ITS Carolinas 2018 Annual Meeting

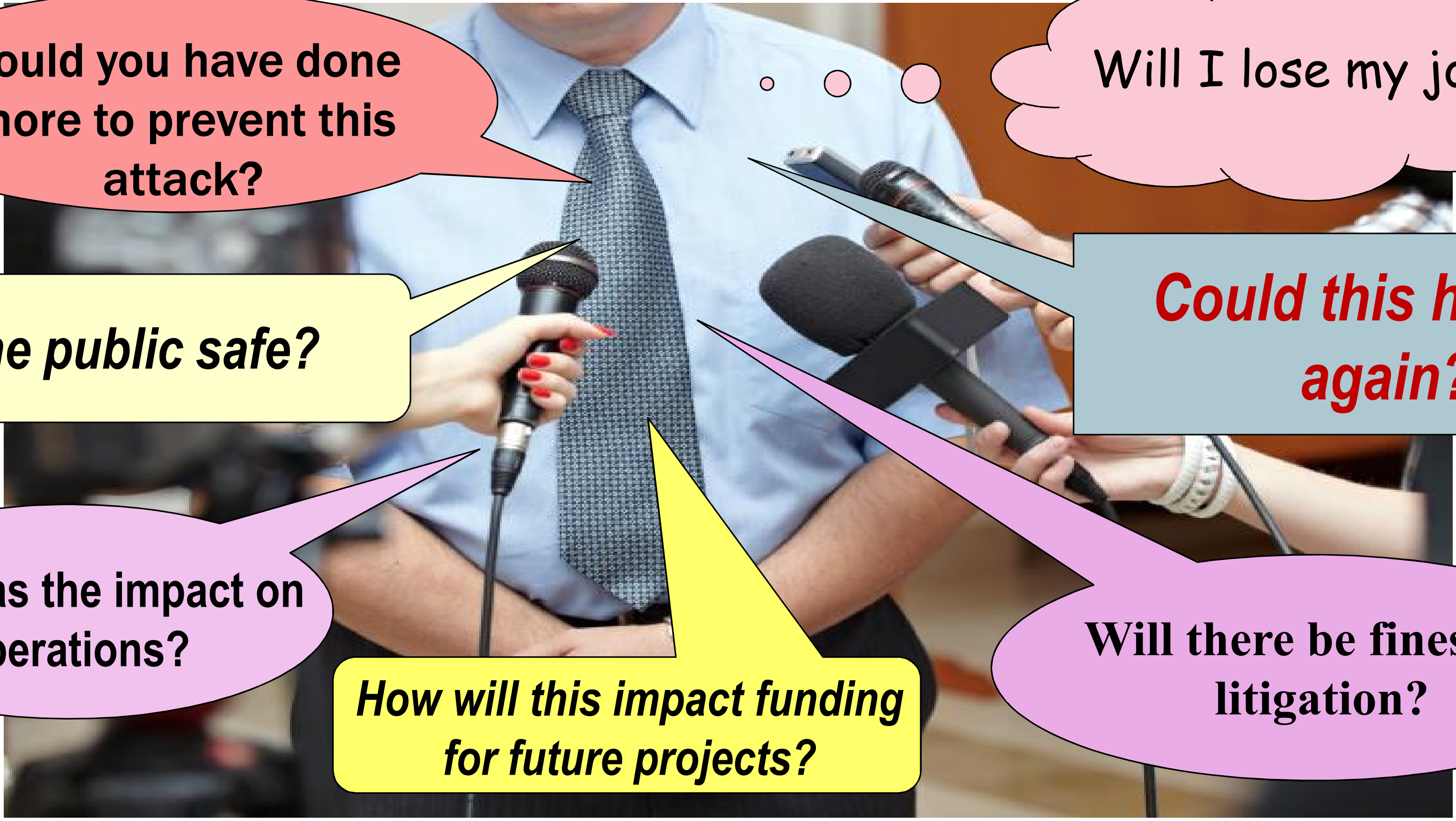
Cybersecurity: Going Beyond Protection

PHOENIX CONTACT
INSPIRING INNOVATIONS

Security breaches are inevitable…

Being a headline is not ® Mandiant – A FireEye™ Company

Tough questions after attack…



Could you have done more to prevent this attack?

Will I lose my job?

Is the public safe?

Could this happen again?

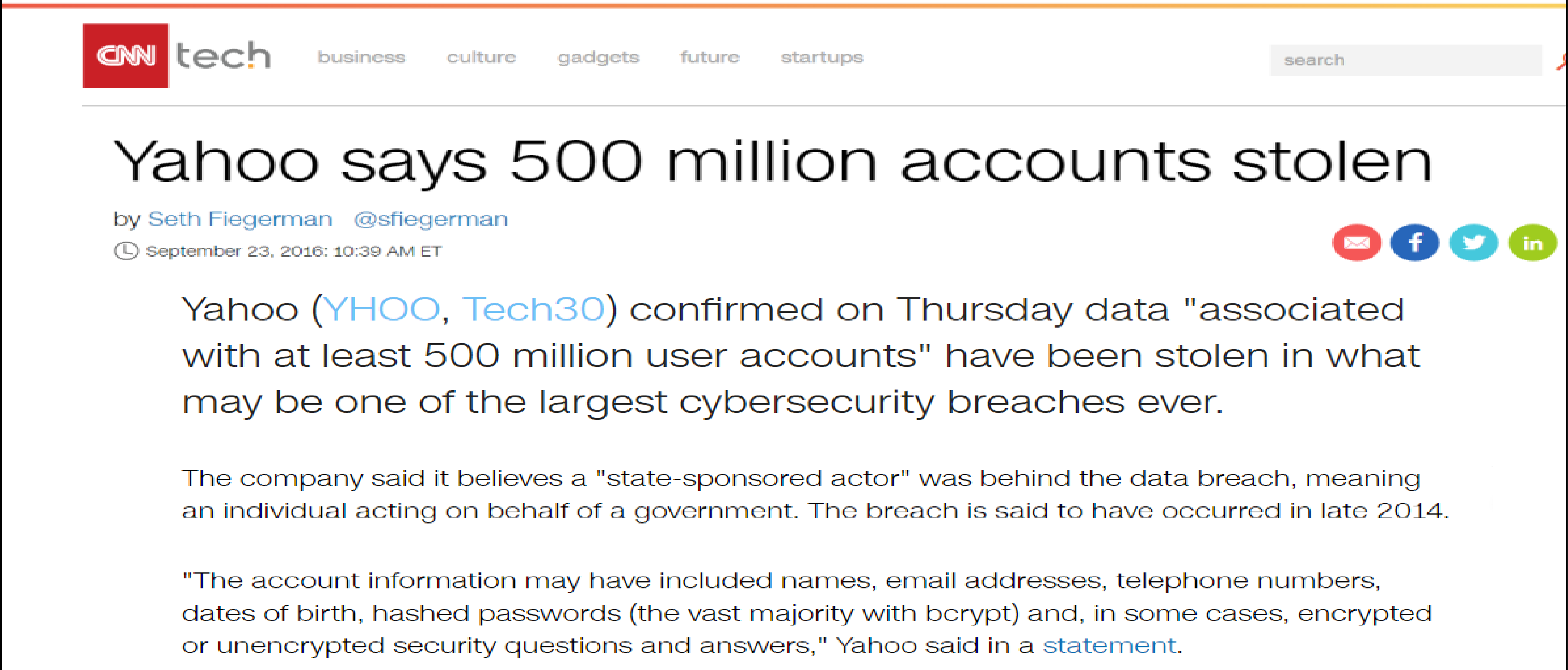
What was the impact on operations?

How will this impact funding for future projects?

Will there be fines and litigation?

Agenda

- The New Norm - Managing Cyber Threats
- Protecting Critical Infrastructure
- NIST Cybersecurity Framework (CSF)
- CSF Core Functions



