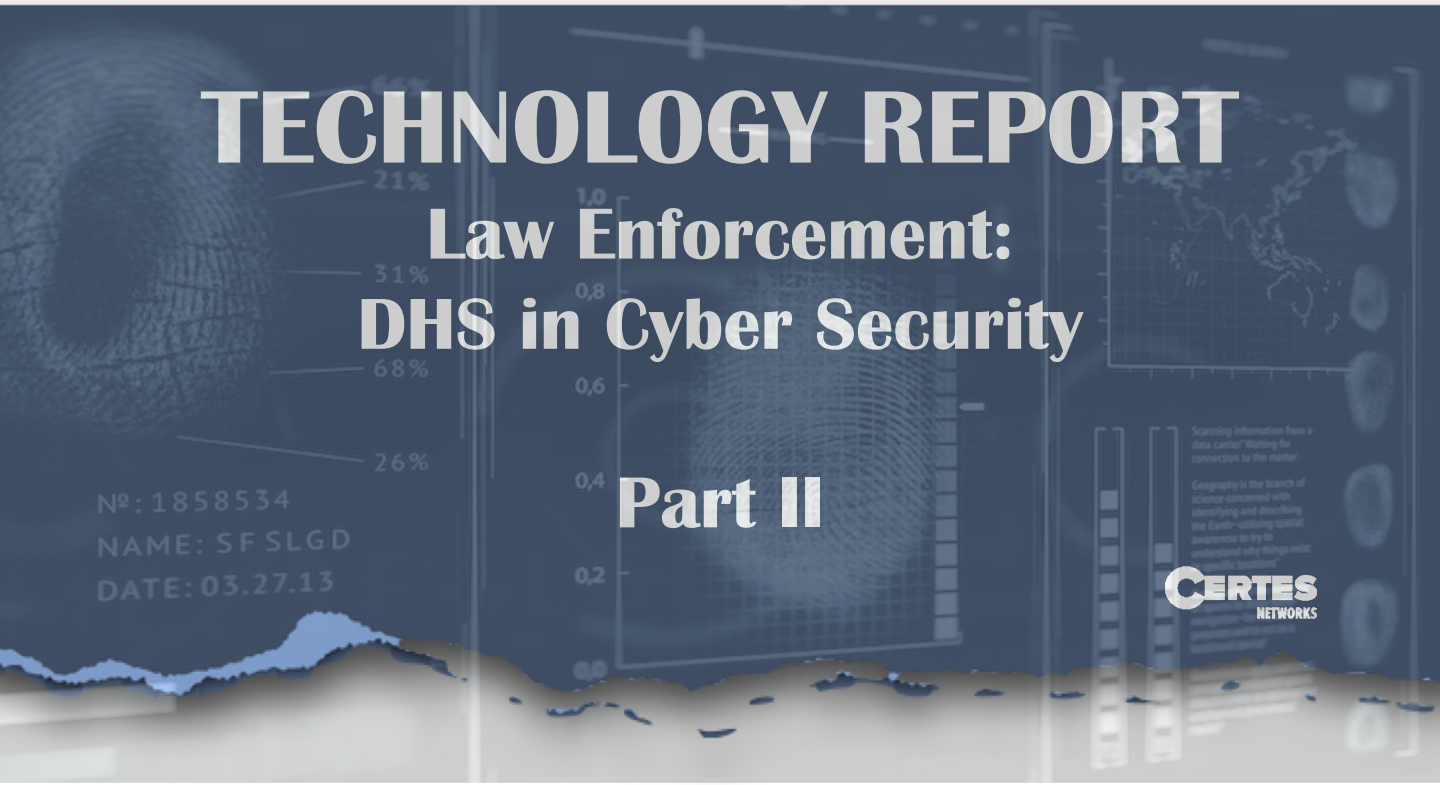
CERTES NETWORKS



Intelligence community works together to mitigate threats to U.S. cyber and communications systems

Establishing Organization Cybersecurity Protocols

Universal to law enforcement organizations is the increase of digital evidence, such as reports, photos, videos and other electronic records that must be collected, stored and maintained in a manner that ensures the integrity and verification of the data's authenticity. However, many law enforcement agencies rely on local government information technology (IT) staff to ensure cybersecurity with little direct control over hiring processes or the technology used to secure the data.

