Mark Ghilarducci

Director, Governor's Office of Emergency Services Governor's Homeland Security Advisor
State of California
Chair, Response & Recovery Committee, National Emergency Management Association

STATEMENT FOR THE RECORD
On behalf of the
National Emergency Management Association

Submitted to the House Homeland Security Committee

United States House of Representatives

Enhancing Preparedness and Response Capabilities to Address Cyber Threats

May 24, 2016

National Emergency Management Association
444 N Capitol Street, NW, Suite 401
Washington, D.C. 20001
202-624-5459

Introduction

Thank you Mr. Chairman, Ranking Member and distinguished members of the Committee. My name is Mark Ghilarducci, and I am the Director of the Governor's Office of Emergency Services as well as the Homeland Security Advisor to Governor Jerry Brown for the State of California.

I am here on behalf of the National Emergency Management Association (NEMA), which represents the emergency management directors of the 50 states, territories, and District of Columbia. NEMA's members, many of whom, like me, also serve as Homeland Security Advisors, are prepared to deal with an ever changing and increasingly complex set of challenges that test traditional approaches to natural and manmade disasters. I appreciate the chance to come before you today to discuss the current concerns related to consequences of cyber-attacks and the role of the emergency management community in responding to these unique events.

Where Are We Now?

We are witnessing a more diverse array of threats than at any other time in history. The skill, speed, and adaptability of these threats are challenging our defense in ways we have not seen before. The emerging threat landscape for the nation is characterized both by standing threats, as well as dynamic and fluid ones ushered in by advancements in technology. As we witness our society make unprecedented advancements in innovation, we become more and more reliant on information technology and increasingly vulnerable to devices that are developed and distributed with minimal security requirements. The ranges of threat actors, methods of attack, targeted systems, and victims are also expanding.

We are transitioning into Next Generation Public Safety, and information systems are now the backbone of national and economic security in the United States. Our success as a nation depends upon critical infrastructure functioning reliably at all times. The threat to this infrastructure by those with malicious intent to exploit vulnerabilities, steal information and money, and disrupt, destroy, or threaten the delivery of essential services are unlike any other. Cybersecurity threats exploit the risks associated with the increased complexity and connectivity of these systems, which places our nation's security, economy and public safety at greater risk.

This risk affects both the private and public sectors. We have seen 'Ransomware' in the public and private sector in California and across the United States designed to prevent public and private institutions from accessing their own data. Criminal tools and malware are increasingly being discovered on state and local government networks.

As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-impact events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. Long-term power outages, loss of water, and disruption in the movement of goods, services and people as a result of disrupted transportation systems are a few of the potential consequences of a successful cyber-attack on our critical infrastructure.

The aftermath of a cyber event with physical consequences will challenge existing hierarchies, reporting structures, and planning assumptions. In the event of an incident, most emergency managers will turn to the Robert T. Stafford Disaster Relief and Emergency Assistance Act (PL 92-288) for federal assistance, but unless the consequences of a cyber-attack have large scale physical consequences, funds from the Stafford Act will be limited.

Many of the fixes, whether administrative or legislatively initiated, throughout the last few years seem to only address the prevention and preparedness side of cybersecurity. While the pre-event aspects of cybersecurity maintain a high level of importance, so too will the post-event considerations especially when considering the potential disastrous physical consequences of a cyber-attack.

Current Challenges Facing State Emergency Management/Homeland Security

While cybersecurity and cyber response capabilities continually rate very low in FEMA's annual National Preparedness Report, identifying the capability gaps and needs is often a difficult task for state and local government and has limited measurable improvement toward the National Preparedness Goal.

- Cyber risk must be managed as it is not possible to eliminate; the diverse possibilities of malicious actors penetrating, intruding, and circumventing from the inside continue to grow and will hold every Internet communication technology system at risk for years to come.

- The risk calculus employed by some state and local organizations does not adequately address the top cyber threats or systemic interdependencies across critical infrastructure sectors.

