Guiding Principles for Emergency Management on Cybersecurity

NEMA Homeland Security Committee
October 2020

The confluence of COVID-19, election security, and the resultant exponential increase in bandwidth demand and the proliferation of IT solutions from teleworking has catapulted cybersecurity to the forefront of national security discussions with a new urgency. The cascading impacts of a cybersecurity incident during the COVID-19 response have reinforced the need to ensure state government enterprises are secure and resilient in the face of cyber threats. To that end, the National Emergency Management Association (NEMA), the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS CISA), and Auburn University's McCrary Institute partnered to develop a document that outlines guiding principles for emergency management executives around cybersecurity. CISA, the lead federal agency in this effort, also continues to aggressively highlight the critical importance of cybersecurity and provides many valuable resources for state, local, tribal, and territorial (SLTT) governments and private organizations. In creating this document, we consulted their Cyber Essentials Toolkit[1], as well as the resource centers of partner organizations such as the National Governors Association (NGA)[2] and National Association of State Chief Information Officers (NASCIO)[3].

When considering the enterprise-level threat posed by a cyber incident, leadership is a critical element of risk mitigation. As such, this document (and the CISA Cyber Toolkit) channel leadership development theory: know yourself to lead yourself, lead yourself to lead others, and know the team to lead the team. These documents contextualize the *leadership trinity* within its essential elements: leadership, culture, and strategy.

LEADERSHIP

Leadership is arguably the most critical component in developing the foundation for a robust cybersecurity program and culture. One of the first steps to creating a successful program and culture is understanding and communicating cyber as a significant risk to the enterprise. Embracing this mentality and then ingraining it into culture and strategy is key, as successful emergency management operations in other areas of work are dependent on effective risk assessments and communications. Most, if not all, of our communications and data ride on our networks. A cyber incident at the wrong time could have devastating impacts on life and property for the residents we serve.

Amidst all of the competition for limited time and funding, leaders are responsible for developing and driving a strategy that includes investments in cybersecurity focused both on technology (hardware and software) and training and education (awareness) to create a mutually reinforcing partnership between staff and technology. While emergency management leaders do not always come to cybersecurity with technical expertise, they can leverage experience with other incidents to ask the right questions when planning for incident response and then surround themselves with a highly capable team empowered to operationalize and message the cybersecurity strategy and priorities.

Emergency management prides itself on its ability to convene and build partnerships. At the state executive level, tap into the expertise provided by leaders including your state Chief Information Officer (CIO), Chief Information Security Officer (CISO), and Homeland Security Advisor (HSA) to prevent stove-piped cybersecurity

[1] Cyber Essentials Toolkits. (2020). Retrieved from https://www.cisa.gov/publication/cyber-essentials-toolkits
[2] Resource Center for State Cybersecurity. (n.d.). Retrieved from https://www.nga.org/bestpractices/divisions/hsps/statecyber/
[3] Resource Center. (2020, June 10). Retrieved from https://www.nascio.org/resource-center/

initiatives as these may leave gaps of vulnerability that malicious actors can exploit. Work with these and other stakeholders, including local governments, critical infrastructure, and the private sector as you build emergency management-centric cyber response plans. There are currently 26 examples at the state level with governors and legislators creating commissions, task forces, teams or advisory councils and boards to accomplish this task[4].

One such example is Louisiana. In 2017, Louisiana Governor John Bel Edwards established the Louisiana CyberSecurity Commission via Executive Order to address cyber threats through partnerships between state and local government, institutes of higher education, the federal sector in the state, and the private sector[5]. The process also resulted in the state creating an Emergency Support Function (ESF) dedicated to cybersecurity responses ("ESF-17"). When school districts in Louisiana were attacked in 2019 the state leveraged the ESF to respond and investigate the incident.

The inherent paradox of cybersecurity is that humans are the first line of defense, but are also the threat and the vulnerability, in addition to the perpetrator. These bad actors leverage human biases that make us incredibly susceptible to phishing and social engineering attacks to access systems. Although IT solutions are an important component to protecting networks and data, humans remain a critical component to effective cybersecurity. For that reason, leaders must develop baseline cybersecurity procedures and policies that are well understood by employees and stakeholders to drive behaviors and habits that build a robust cybersecurity culture. Here are a few programs, policies and procedures you can implement as appropriate to your needs[6]:

- Every employee must pass mandatory cyber training prior to earning access to the network;
- Employees sign a cybersecurity policy to demonstrate a commitment to the requirements and personal accountability;
- Conduct aggressive and sophisticated phishing campaigns with metrics, accountability and retraining; and
- Leaders model the cybersecurity behavior and mindset expected of all employees.

Lastly, regardless of whether you own and operate your network or your operations ride on someone else's network, you are responsible to make sure it meets the minimum requirements of reliability and security. Although this may slightly change operations, here are simple steps a leader should take to enhance cybersecurity posture[7]:

- Inquire about updates to operating systems and third-party software and implement automatic updates where possible;
- Employ secure configurations and remove unsupported and unauthorized hardware/software; and
- Implement email and web browser security settings.