Yahoo says 500 million accounts stolen

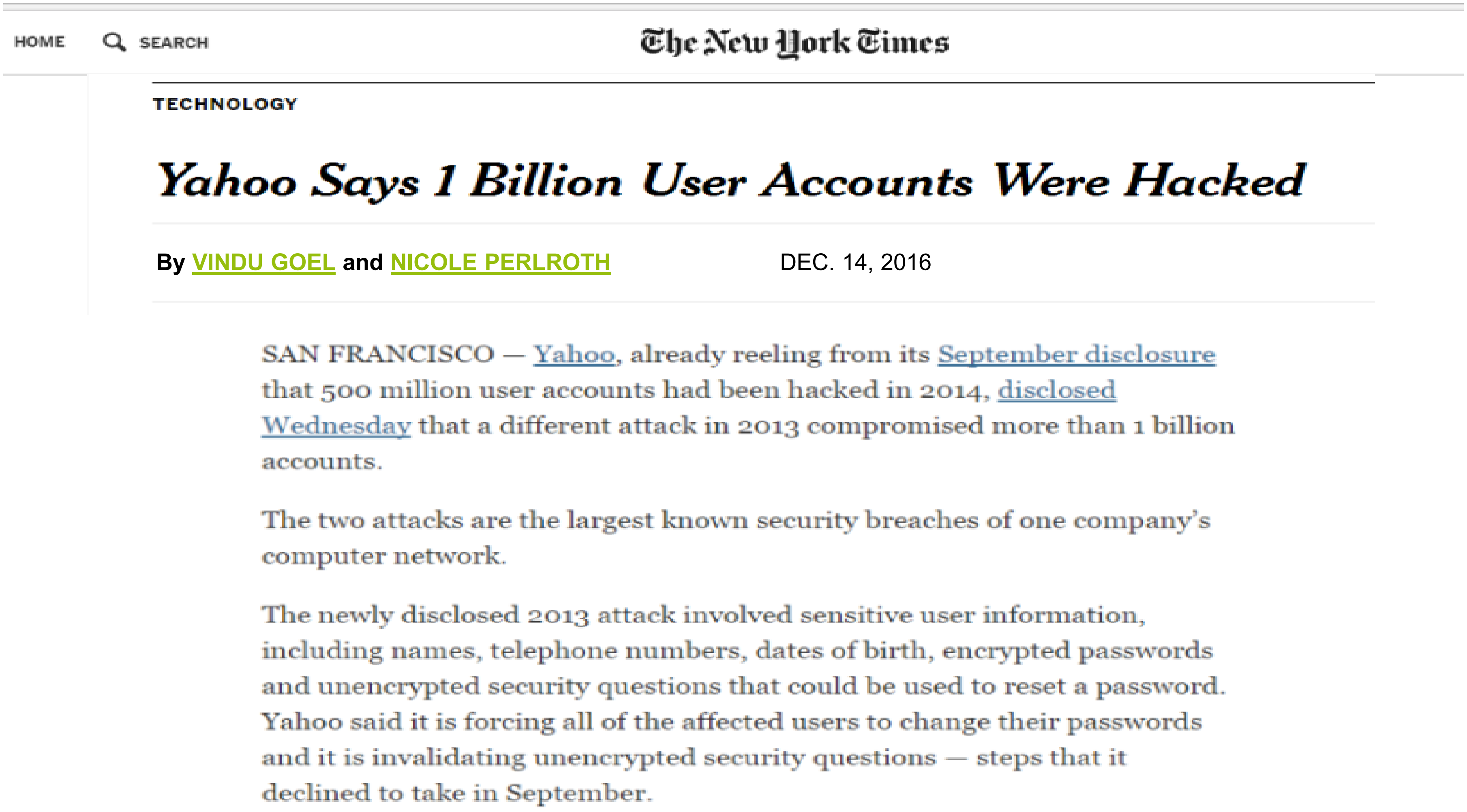
by Seth Fiegerman @sfiegerman

September 23, 2016: 10:39 AM ET

Yahoo (YHOO, Tech30) confirmed on Thursday data "associated with at least 500 million user accounts" have been stolen in what may be one of the largest cybersecurity breaches ever.

The company said it believes a "state-sponsored actor" was behind the data breach, meaning an individual acting on behalf of a government. The breach is said to have occurred in late 2014.

"The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers," Yahoo said in a statement.



TECHNOLOGY

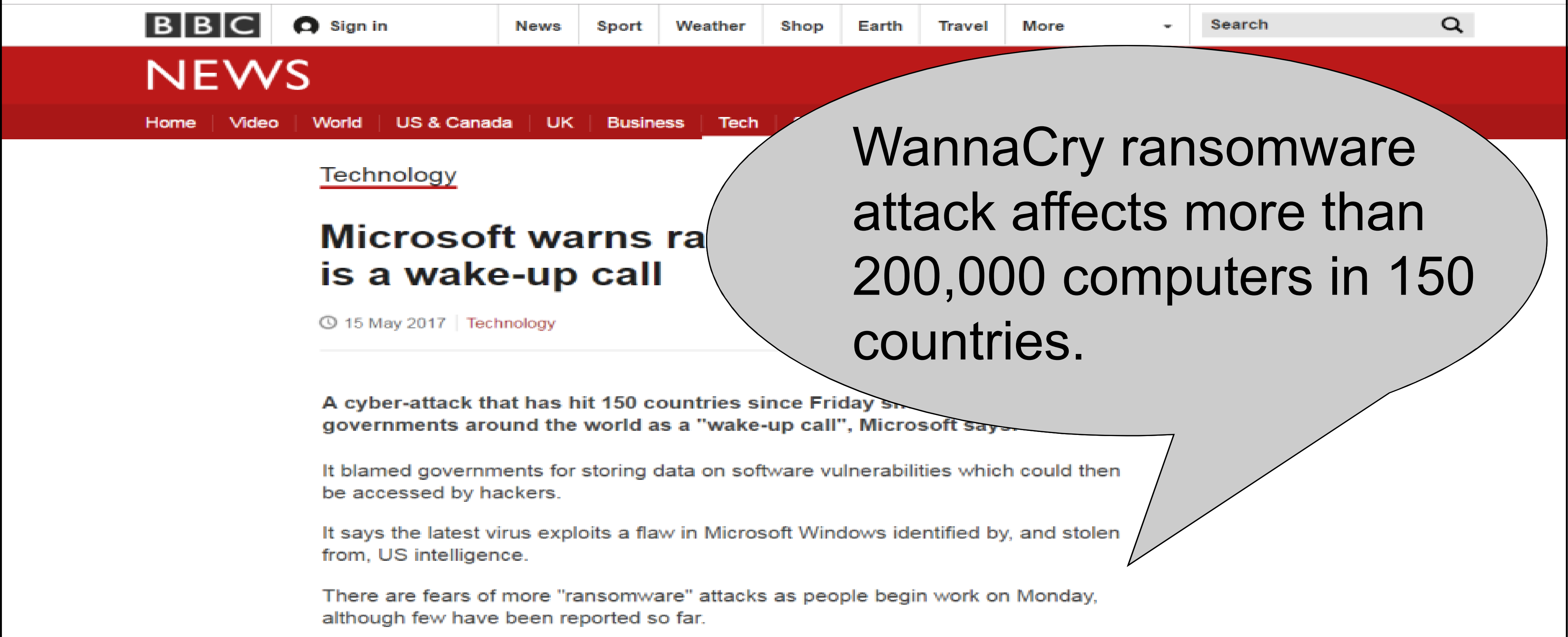
Yahoo Says 1 Billion User Accounts Were Hacked

By VINDU GOEL and NICOLE PERLROTH DEC. 14, 2016

SAN FRANCISCO — Yahoo, already reeling from its September disclosure that 500 million user accounts had been hacked in 2014, disclosed Wednesday that a different attack in 2013 compromised more than 1 billion accounts.

The two attacks are the largest known security breaches of one company's computer network.

The newly disclosed 2013 attack involved sensitive user information, including names, telephone numbers, dates of birth, encrypted passwords and unencrypted security questions that could be used to reset a password. Yahoo said it is forcing all of the affected users to change their passwords and it is invalidating unencrypted security questions — steps that it declined to take in September.



Technology

Microsoft warns ra
is a wake-up call

15 May 2017 | Technology

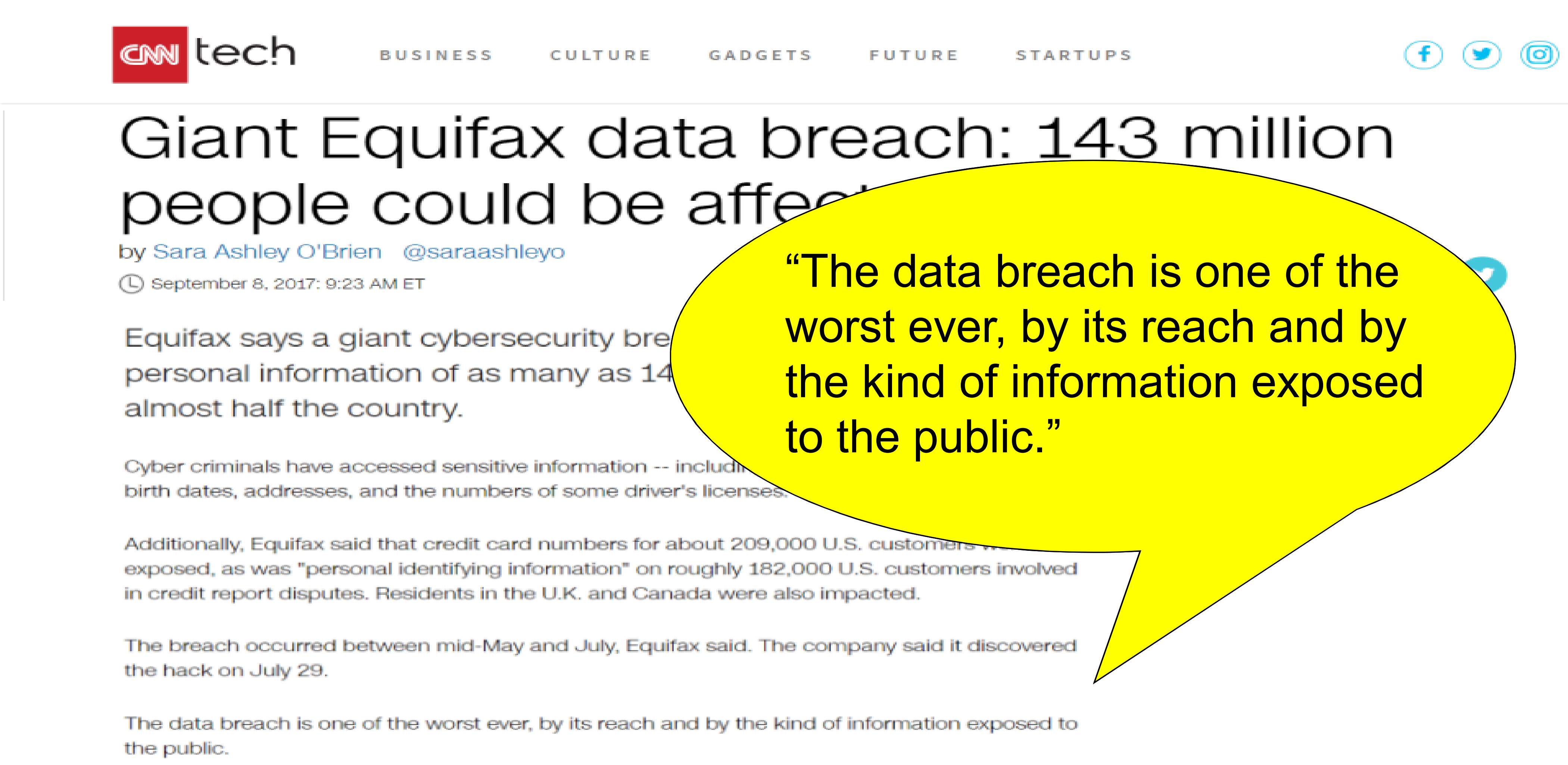
A cyber-attack that has hit 150 countries since Friday s governments around the world as a "wake-up call", Microsoft says.