- State leaders must accept the predictability of cyber-attacks, and build security systems and procedures that can not only preempt attacks through cyber defense, but enable organizations to withstand attacks when they succeed, or in other words build cyber resilience.

- A coordinated approach to cybersecurity preparedness and incident response is in its nascent stages, even at the federal level. As the federal government is still working to build federal institutions, policy, and strategy, it has left states to build cybersecurity capacities with limited resources and trained personnel, and a lack of guidance or successful blueprint to follow—all while facing threat actors who are advanced, nimble, quick to adapt and overcome defenses and who intend to harm private citizens and government services.

- A dedicated cybersecurity grant funding stream would also ensure states were prepared to adequately build their cyber capabilities and defenses. Currently there is no funding dedicated specifically to this priority.

- States are still playing catch-up in developing a "whole of government," statewide approach to cybersecurity.

Best Practices at the State Level/Ongoing Efforts to Improve Resilience

I am excited to discuss some California examples of best practices we are implementing to ensure the Golden State is safe and secure and cyber resilient.

- ***Cyber Hygiene Partnership with DHS' National Cybersecurity Communications Integration Center (NCCIC)***: We are moving to embrace and implement the DHS' National Cybersecurity Communications Integration Center's Cyber Hygiene campaign across California State Agencies. Working with NCCIC staff, we are working to push this program to all of California's state executive agencies as a start. This program is voluntary, but it will allow us to baseline state agencies' vulnerabilities and provide an overall state profile for a majority of public facing assets. This is a good metric for performance and will help our team develop a long-term state strategy. To date, only thirteen organizations across all of California are taking advantage of this federal program.

- ***Integrating and Automating Data Feeds***: One of the things we are spearheading in California is a Cal OES-supported project at our California fusion centers that supports automating cyber threat intelligence, as we believe that is a fundamental facet to cyber resilience on all levels of government. We must get past the manual human-to-human transactions that continue to dominate state and local cyber information-sharing and move towards an automated cyber threat intelligence design, which we believe should anchor states' resilience and inform cyber response efforts. We are also working, in conjunction with DHS/NCCIC, on a program called Automated Indicator Sharing Initiative, which shares observable cyber "indicators" to also help bolster the state's defense through a machine indicator exchange.

- ***California Cybersecurity Integration Center (Cal-CSIC)*****:** We recently stood up our California Cybersecurity Integration Center (Cal-CSIC) (pronounced Cal-SICK) as a way to mature this approach, but one of the biggest challenges we face is establishing a blueprint for integrating disparate efforts and mission sets into a unified, coordinated and streamlined operation that reflects the full intelligence cycle from collection, analysis to dissemination, and that supports a robust cyber response.

  The Cal-CSIC does the following critical cybersecurity functions, directly impacting my ability to manage both the homeland security and emergency management portfolios in California:

  - Expands upon current capabilities in our state's primary fusion center to build out a cybersecurity center focused specifically on protecting California.

  - Resides within the Cal OES Homeland Security Division, aligning with DHS's organizational structure.

  - Its co-location with the California State Threat Assessment Center (STAC) allows for communications to be properly vetted and classified, ensuring connectivity between the intelligence community, law enforcement and fusion centers.

  - Provides a statewide nexus for cyber threat information sharing for the State of California, intelligence community, and law enforcement.

  - Promotes situational awareness of cyber threats, cyber hygiene, and best cybersecurity practices for all California organizations.

  - Augments the State Operations Center activities during emergency incidents through media analysis and resilient communications.

  - Marries our critical infrastructure analysts and assessors to our cybersecurity professionals to create a novel holistic security assessments capability.

  The National Cybersecurity Communications Integration Center (NCICC) and Multi-State Information Sharing Analysis Center (MS-ISAC) operate as focal points for cyber and physical protection of federal, state, local, tribal, territorial government (FSLTT) and Critical Infrastructure/Key Resources (CI/KR) network, storage and communications systems and seeks to address prevention, protection, response and recovery.

