FACT SHEET

# Cyber Risk Analysis

Putting state and local cybersecurity on a solid footing

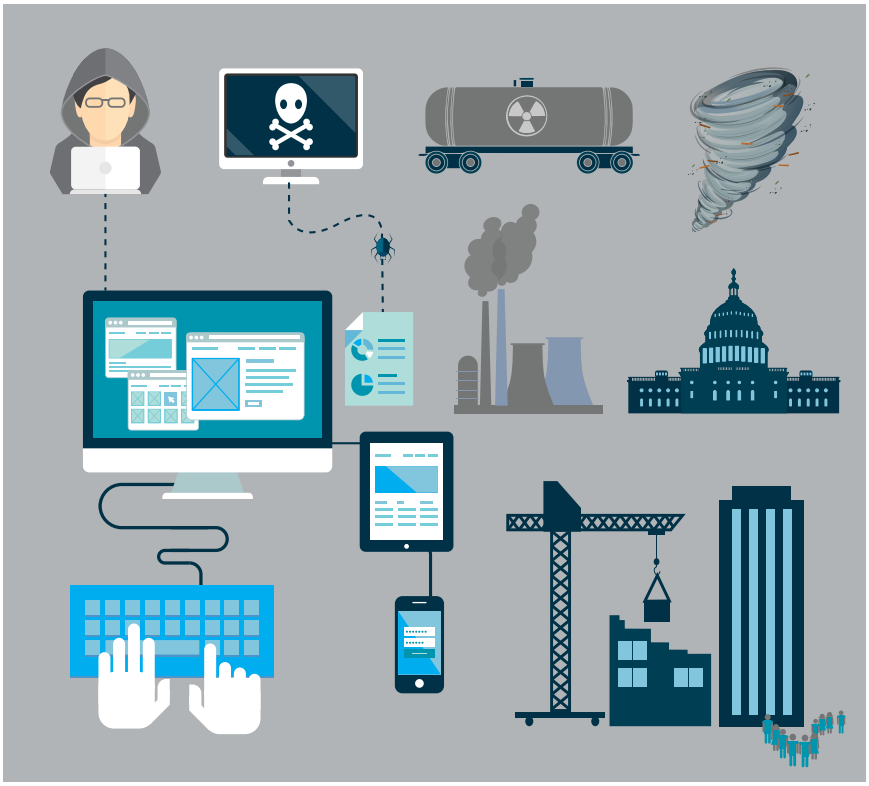
haystax

## The Problem

Defending against cyber threats has become one of the greatest challenges facing organizations today. Despite this, state and local government agencies only have constrained resources to cope with potential threats. Cities may have hundreds of interconnected software systems and networks operating within their jurisdictions, each with a unique threat profile, vulnerabilities and potential consequences. As a result, it can be difficult to determine how best to address cybersecurity and even more difficult to determine where to begin.

A number of federal and state agencies and private firms have developed and published guidance to assist government entities in determining the nature of cyber risk. However, these often have problems that complicate their implementation at the state and local level:

***Wrong scope:*** Most guidance assumes that the agency has considerable resources and time, when the opposite is true for most state and local governments.



***Limited connection to physical assets:*** Most approaches only address systems and networks. While systems are central to any cyber risk assessment, it is also important to consider the buildings and operations that house and regularly use these systems, including transitory physical operations such as polling places.

***Assessment approaches not easily sustainable:*** Most approaches do not provide for a repeatable, sustainable process. In cybersecurity, being able to quickly review and reassess the factors that inform local risk is paramount.

## Our Solution

At Haystax, our goal is to bring together local knowledge and research into an innovative product to help users prioritize their cybersecurity needs and make the best decisions. Unlike other tools and methods, we provide a sustainable, expert-informed product that captures local cyber risks. Our solution provides the following benefits:

***Right scope:*** Our analysts coordinate and conduct the risk analysis, engaging with subject matter experts when necessary. With a minimal time commitment, we can provide you with risk profiles not only for the systems in your community, but also for your critical facilities and community organizations.

***Direct connection to your infrastructure:*** Our analysis considers the buildings and operations that use your systems every day, providing a concrete connection between your cyber risk and the other risks your community faces.

***A sustainable, expandable approach:*** Like all Haystax products, we designed our cyber risk offering to grow with your community. Even after the initial analysis, you will be able to adjust the risk and priority inputs to include new systems, reflect emerging threats, account for changes to procedures and capture cyclical threats and vulnerabilities such as those surrounding elections infrastructure.

8251 Greensboro Drive, Suite 1000, McLean, VA 22102 / 571-297-3800 / info@haystax.com / www.haystax.com

Our five-step process allows local agencies to determine how best to allocate their limited resources by establishing a risk score and priority for each system, based on current research and subject matter expertise.