It blamed governments for storing data on software vulnerabilities which could then be accessed by hackers.

It says the latest virus exploits a flaw in Microsoft Windows identified by, and stolen from, US intelligence.

There are fears of more "ransomware" attacks as people begin work on Monday, although few have been reported so far.

WannaCry ransomware attack affects more than 200,000 computers in 150 countries.



Giant Equifax data breach: 143 million people could be affec

by Sara Ashley O'Brien @saraashleyo

September 8, 2017: 9:23 AM ET

Equifax says a giant cybersecurity bre
personal information of as many as 14
almost half the country.

Cyber criminals have accessed sensitive information -- includi
birth dates, addresses, and the numbers of some driver's licenses.

Additionally, Equifax said that credit card numbers for about 209,000 U.S. customers w
exposed, as was "personal identifying information" on roughly 182,000 U.S. customers involved in credit report disputes. Residents in the U.K. and Canada were also impacted.

The breach occurred between mid-May and July, Equifax said. The company said it discovered the hack on July 29.

The data breach is one of the worst ever, by its reach and by the kind of information exposed to the public.

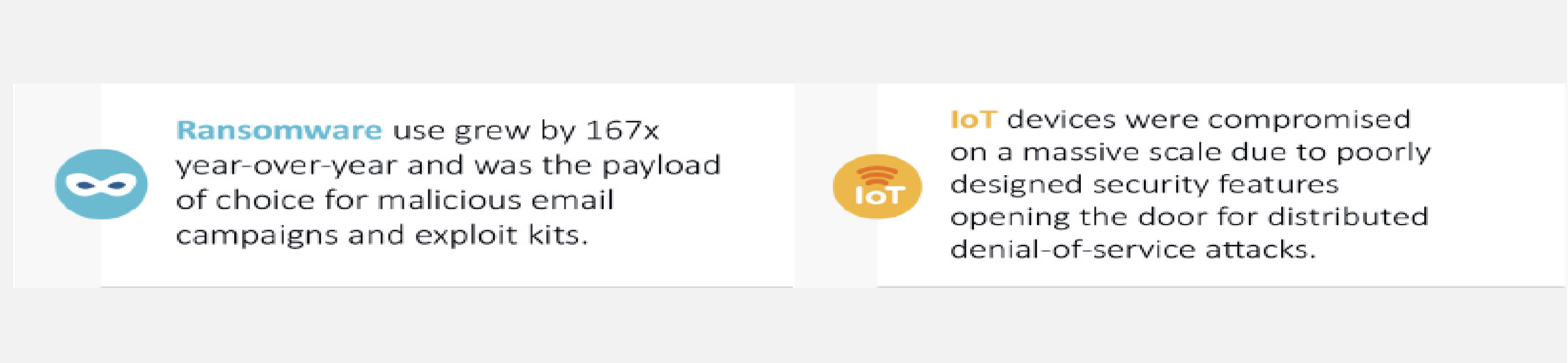
“The data breach is one of the worst ever, by its reach and by the kind of information exposed to the public.”

PHOENIX CONTACT
INSPIRING INNOVATIONS

SONICWALL™

2017 Annual Threat Report

- Key Findings From 2016: Cyber Criminal Advances

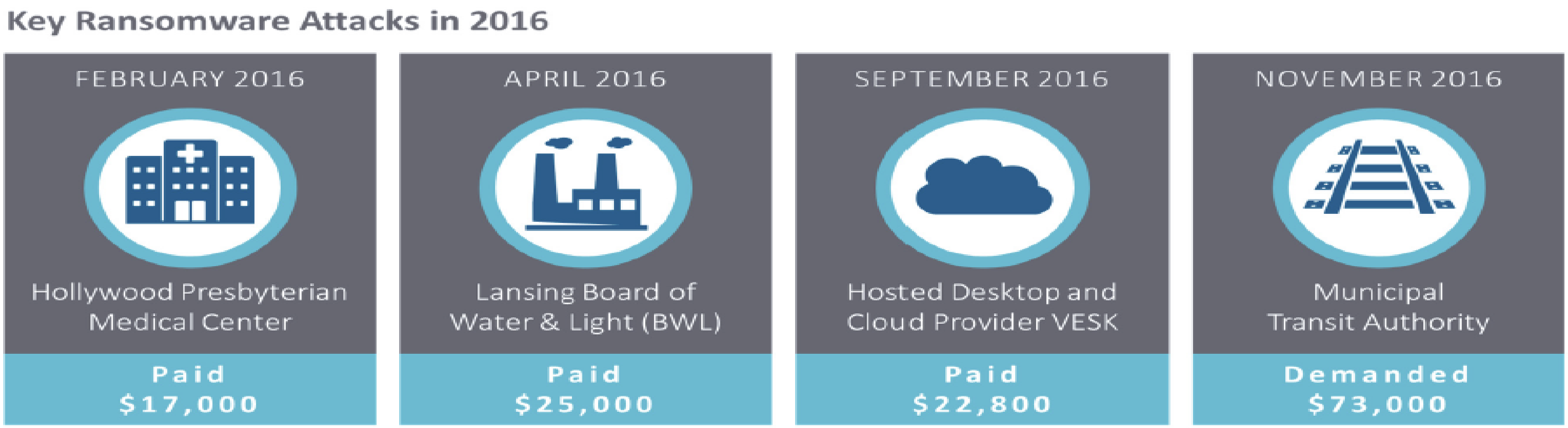


Ransomware use grew by 167x year-over-year and was the payload of choice for malicious email campaigns and exploit kits.

IoT devices were compromised on a massive scale due to poorly designed security features opening the door for distributed denial-of-service attacks.

