and enhance situational awareness in the field

New technology solutions deployed across DHS, state, and local law enforcement agencies have enabled the government to be more nimble in addressing evolving threats. In this section are examples cited at the Homeland Security Conference of evolving biometric, sensor, and mobile technology already in use at the Department. These solutions enable data driven decision making, increase situational awareness, and expedite response time in the field.

Biometrics

DHS, state and local law enforcement organizations are collecting and analyzing biometric data to drive mission impact. Biometrics are a less intrusive, more effective method of identity verification and enable more immediate decision making in the field. The increased use of biometrics at points of entry has the potential to help Customs and Border Protection (CBP) expedite traveler screening at US entry points and confirm when a specific foreign national has departed the country. CBP is currently exploring iris recognition biometrics to enable accurate identification of foreign nationals departing the country and provide real-time data on individuals with invalid visas.

The Office of Biometric Identification Management (OBIM) already provides enterprise-level biometric information to its customers, which include over eight DHS components, multiple federal agencies, State & Local enforcement, the intelligence community, and international partners. OBIM serves its customers by matching, storing, sharing, and analyzing biometric data. As a result, both the demand for, and expectations of, OBIM's systems are high. For example, OBIM's systems are expected to verify a person's identity and ensure that the person is not one of the 7.2 million suspected terrorists on the Terrorist Watch List, all within a span of 10 seconds.⁵

As **Patrick Nemeth**, head of the Identity Operations Division at OBIM, observed at the Homeland Security Conference, IDENT has more than one hundred seventy-five million unique identities stored in the system, and the biometric watchlist has about 8.6M unique identities on it. Daily biometric transactions are over 300,000 per day.⁶ OBIM, like other organizations that support law enforcement, should maintain this level of mission performance despite shrinking budgets. OBIM Acting Director **Shonnie Lyon** summarized the current status as,

"The demand for our services is increasing. How do we do that with the current systems we have and funding we have?"⁷

OBIM's systems are expected to verify a person's identity and ensure that the person is not one of the 7.2 million suspected terrorists on the Terrorist Watch List, all within a span of 10 seconds.

Sensors

Sensors are another potential game-changing capability for law enforcement. Sensors are mechanical devices sensitive to light, temperature, or radiation level that transmit a signal to a measuring or control instrument. A sensor can be installed on personnel's clothing or wristwatches as a "wearable" sensor, suspended on a tower at the border, or in the air on a drone.

Regardless of where they are installed, sensors provide border agents and law enforcement personnel with an enhanced ability to gather asset intelligence on the border. Reports state that "Already, some of CBP's 58,000 person workforce uses various smart wrist-watches, wearable cameras, and clothing equipped with health and safety sensors, improving both effectiveness and safety for border agents in the field."⁸ In addition, sensors on drones and integrated fixed towers on the border can pinpoint locations using geospatial data analysis programs. At the Conference, **Michael Fisher**, Chief of US Border Patrol, explained that this geospatial intelligence is a key indicator for Border Patrol when measuring risks and strategically targeting criminal networks.

[Border security] doesn't work if you only assume that 'if you arrest more people it'll change.' It's about infiltrating the networks.

Michael Fisher, Chief of US Border Patrol

Mobile Technology

Mobile technologies further enable law enforcement personnel to manage threats adeptly. At the Homeland Security Conference, multiple speakers advocated for the need to extend data-driven decision making to the field. This requires law enforcement agencies to deploy mobile capabilities to their workforce. In order to do this, mobile devices should be able to receive and transmit data across a wireless network that is both secure and resilient. Through this network, law enforcement personnel could transmit information seamlessly from anywhere, to anyone. As a result, people rather than hardware, would become the network access point.

Furthermore, mobile technologies can instantaneously notify agents and/or respondents of a robbery, natural disaster, or imminent terrorist attack, and communicate necessary protocol to the user with the notification. As **Bill Eggers** lays out in a recent publication on wearables, "Imagine...What if employees could have specific instructions for those procedures delivered at the point of impact?"⁹ Reaction time could improve significantly, and users would have increased situational awareness at the site of the incident. Mr. Eggers cites the response to the 2010 earthquake in Haiti an example of the power of mobile technology delivering information at the point of impact:

When a 2010 earthquake wreaked havoc in Haiti...responders needed maps. Soon, a crowdsourced application developed by the NGOs Ushahidi and Humanitarian Open Street Map became the default tool for search and rescue teams. More than 600 volunteers traced roads and encampments from aerial images into a computer program. They mapped data from the World Bank, Yahoo!, and Japan's space agency. In support, the US military released P3 and GlobalHawk imagery.