Establish System Catalog » Conduct Initial Analysis » SME Review Workshop » Final Risk Analysis » User Training and Information

We begin by compiling a jurisdictional system catalog through soliciting stakeholder and agency information and feedback. Next, we conduct an initial prioritization pass and risk analysis informed by national trends in the field. This analysis not only considers threats from adversarial organizations and individuals, but also from natural hazards and user error, as well as cyclical threats such as those to elections. Then, we review these initial inputs with your local subject matter experts, collecting feedback and suggestions based on local experience.

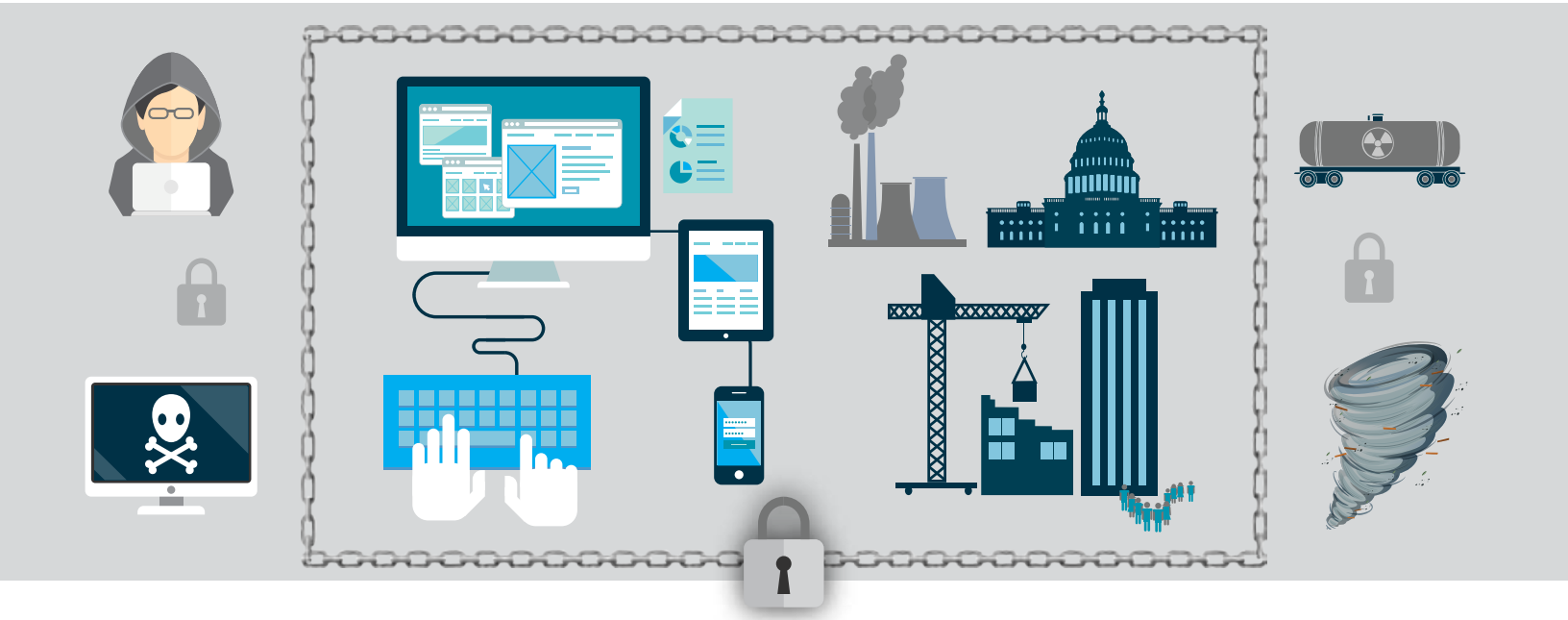
Our analysts incorporate the local expert feedback into the final risk analysis, which yields a completed risk assessment in an expandable tool designed to inform subsequent analytical efforts. This cyber tool makes it easy to identify your community's high-priority and high-risk systems, where and when they are accessed, what organizational security weaknesses affect them and the potential consequences of a cyber incident. In the final step, Haystax will train your organization in the use of your cyber tool, including how to update risk profiles and understand its outputs. This training provides a solid foundation for continuing your community's cyber risk management program.

## Your Next Step

At Haystax, we are committed to helping public safety officials across the U.S. create safer, more secure communities. Our cybersecurity solution not only allows you to get your cybersecurity program on a solid, defensible footing, but it can also help you compete for Department of Homeland Security (DHS) grant funding.

Beginning in FY 2020, DHS is requiring states and urban areas to allocate five percent of homeland security grant funding towards projects that enhance cybersecurity, including those that aid in the implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Federal guidance and best practices, including the NIST Framework, are central to our cyber risk analysis.

**Don't wait for a cyber emergency to happen.**
**Contact Haystax today.**



8251 Greensboro Drive, Suite 1000, McLean, VA 22102 / 571-297-3800 / info@haystax.com / www.haystax.com