SONICWALL™

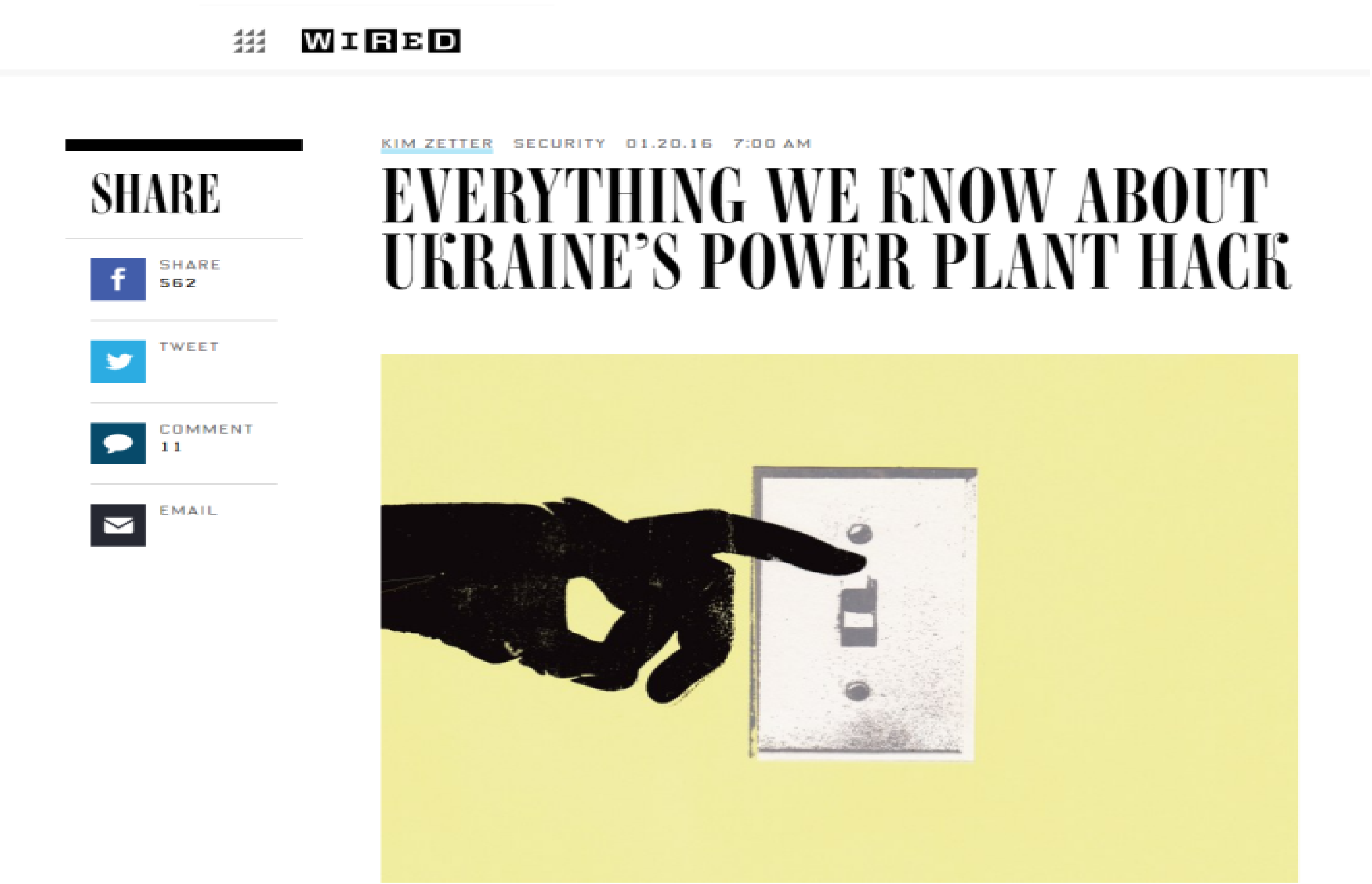
2017 Annual Threat Report



Key Ransomware Attacks in 2016

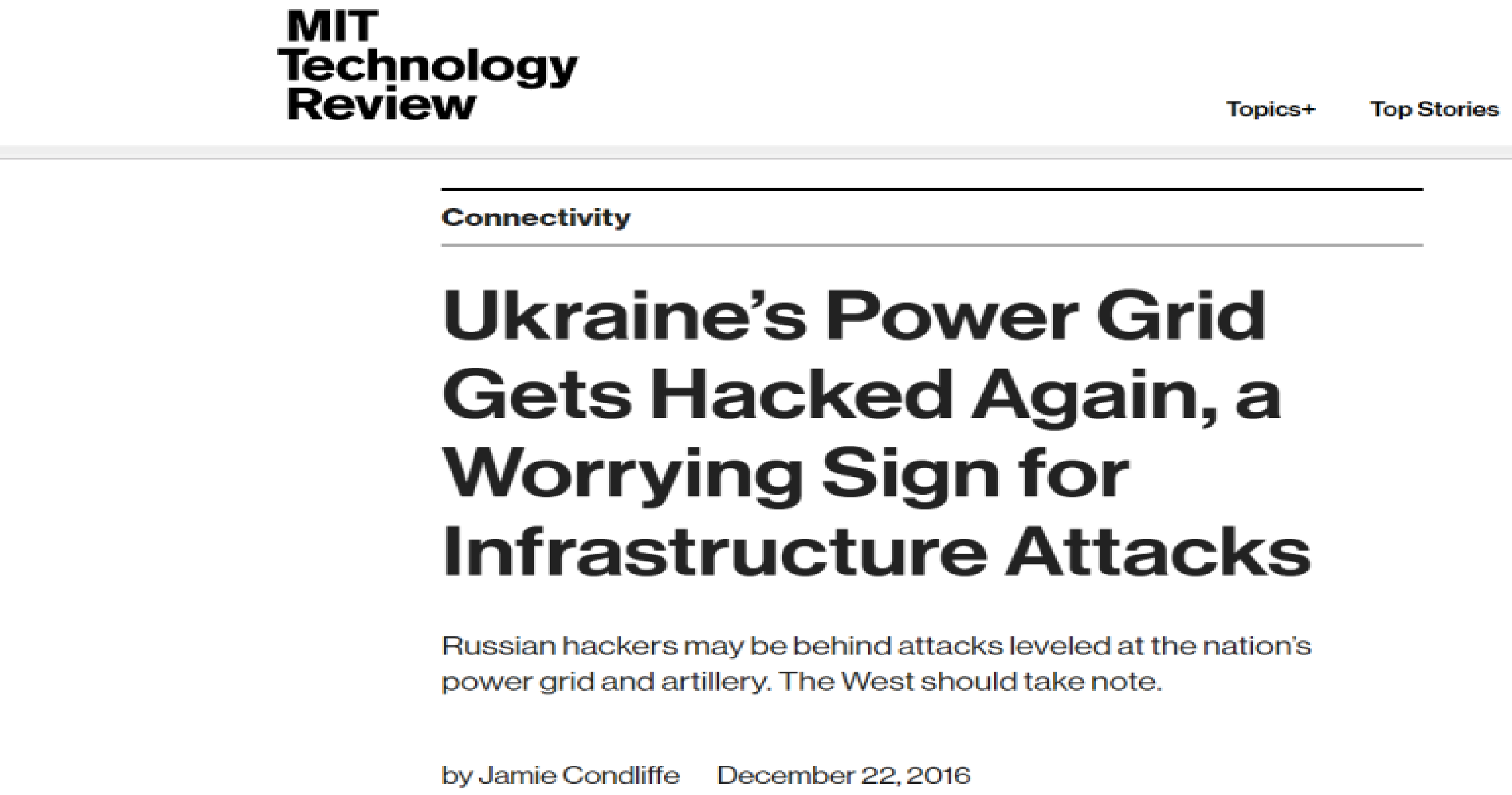
FEBRUARY 2016	APRIL 2016	SEPTEMBER 2016	NOVEMBER 2016
Hollywood Presbyterian Medical Center	Lansing Board of Water & Light (BWL)	Hosted Desktop and Cloud Provider VESK	Municipal Transit Authority
Paid $17,000	Paid $25,000	Paid $22,800	Demanded $73,000

Key Findings From 2016: Cyber Criminal Advances



KIM ZETTER SECURITY 01.20.16 7:00 AM

EVERYTHING WE KNOW ABOUT UKRAINE'S POWER PLANT HACK



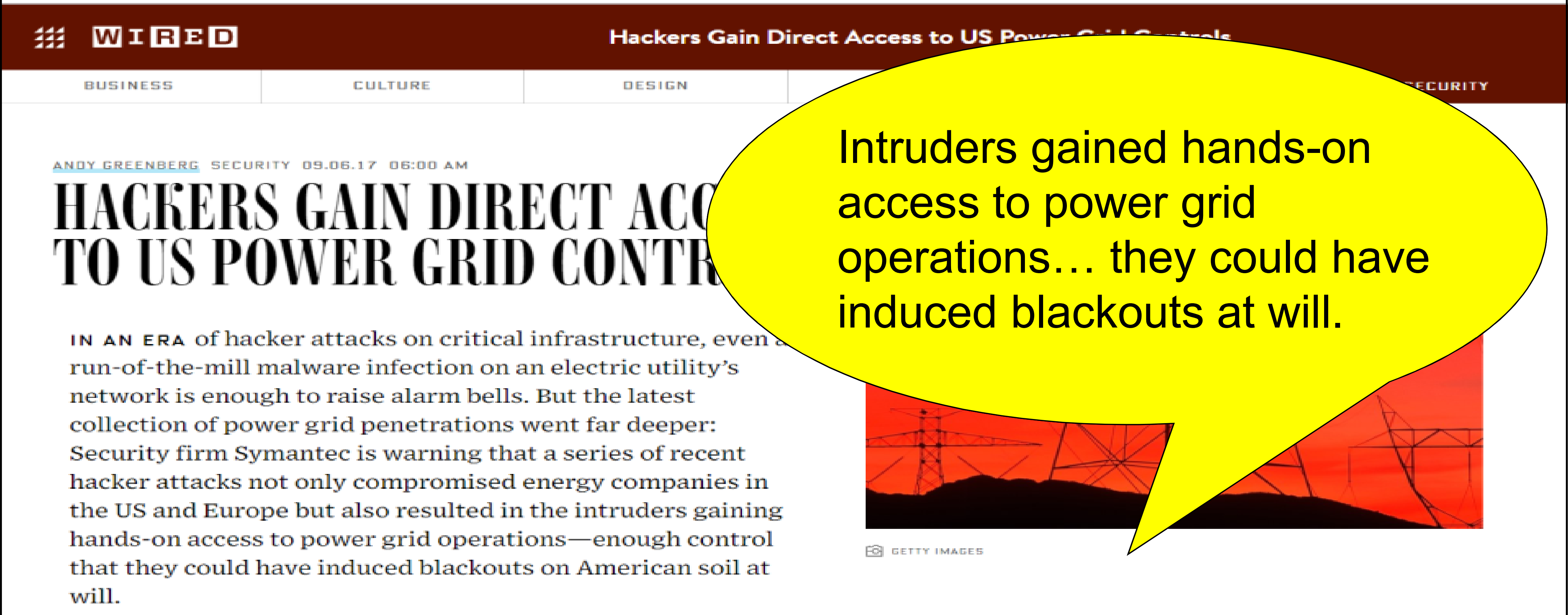
MIT Technology Review

Connectivity

Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks

Russian hackers may be behind attacks leveled at the nation's power grid and artillery. The West should take note.

by Jamie Condliffe December 22, 2016



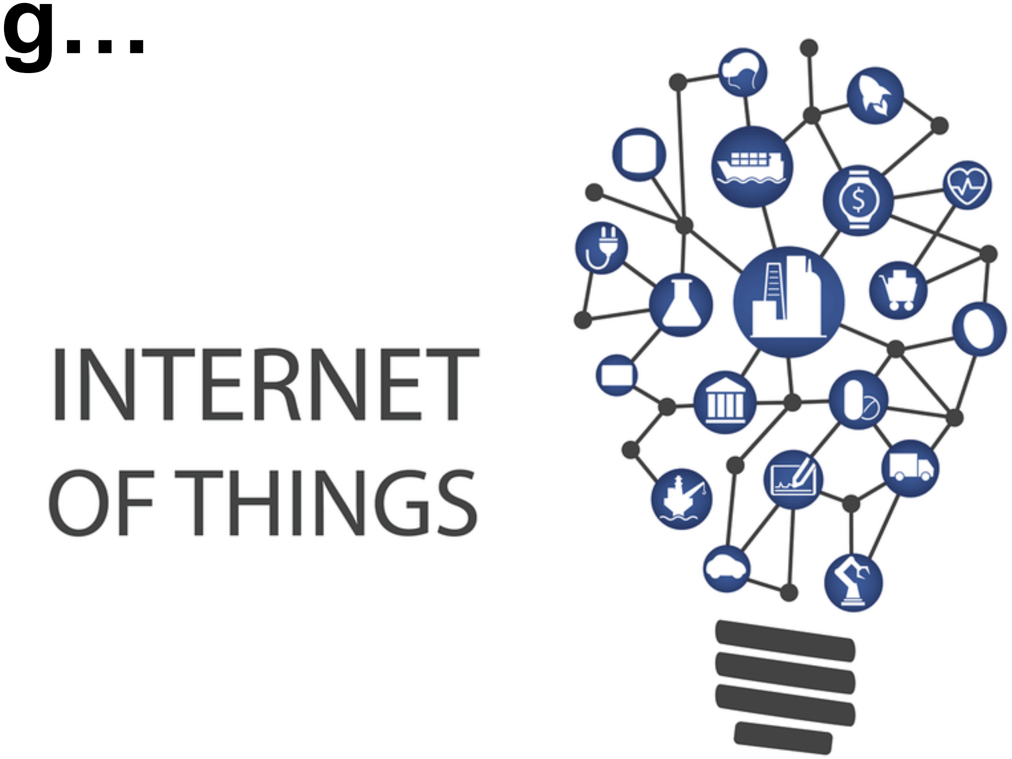
ANDY GREENBERG SECURITY 09.06.17 06:00 AM