Search and rescue groups could read the resulting maps from handheld GPS units. In the evolving disaster area, crowdsourced markers identified resources such as refugee camps and cholera response centers. Multiple nations, NGOs, volunteers, and ordinary Haitian citizens came together in an unprecedented way, sharing information to save lives.¹⁰

By delivering maps and critical information to responders on the ground, the crowdsourced mobile application increased the situational awareness of Haiti responders, allowing them to react quickly and effectively. Similarly, speakers at the Conference spoke of the need to equip law enforcement personnel with mobile solutions to allow them to react proactively to threats.



Navigating the data stream

Law Enforcement agencies are harnessing the potential of “big data” through information sharing

In addition, the Conference also provided a first-look at how law enforcement organizations are using big data to both respond and predict current and emerging threats. Biometric, sensor, and mobile technologies have the ability to collect mission-critical data, yet the data must be deciphered and put in context in order to drive mission impact. This is done by connecting disparate, high-volume datasets. An increasingly common example is information sharing between the thousands of stakeholders across local, state and federal law enforcement organization. As many threats and investigations cross jurisdictional boundaries, accessing and analyzing data across multiple levels is crucial for mission success.

The value created by information sharing across offices is evident in the creation of regional information sharing environments that bridge federal, state, and local institutions. These environments enable information acquisition, analysis, and dissemination across various law enforcement departments. One example cited at the Conference is **COPLINK**, which has been called “Google for police officers.”¹¹ COPLINK uses law enforcement data and analytics shared across jurisdictions. “COPLINK improves situational awareness for law enforcement officers by including ‘automated geospatial searches of recent events’ that draws on state and local criminal records from multiple jurisdictions’ databases.”¹² Information sharing environments such as COPLINK streamline and quicken the work of law enforcement personnel by aggregating distinct data sources during investigations.

The greatest value is when stakeholders are able to “connect the dots” and understand the big picture of threats the US faces. As **Mr. Tombe** explained, “the power of big data allows us an entry point into predictive analytics.” With the amount of data at the fingertips of law enforcement agencies comes the opportunity to use predictive analytics to model mission requirements, potential risk factors and justify resource needs. Mr. Tombe and others at the Conference made clear that while yesterday’s approach to countering threats was reactive, today’s approach should be proactive. As information sharing increases and new technology is implemented throughout the enterprise, predictive analytics can bridge the gap between a response plan and a data-driven mitigation strategy.

Predictive analytics can bridge the gap between a threat response plan and a data-driven mitigation strategy.



Partnering with the Private Sector

The Department is collaborating with Private-Sector Partners to protect critical infrastructure and mitigate insider threats

In a funding-constrained environment, the Department cannot fulfill its evolving mission requirements on its own. In order to perform key mission areas, the department has often engaged the private sector through Public-Private Partnerships (PPP). Typically, a PPP is a jointly-funded alliance between public and private entities with the stated goal of achieving a specific public mission. At the Homeland Security Conference, stakeholders shared how PPPs are specifically being used to protect critical infrastructure assets and thwart insider threats.

One example of this type of PPP in the Department is the Office of Infrastructure Protection (IP) Critical Infrastructure Protection and Resilience Program. The program is grounded on the principle that neither the government nor the private sector alone have the knowledge, authority or resources to protect critical infrastructure. IP has established working relationships with public and private sector partners in all fifty states and Puerto Rico, sharing information, maintaining communications with critical infrastructure owners and operators and coordinating response and recovery.¹²

In recent years, the focus in protecting critical infrastructure has been in securing assets from attacks via the Internet. Because power grids and public utilities often rely on broadband networks, they may be vulnerable to cyber-attacks. At the Conference, **Retired Brigadier General Gregory Touhill**, the Deputy Assistant Secretary for Cybersecurity Operations and Programs, explained that many US power grid technologies were built in the 1970s and consequently have not been tested for modern-day cyber-attacks. These vulnerabilities make this infrastructure a target for criminals and terrorist groups.

A shift has occurred, as entities are being more proactive and adopting risk-based approaches.