But when, in fact, it is the responsibility of the agency to ensure all aspects of their cybersecurity measures are sufficient, rest assured that when a system is compromised the police agency and its law enforcement partners will be held accountable, not the IT contractors.

Therefore, silos must be broken down and police leaders should collaborate with IT professionals to ensure priorities and strategies are developed together. Mutual goals must be agreed upon to prevent a cyberattack and procedures must be clearly laid out prior to one occurring. Having communications and expectations already established can help ensure an effective post-investigation will be conducted allowing for the rapid recovery of affected files and systems.

The Role of the Department of Homeland Security in Cybersecurity

The DHS National Protection and Programs Directorate (NPPD) is responsible for helping to secure the U.S. critical infrastructure and enhance its resiliency. Within NPPD, the Office of Cybersecurity and Communications (CS&C) takes the lead on cybersecurity, critical infrastructure security, and resilience, engaging the public at all levels of government and private sectors, as well as international partners, to prepare for, prevent, and respond to cyber incidents that could degrade or overwhelm U.S. strategic assets.

Under the auspices of DHS is the National Cybersecurity and Communications Integration Center (NCCIC), a 24/7 cyber situational awareness, incident response, and management center where government, private sector, law enforcement, international, and intelligence community partners work together to detect, prevent, respond to, and mitigate threats to U.S. cyber and communications systems.

The NCCIC works in partnership with the FBI, U.S. Secret Service, and other law enforcement agencies for coordination, integration, and information sharing related to domestic cyberthreat investigations. Further, the NCCIC, FBI and U.S, Secret Service have developed joint to ensure outreach and response activities are coordinated on behalf of victims of cybercrime and incidents.

Cybersecurity Training and Engagement

The need for cybersecurity awareness training has reach a critical stage and DHS has long recognized that cybersecurity is a shared responsibility that depends on engagement with strategic partners, including law enforcement, and the public and private sectors.

Human failure to properly defend against cybercrimes and schemes limits how technology should and could be used to defend against the same. In July 2017, DigitalGuardian.com reported that 91 percent of successful cyberattacks are launched via a phishing email. Between 2014 and 2017, Michigan auditors conducted a covert simulated “phishing attack” on 5,000 randomly selected state employees to see how they would deal with a potential “threat.” One-third of the recipients opened the email; one-quarter of them clicked on the simulated malicious link; and almost one-fifth provided their user ID and password.

Part of a successful cybersecurity strategy, therefore, is to ensure that staff receives cybersecurity training at every level of an organization and that the training be specifically tailored to their area of access and responsibility. End users need to be aware of email requests that may look innocent but indeed are malicious, hazards related to unapproved USB devices, proper password protocols and dual-factor authentication, for example, as well as best practices related to mobile devices that connect to an agency’s network.

Preparedness and Partnerships Are Key

The sophistication of cyberattacks continue to evolve and are becoming harder to detect early. It is not a matter of if, but when, a police department's technology will eventually be breached. Even with the most robust prevention measures in place, there is no guarantee against profiteering—so contingency and crisis planning are critical to ensure operational continuity and recovery following a cyberattack. Policies and practices must be adopted to balance preserving evidence of the crime with the need to restore data access and systems.

The FBI does not recommend paying a ransom if one becomes the victim of a malware attack. Paying a ransom does not guarantee an organization will regain access to their data; in fact, many organizations that experienced malware attacks were never provided with decryption keys despite paying a ransom. Paying an adversary only encourages them to target other organizations and invites further criminal activity.

Therefore, it is imperative to prepare for and rehearse the response to a cyberattack as almost no organization will have all of the resources necessary to conduct a comprehensive response. Also, third-party security audits are one of the most effective ways to test an agency's ability to withstand a cyberattack and identify areas for improvement. And, if internal resources are insufficient, DHS provides assistance to state and local governments free of charge to manage and respond to an incident or crisis.

Lastly, partnerships between public safety, information security managers, and fusion centers, which are designed to promote information sharing at the federal level between agencies such as the FBI and DHS, DoJ and state, local and tribal law enforcement, are instrumental and can increase a region's ability to prepare, train and respond to cyberthreats. These partnerships should also include law enforcement collaborating with other sectors, particularly those in critical infrastructure, like transportation, energy, and health care.

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1(888) 833-1142
Fax: 1(412) 262-2574

info@certesnetworks.com
sales@certesnetworks.com

We offer an encryption solution that is simple, scalable and uncomplicated.