HACKERS GAIN DIRECT ACC TO US POWER GRID CONTR

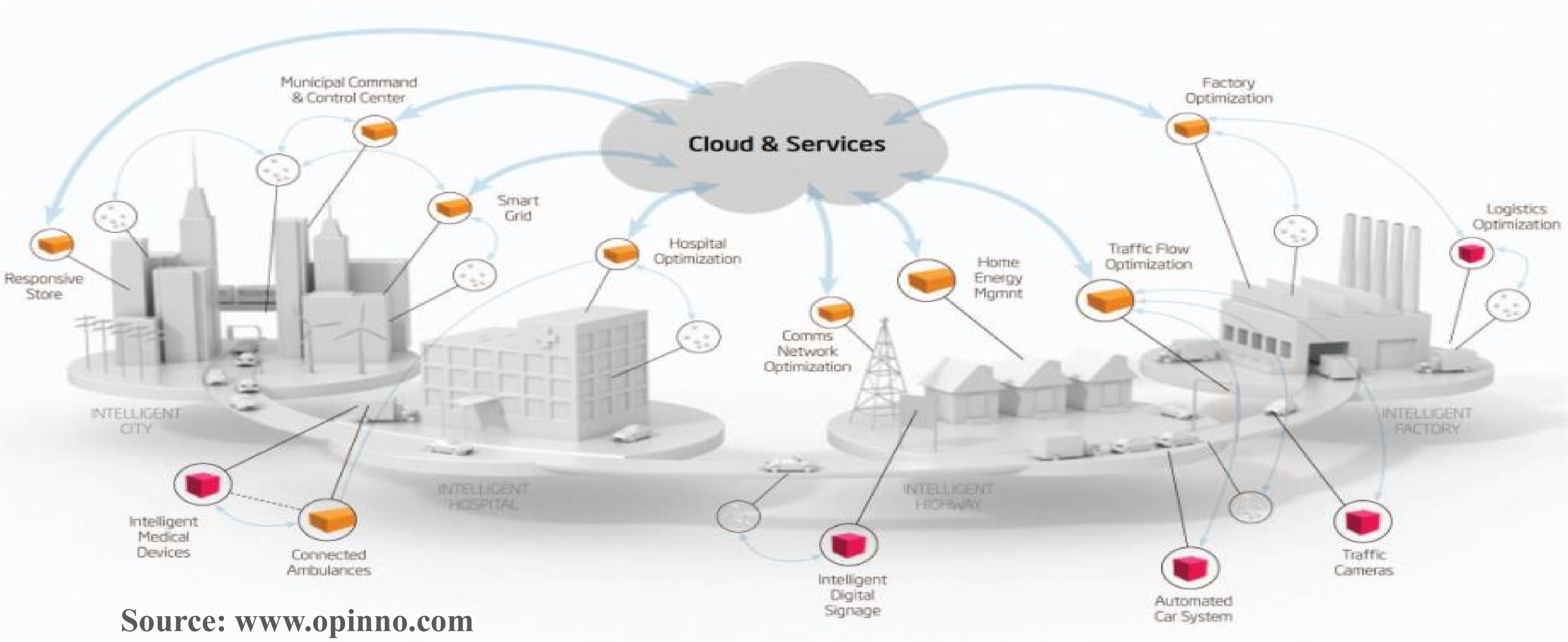
IN AN ERA of hacker attacks on critical infrastructure, even a run-of-the-mill malware infection on an electric utility's network is enough to raise alarm bells. But the latest collection of power grid penetrations went far deeper: Security firm Symantec is warning that a series of recent hacker attacks not only compromised energy companies in the US and Europe but also resulted in the intruders gaining hands-on access to power grid operations—enough control that they could have induced blackouts on American soil at will.

Intruders gained hands-on access to power grid operations… they could have induced blackouts at will.

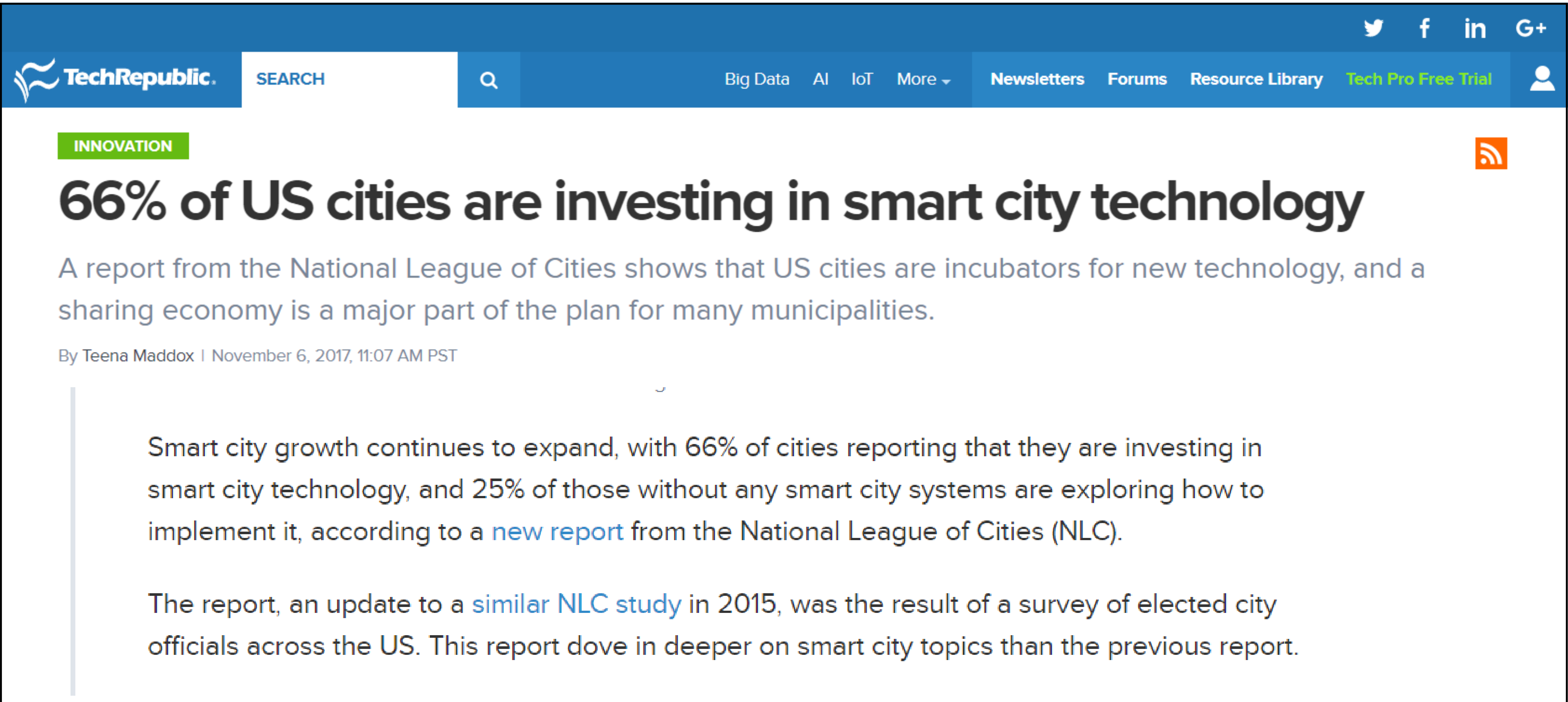
Why security will become even more challenging…



Smart Cities



Source: www.opinno.com



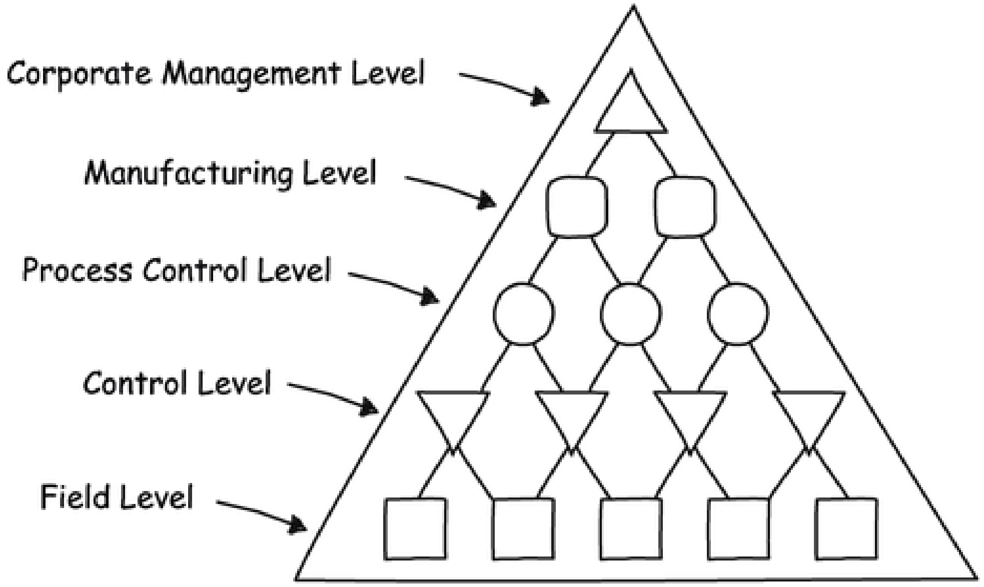
66% of US cities are investing in smart city technology

A report from the National League of Cities shows that US cities are incubators for new technology, and a sharing economy is a major part of the plan for many municipalities.