CULTURE

With finite resources, it is critical to drive toward a resilient system with the capacity to resume operations quickly. To ensure this rapid restoration of services and ability to charge back amid challenge, plans must be in

[4] Greenberg, P. (n.d.). National Conference of State Legislatures Statewide Cybersecurity Task Forces. Retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/statewide-cybersecurity-task-forces636129887.aspx
[5] Exec. Order No. 17-31 Louisiana Cybersecurity Commission. (2017, December 6). Retrieved from https://lacybercommission.la.gov/wp-content/uploads/2018/07/Governors-Louisiana-Cybersecurity-Commission-Executive-Order-17-31.pdf
[6] Cyber Essentials Toolkit. Essential Element: Your Staff, The Users. (2020). Retrieved from https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Toolkit%202%2020200701.pdf
[7] Cyber Essentials Toolkit. Essential Element: Your Systems. (2020). Retrieved from https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Toolkit%203%2020200806_508.pdf

place to support continuity of operations so that if one system fails, the other mitigates the consequences. Depending on the enterprise, this could mean retaining the capacity to perform key functions manually should operations online become compromised. Hope is not a substitute for strategy, so leaders must deliberately drive a culture that builds in system resilience to be more capable of responding to and overcoming cyber incidents.

This requires transitioning from a security culture that is reactive to one that is proactive. The threat environment is ever-changing and therefore implementing a risk management program that is designed to address potential vulnerabilities is critical, especially when the state is undergoing IT modernization or consolidation. Coupling this with a vulnerabilities management program and controls management to define policies and processes required for the safe delivery of data and program elements while analyzing the security system's effectiveness, also reinforces a culture that is prepared for intrusive attempts to infiltrate enterprise systems. Understanding, transferring, mitigating, and accepting risk is key to maturing a cyber program.

Building security in from the start is always preferable to retrofitting it after an incident occurs. An effective training and awareness program to ensure that everyone is capable and understands their role in the security program is another piece of the resilience jigsaw puzzle. A good training and awareness program will address formal and informal education requirements for roles and responsibilities for all security programs. Establishing a strong training and awareness program for emergency management is crucial, but it is equally important to provide opportunities for IT to understand emergency management so that they too are prepared to respond in an organized and integrated manner in the event of an incident. Oklahoma is providing opportunities for IT staff to become emergency management certified to strengthen these twin pillars of response.

While not often owning responsibility for cybersecurity processes for the state, emergency management's mastery of incident management to respond to threats and incidents in a flexible but coordinated manner and ability to build partnerships allows for a unique position in the cyber domain. All stakeholders involved in building a resilient cybersecurity culture must pull together because an effective response requires the coordination of supply chains and partners, as well as effective situational awareness management to provide information to key stakeholders for a common threat picture. Emergency management can leverage these groups' capabilities to form a single security strategy, which should include regulatory and legal action plans as well as information on vendor capabilities and third-party service offerings from government, law enforcement, and private industry partners. Keep in mind that what starts as a cyber incident does not necessarily end there: real-world consequences, such as loss of life or significant damage to national or economic security, are possible.

Successful cyberattacks are often perpetrated against local government agencies that have limited resources and may consider themselves too small to be worthwhile targets for hackers. As part of the regular outreach state emergency management agencies conduct with local jurisdictions during the application process for grants such as the State Homeland Security Program (SHSP) and Hazard Mitigation Assistance (HMA), asking questions and promoting discussions about their cybersecurity posture and resilience can create opportunities to promote a statewide resilient cybersecurity culture with federal grant partnership. Due to resource limitations, critical IT and cyber resources are hard to come by in state and local government. Building a local (state-led) focus group to identify where resources are in your local communities, higher education institutions, state government, and private industry is crucial. The next step in creating a flexible and efficient cyber response is to build teams willing to assist through mutual aid packages and agreements to help supplement response, support each other, and strengthen recovery efforts.

Emergency management holds close the adage that you do not want to be exchanging business cards for the first time at the incident. In cyber, as in the event of a more traditional physical incident, it is far better to

develop a robust strategy, response architecture and plan with relevant partners prior to an incident. It is important to conduct regular exercises to ensure that what you have created is effective and updated to meet current needs. The challenge is admittedly substantial, but there is no need to reinvent the wheel. An array of best practices developed from lessons learned already exist. Finally, encouraging and enforcing basic cyber hygiene measures—the cyber equivalent of pandemic guidance to wash your hands and wear a mask—will reduce our exposure to cyber risks if applied widely.

STRATEGY

Everything is connected; machines, data, people, and facilities. Understanding these connections requires taking inventory of assets, mapping networks and supply chains, and identifying all who have access to them at a granular level. Regularly assess the trustworthiness and required access and privileges of the manufacturers your systems rely on and of any third parties who have privileges without a genuine and ongoing need for such access. For those who do need sensitive access, adhere to the maxim: trust but verify, and be continuously vigilant about monitoring even after verifying.

Understanding the myriad connections in your systems is key to a rapid and successful response during a crisis. Interconnections of traditional IT systems and operational technology (OT) systems have developed an environment of speed and convenience but have also created an avenue of risk that threat actors seek to exploit. This is especially true during times of crisis and confusion.