Michael Gelles, Director, Deloitte Consulting LLP

In February 2013, President Obama signed Executive Order 13,636, which outlined a national policy on how to protect critical infrastructure from cyber-attacks. Under the Executive Order, the National Institute of Standards and Technology (NIST) developed a Cybersecurity Framework which establishes leading practices to address cyber threats to critical infrastructure. The NIST Cybersecurity Framework was created through the input of private sector stakeholders and is another example of PPPs in action.

Likewise, the government and private sector are collaborating to mitigate insider threats within their own organizations. Insider threats can occur when an employee or contractor with access to government resources attempts to harm the security of the U.S. Particularly in response to the 2013 PRISM leaks, both companies and agencies are building insider threat programs to identify potential breaches and prevent them before they occur. According to **Dr. Michael Gelles**, Director at Deloitte Consulting LLP, "A shift has occurred, as entities are being more proactive and adopting more risk-based approaches." Organizations are looking for key indicators using behavioral data which can assess which individuals may be most likely to pose an insider threat. For example, in the aviation industry, analysts may study cell phone searches by staff working in and around aircraft. The government is aiding US businesses in mitigating insider threats by providing guidance and leading practices through the US Computer Emergency Readiness Team (US-CERT), led by DHS. In September 2014, US-CERT provided tactical recommendations to industry on preventing data breaches. This ongoing dialogue between industry and the government will continue to be necessary in order to protect public assets and secure classified or proprietary information.

Conclusion

Fundamentally, the Homeland Security Conference made clear that today's threat environment requires DHS to be an agile organization. In government, it is often difficult to iterate new solutions, test services and risk failing forward. However, the threats that DHS is responsible for mitigating and preventing are fluid and complex. As DHS continues to mature as an organization, it will be important to foster this agile approach to doing business.

This approach will entail many of the tools and strategies already being leveraged by the Department, such as mobile technologies in the field, data-driven decision making and public-private partnerships. By continuing to prioritize these efforts, DHS will be able to identify new opportunities and combat threats to the American homeland.



Works cited

1. Jerry Markon, "Department of Homeland Security has 120 Reasons to Want Streamlined Oversight", The Washington Post, September 25, 2014, <http://www.washingtonpost.com/blogs/federal-eye/wp/2014/09/25/outsized-congressional-oversight-weighing-down-department-of-homeland-security/>
2. Department of Homeland Security Strategic Plan, FY2012-2016, <http://www.dhs.gov/xlibrary/assets/dhs-strategic-plan-fy-2012-2016.pdf>
3. Wolf Tombe, Chief Technology Officer, CBP, Department of Homeland Security (DHS), "Addressing Future Threats and Enhancing Border Security Through Innovation"
4. Ibid
5. Nicole Blake Johnson, "DHS Office Emerges as Biometric Hub". Federal Times, November 5, 2013. <http://www.federaltimes.com/article/20131105/IT/311050008/DHS-office-emerges-biometrics-hub>
6. Patrick Nemeth, "OBIM Mission Update," October 7, 2014, Homeland Security Conference presentation
7. Ibid
8. Frank Conkel, "The Next Step in Securing the Border: FIDO and a Smart-Sensor Collar", Nextgov.com, October 7, 2014, <http://www.nextgov.com/emerging-tech/2014/10/next-step-securing-border-fido-and-his-smart-sensor-collar/95996/>
9. Shehryar Khan & Evangeline Marzec, "Wearables", DU Press, February 21, 2014. <http://dupress.com/articles/2014-tech-trends-wearables/>
10. William D. Eggers, Rob Hamill, & Abed Ali. "Data as the New Currency", DU Press, July 24, 2014, <http://dupress.com/articles/data-as-the-new-currency/>
11. "Now Under IBM, Coplink unveils new mobile app", Inside Tucson Business, October 28, 2011. http://www.insidetucsonbusiness.com/news/top_stories/now-under-ibm-coplink-unveils-new-mobile-app/article_469f5008-00ed-11e1-8729-001cc4c002e0.html
12. Ibid
13. Department of Homeland Security Critical Infrastructure Protection Partnerships and Information Sharing, <http://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing>

Authors

Robert Jacksta

Specialist Leader

Deloitte Consulting LLP

Arjun Verma

Consultant

Deloitte Consulting LLP

Danielle Melfi

Business Analyst

Deloitte Consulting LLP

Bo Swindell

Business Analyst

Deloitte Consulting, LLP

Adam Robbins

Consultant

Deloitte Consulting LLP

For more information on IDGA, contact:**Brittany Hicks**

P: +1 212 885 2756

E: Brittany.Hicks@idga.org

About Deloitte

This publication contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.