By Teena Maddox | November 6, 2017, 11:07 AM PST

> Smart city growth continues to expand, with 66% of cities reporting that they are investing in smart city technology, and 25% of those without any smart city systems are exploring how to implement it, according to a new report from the National League of Cities (NLC).
>
> The report, an update to a similar NLC study in 2015, was the result of a survey of elected city officials across the US. This report dove in deeper on smart city topics than the previous report.

Lines Between IT / OT BLURRED

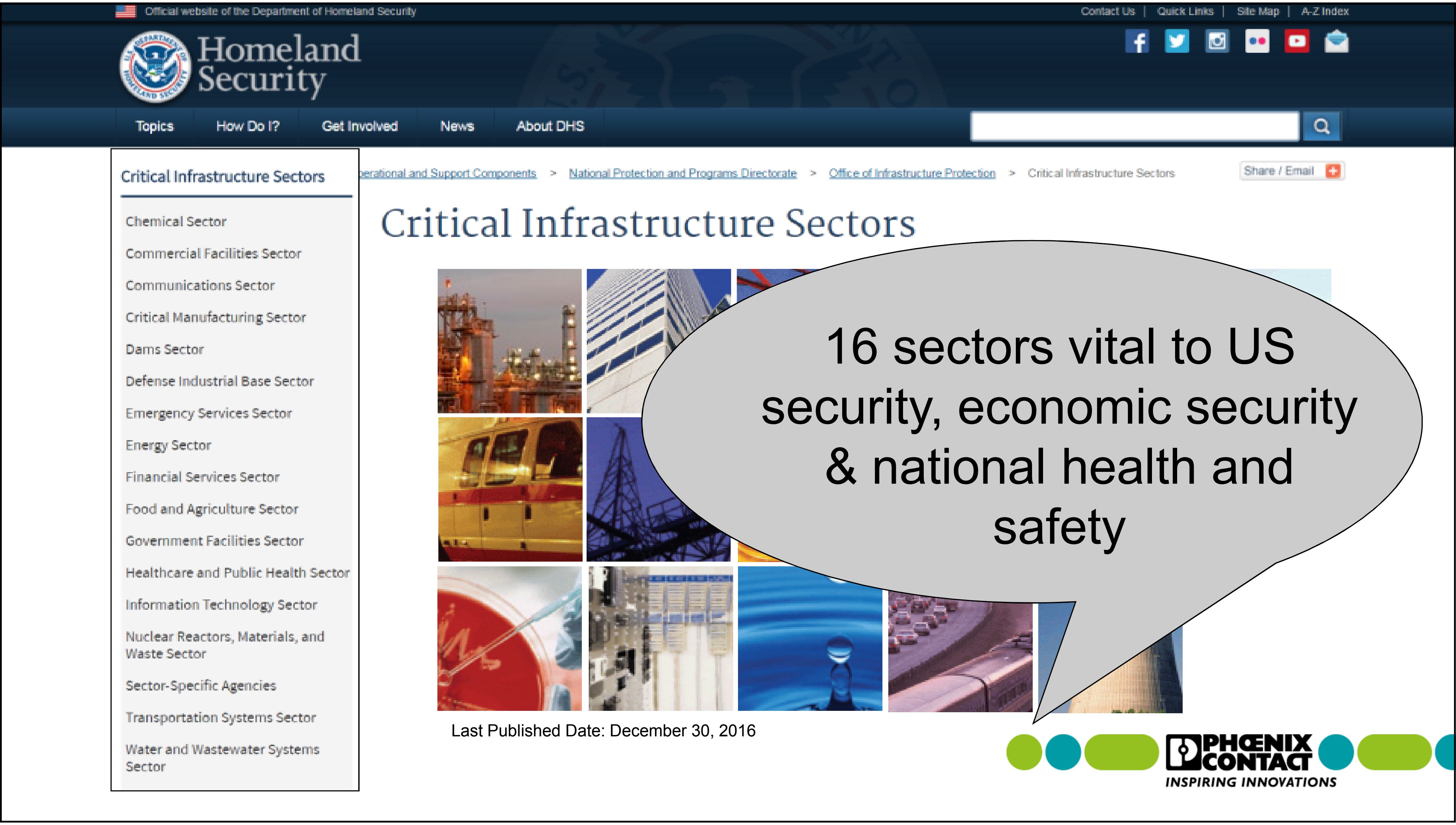


SONICWALL™

2016 Dell Security – Annual Threat Report

Breaches in 2015 succeeded not because the victims lacked security altogether, but because thieves found and exploited a small hole in their security program.

PHOENIX CONTACT
INSPIRING INNOVATIONS



Official website of the Department of Homeland Security

Contact Us | Quick Links | Site Map | A-Z Index

Homeland Security

perational and Support Components > National Protection and Programs Directorate > Office of Infrastructure Protection > Critical Infrastructure Sectors

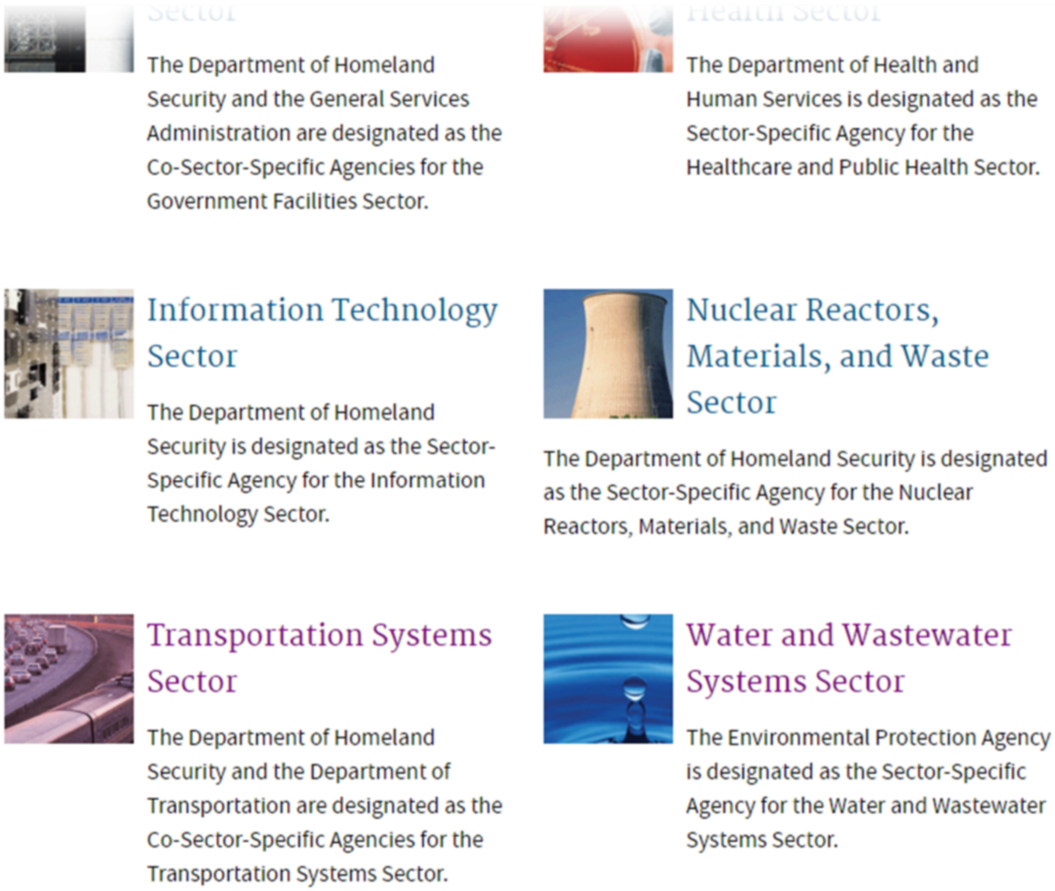
Critical Infrastructure Sectors

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Sector-Specific Agencies
- Transportation Systems Sector
- Water and Wastewater Systems Sector

Critical Infrastructure Sectors

Last Published Date: December 30, 2016

16 sectors vital to US security, economic security & national health and safety



Sector

The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

Health Sector

The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Information Technology Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

Nuclear Reactors, Materials, and Waste Sector

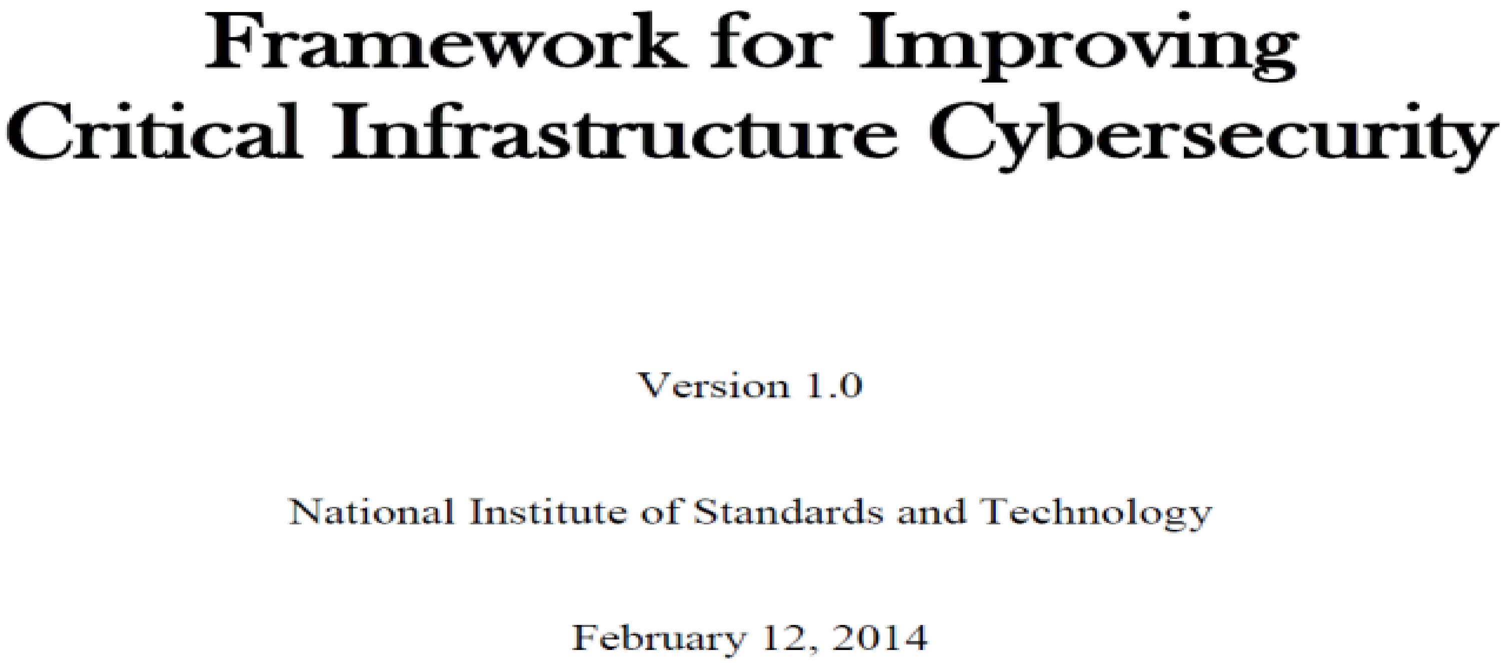
The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.