To fully understand the threat and system impacts, the system must be defined. All technology, IT and OT, needs to be identified. Resources such as people, facilities and business operations need to be mapped and evaluated for impact if compromised whether by intentional or unintentional threats. Elements critical to business operations can then be identified – particularly those that may even be outside the organization such as a supply chain, vendors, contractors, cloud services or third-party facilities. When mapping networks, take care to exercise resiliency in planning by ensuring that maps of the network are not stored on the network itself.

Once all the critical elements of your operations have been identified, controls can be implemented to augment the security of the operational environment. It is important to align security controls of the organization with all partners and services to ensure that no gaps exist in operational and communications lines between these entities. During and following any planning processes, it is critical to conduct exercises with all critical stakeholders whether internal or external to the organization for a successful security program. Exercises are the bread and butter of emergency management and provide further opportunities for supporting local governments as they also scale up their capabilities. This can also include school districts as they are among the most targeted industries for cybercriminals given that they often have limited cybersecurity resources within their own organizations and are switching to an online-based format at significant rates due to COVID-19[8].

It is important to have a strategy not only for preparedness, but for when an incident occurs. Colorado was the first state to implement a disaster declaration in the wake of their SamSam cyberattack, allowing for a unified command and bring in resources from the state's National Guard. While this model may not be effective for all states and all cyber incidents, this shift to treating a cyber incident like a natural disaster, developing a strategy ahead of time, and exercising your plan is worthy of consideration.

[8] IBM Survey: Only 38% of State and Local Government Employees Trained on Ransomware Prevention. (2020). Retrieved from https://newsroom.ibm.com/2020-02-27-IBM-Survey-Only-38-of-State-and-Local-Government-Employees-Trained-on-Ransomware-Prevention

Taking proactive steps to enhance cybersecurity will benefit your organization and help support both national and economic security, which are inextricably intertwined and mutually reinforcing. Fortunately, there are many national strategies and policies already in place that identify and seek to incentivize cybersecure practices, including the National Cyber Strategy[9]. The most critical of our critical infrastructures ("Section 9 entities[10]") and national functions[11] demand our most concerted efforts; but the more multilayered our approach, the more robust our overall level of resilience will be.

CONCLUSION

Cybersecurity has long been a challenge states listed in the national Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR). Up until now, cybersecurity has been reported as receiving lower levels of grant funding through FEMA's preparedness grants than other types of emergency management operations[12]. With the global onset of COVID-19, remote online work has (where possible) become the norm rather than the exception, bringing with it a host of new vulnerabilities exacerbated by the sudden and make-do nature of the shift that previous levels of grant expenditure may not have accounted for. Opportunities borne of these newfound vulnerabilities have not gone unnoticed by bad actors. Add a hurricane, wildfire, or other natural disaster atop this complex mix of vulnerabilities, and it approaches the perfect storm.

Acknowledging that money is tight and emergency management funding must cover a vast array of preparedness, response, recovery, and mitigation actions, it is critical that emergency management leverage its strengths in convening, communication, and risk assessment to establish a state government enterprise that is resilient not only to the cybersecurity challenges of today, but the unanticipated challenges of tomorrow.

[9] National Cyber Strategy of the United States of America. (2018). Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[10] Support to Critical Infrastructure at Greatest Risk ("Section 9 Report") Summary. (n.d.). Retrieved from https://www.cisa.gov/publication/support-critical-infrastructure-greatest-risk-section-9-report-summary
[11] CISA National Critical Functions. (n.d.). Retrieved from https://www.cisa.gov/national-critical-functions
[12] *2020 Biennial Report* (Rep.). (2020). National Emergency Management Association.

Acknowledgements

The National Emergency Management Association Homeland Security Committee would like to thank the state officials and experts who provided input and feedback on this document, as well as the authors of the publications and resources cited.

National Emergency Management Association

The National Emergency Management Association (NEMA) is a nonpartisan, nonprofit 501(c)(3) association dedicated to enhancing public safety by improving the nation's ability to prepare for, respond to, and recover from all emergencies, disasters, and threats to our nation's security. NEMA is the professional association of and for emergency management directors from all 50 states, U.S. territories, and the District of Columbia.

Primary NEMA Contributors:

Brian Hastings, Director
Alabama Emergency Management Agency
Chair, NEMA Homeland Security Committee

Jennifer Harper, Director
New Hampshire Division of Homeland Security and Emergency Management
Vice Chair, NEMA Homeland Security Committee

DHS Cybersecurity and Infrastructure Security Agency (CISA)

Primary CISA Contributor:

Klint Walker, Cybersecurity Advisor
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

Auburn University McCrary Institute

The McCrary Institute, based in Auburn with additional centers in Washington DC and Huntsville, seeks practical solutions to pressing challenges in the areas of cyber and critical infrastructure security. Through its three hubs, the institute offers end-to-end capability – policy, technology, research and education – on all things cyber.

Primary McCrary Institute Contributor:

Sharon L. Cardash, Deputy Director
Center for Cyber and Homeland Security