  The Cal-CSIC will address prevention, protection, response and recovery while providing detail on cyber threats and trends specifically to California. The Cal-CSIC can use this analysis to notify residents of current threats and how to prevent and mitigate those threats. The consolidation of national and state cyber threat data will provide a more strategic picture benefitting prevention and response. The NCCIC will also be a partner in the Cal-CSIC as will other federal agencies to ensure for real-time collaboration and coordination that is needed.

  The Cal-CSIC design forces collaboration between all of the major state agencies that have a role in cybersecurity because those agencies have, or are going to, embed their cybersecurity staff there. This partnership will force down the siloes and stove pipes, and generate a level of collaboration on the cyber front not seen before in state government, which helps to define the roles and responsibilities of each agency during cyber events of statewide significance.

- ***Governor's Cybersecurity Task Force:*** This task force facilitates cybersecurity outreach to private industry, academic, law enforcement, and government partners both inside and outside of California. The Governor's Cybersecurity Task Force is a public-private partnership that serves as the advisory body to the Cal-CSIC to raise awareness of new threats and mitigation techniques.

  Sometimes, simply assembling the right players to have the tough conversations is half the battle. In this case, educating cybersecurity professionals about emergency management, and vice versa, remains a significant challenge. This is why the State of California created the Governor's Cybersecurity Task Force to be wide-reaching, pairing up local emergency management experts with cybersecurity professionals to collaborate on the bigger strategic questions. It has made a tremendous impact, but more work needs to be done to align state and local defense with federal efforts.

Recommendations for the Future

As a nation we must map out a comprehensive collaborative strategy that delivers timely, cost effective, and actionable responses. This will strengthen our national security by better preparing us to respond to potential disruptions that would have cascading consequences on the country. Collaboration, employee cybersecurity training, enterprise defense-in-depth, and real-time information sharing and processing of indicators of attacks are essential elements of a robust cybersecurity posture for all governments. Marrying critical infrastructure assessors and analysts with cybersecurity personnel also will breed unique and nuanced synergies by approaching the problem holistically. This would include:

- Review current statutory authorities for emergency management personnel and ensure resources can and will be available to respond to a cyber-attack.

- Encourage information sharing between intelligence and operational officials to ensure stovepipes do not unnecessarily hinder collaboration and integrated planning.

- Coordinate with state and local officials to ensure their priorities are included in legislative reforms and changes within the Administration’s cybersecurity policies.

- Avoid mandating state and local governments without also providing federal funding.

- Provide adequate and sustainable funding to ensure for the development of robust cyber security interdiction, response and preparedness/education systems at the state and local levels, to better inform and empower communities, where the consequences of cyber attacks are most impactful.

- Ensure that we communicate to American citizens our commitment to protecting their privacy, when incorporating emerging technology—specifically, the Internet of Things or ‘smart devices’.

While these devices maximize efficiency and carry the allure of convenience, we must incorporate the benefits of innovative technology into state and local government with the utmost appreciation for their potential to threaten data privacy, data integrity or continuation of services. This also opens vulnerabilities by allowing threat actors to not only steal data, but also, manipulate it. Threat actors almost certainly will adapt and introduce new tactics that will challenge our defenses so we must seize the opportunities to implant past intelligence from cybersecurity investigations back into the intelligence cycle for further analysis and dissemination.

Conclusion

At all levels, government must be prepared to deal with an ever changing and increasingly complex set of challenges that test our traditional approaches to emergency preparedness and responses to disaster. Capability, experience and flexibility are critical in dealing with emerging issues and the unknown. Changing demographics, emerging technologies, and the interdependencies of our infrastructure and systems create vulnerabilities that differ from those of the past. The cyber threats facing our nation are evolving in such a way that demands purposeful action and a more forward-thinking approach in our national preparedness efforts.

I appreciate the opportunity to testify before you today and stand ready to answer any questions the Committee may have.

Thank you.