Transportation Systems Sector

The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Water and Wastewater Systems Sector

The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.



Framework for Improving Critical Infrastructure Cybersecurity

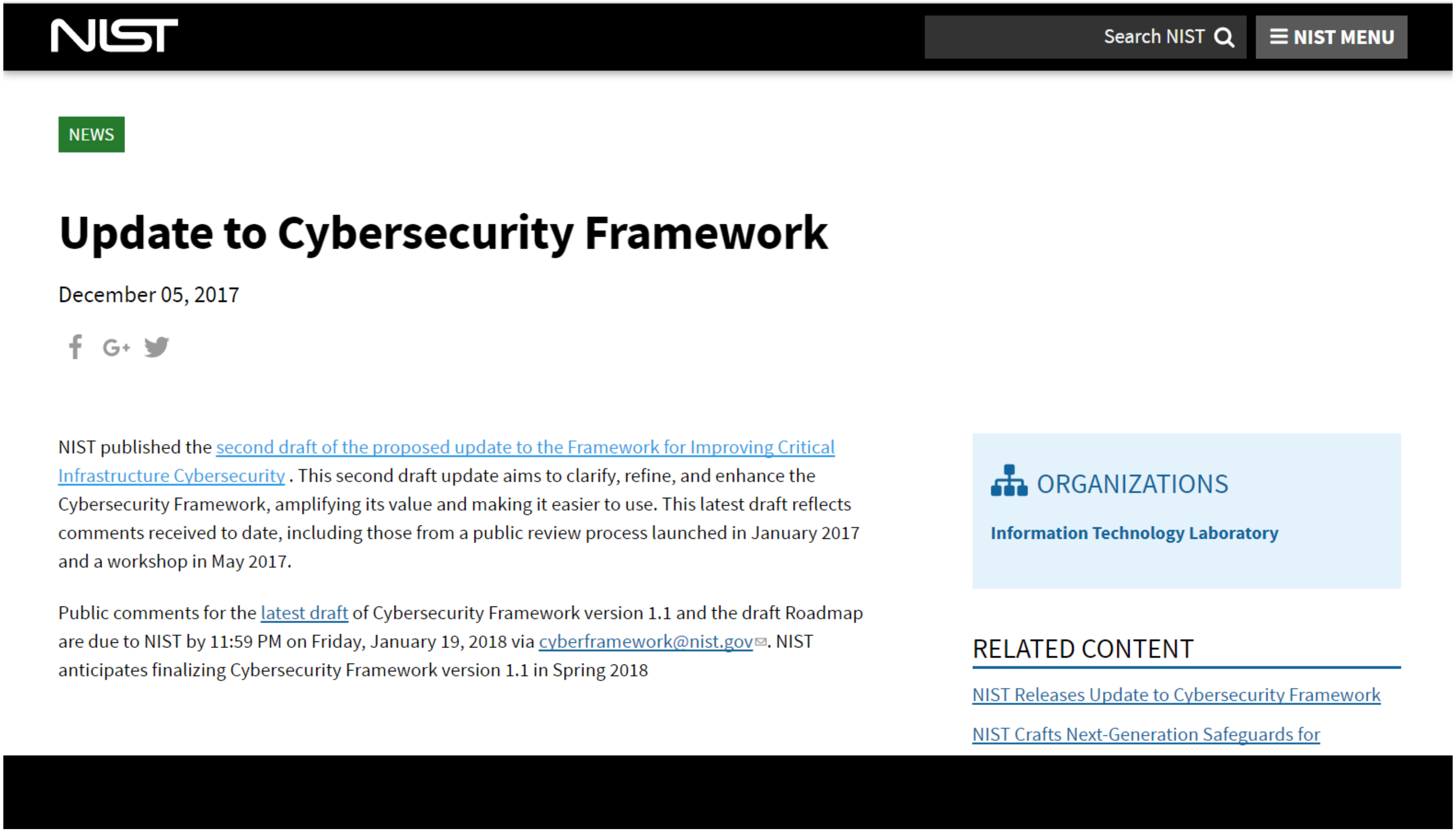
Version 1.0

National Institute of Standards and Technology

February 12, 2014

NIST Cybersecurity Framework

- Voluntary, risk-based approach for managing cybersecurity risks for critical infrastructure
- References industry standards and best practices to help organizations manage cybersecurity risks
- Addresses broad security needs of all critical sectors but **is not a one-size-fits-all approach**. Sector-specific guidance needed to address unique needs of each sector
- More info: **www.nist.gov/cyberframework**



Update to Cybersecurity Framework

December 05, 2017

NIST published the second draft of the proposed update to the Framework for Improving Critical Infrastructure Cybersecurity . This second draft update aims to clarify, refine, and enhance the Cybersecurity Framework, amplifying its value and making it easier to use. This latest draft reflects comments received to date, including those from a public review process launched in January 2017 and a workshop in May 2017.

Public comments for the latest draft of Cybersecurity Framework version 1.1 and the draft Roadmap are due to NIST by 11:59 PM on Friday, January 19, 2018 via cyberframework@nist.gov. NIST anticipates finalizing Cybersecurity Framework version 1.1 in Spring 2018

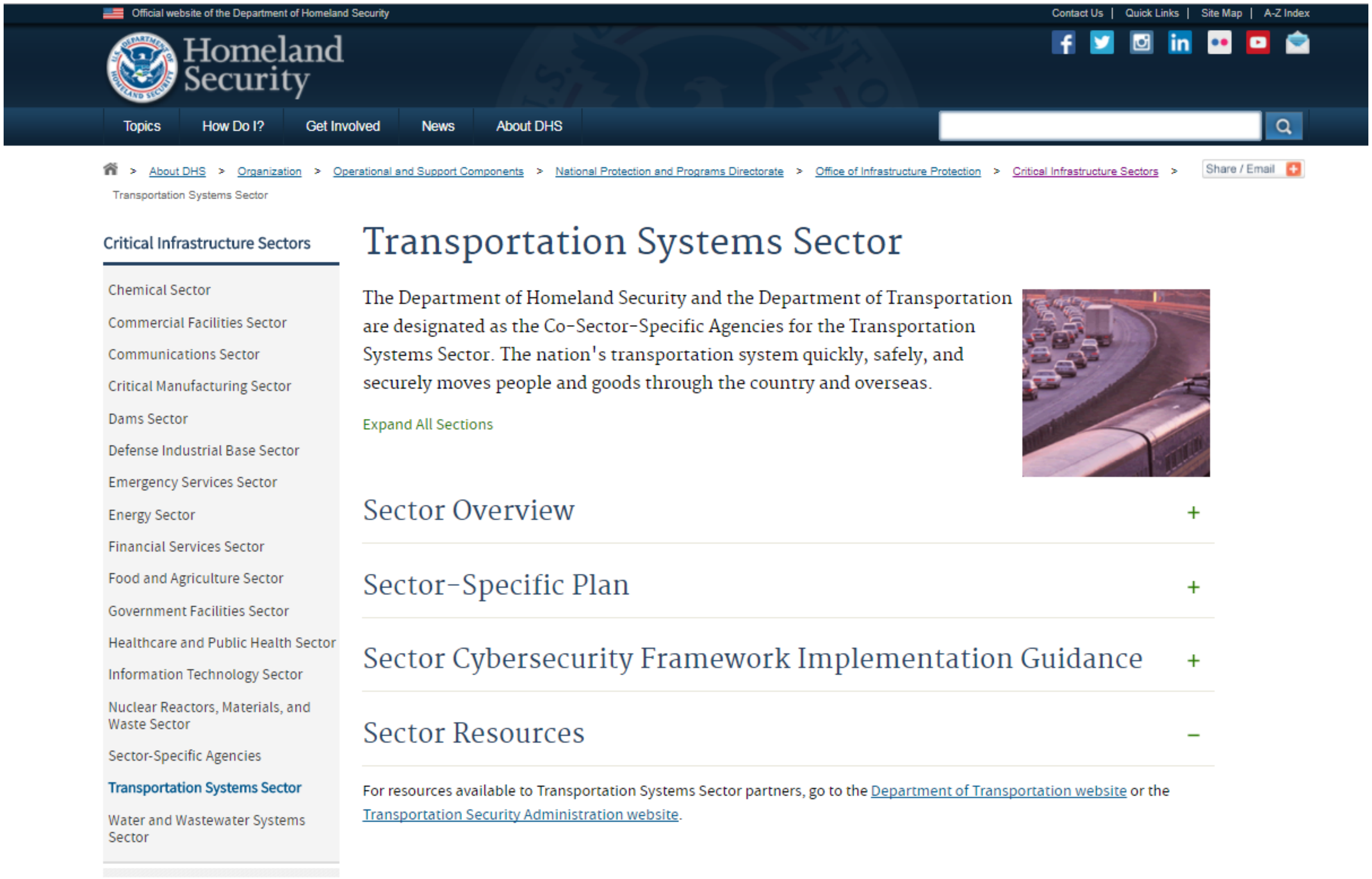
ORGANIZATIONS

Information Technology Laboratory

RELATED CONTENT

NIST Releases Update to Cybersecurity Framework

NIST Crafts Next-Generation Safeguards for



Official website of the Department of Homeland Security
Contact Us | Quick Links | Site Map | A-Z Index
Homeland Security
Topics
How Do I?
Get Involved
News
About DHS

> About DHS > Organization > Operational and Support Components > National Protection and Programs Directorate > Office of Infrastructure Protection > Critical Infrastructure Sectors > Transportation Systems Sector

Critical Infrastructure Sectors

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Sector-Specific Agencies
- **Transportation Systems Sector**
- Water and Wastewater Systems Sector

Transportation Systems Sector

The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector. The nation's transportation system quickly, safely, and securely moves people and goods through the country and overseas.

Expand All Sections

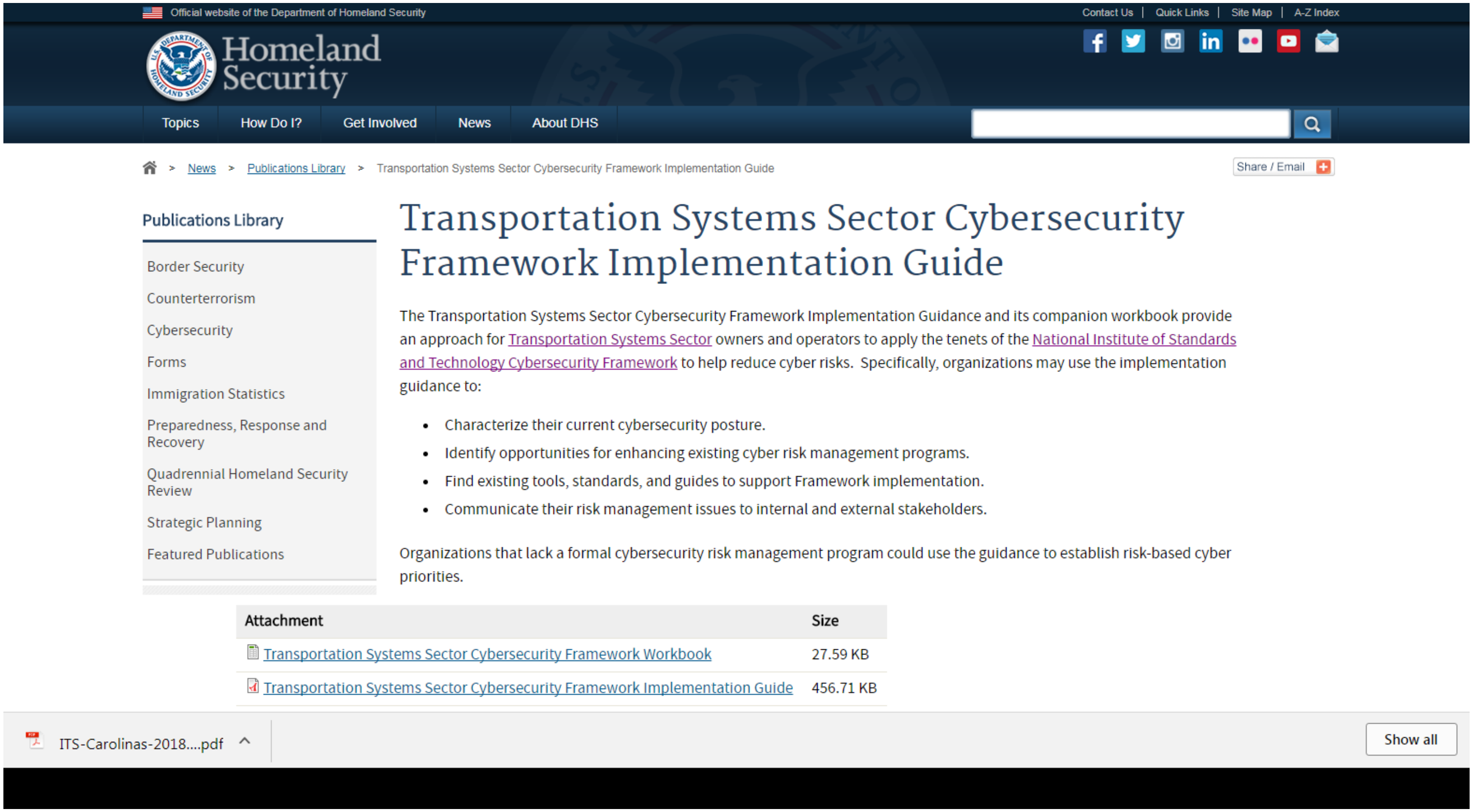
Sector Overview +

Sector-Specific Plan +

Sector Cybersecurity Framework Implementation Guidance +

Sector Resources –

For resources available to Transportation Systems Sector partners, go to the Department of Transportation website or the Transportation Security Administration website.


Official website of the Department of Homeland Security
Contact Us | Quick Links | Site Map | A-Z Index
Homeland Security
Topics
How Do I?
Get Involved
News
About DHS
> News > Publications Library > Transportation Systems Sector Cybersecurity Framework Implementation Guide
Share / Email
Publications Library
Border Security
Counterterrorism
Cybersecurity
Forms
Immigration Statistics
Preparedness, Response and Recovery
Quadrennial Homeland Security Review
Strategic Planning
Featured Publications
ITS-Carolinas-2018....pdf
Show all

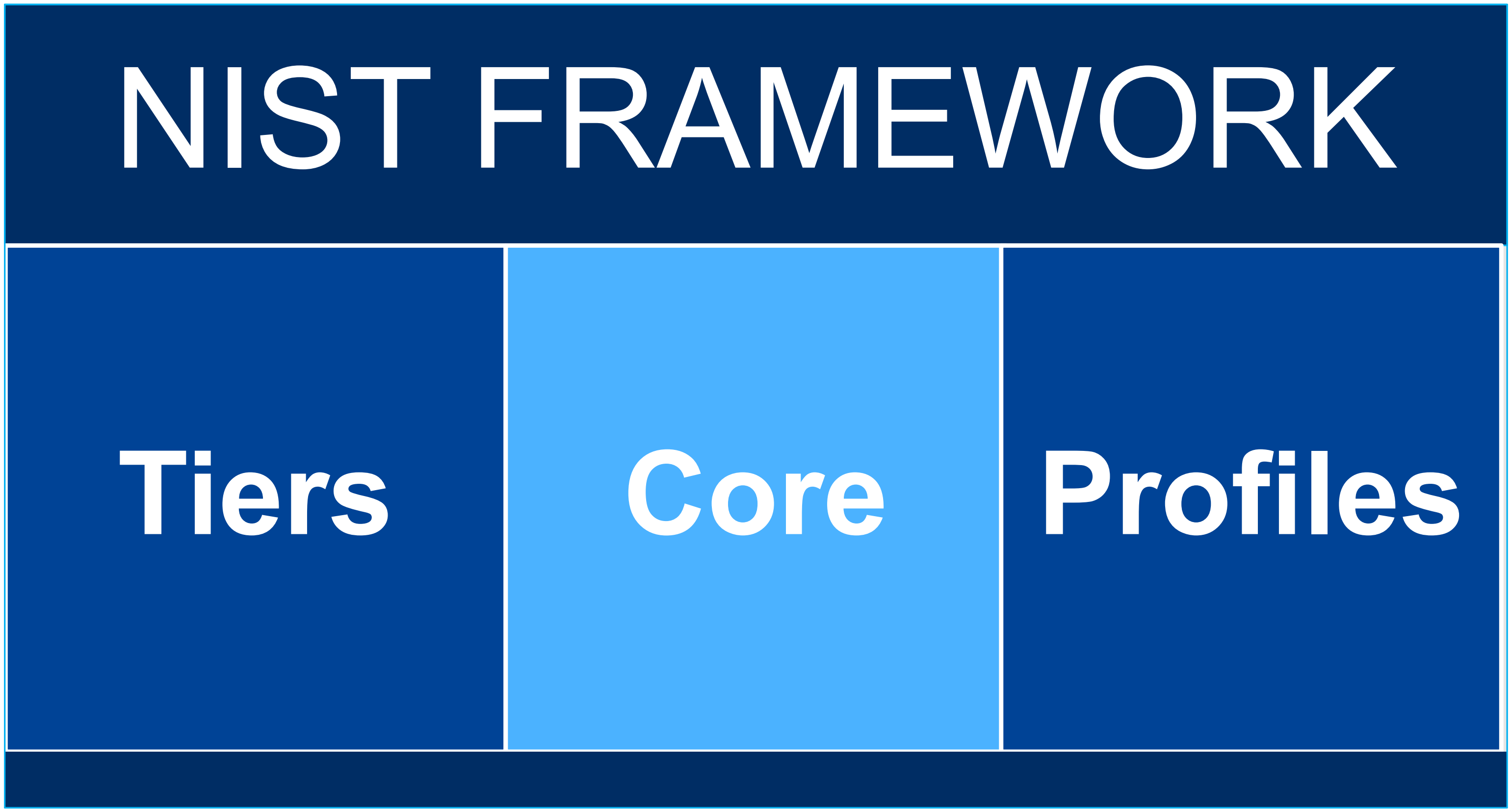
Transportation Systems Sector Cybersecurity Framework Implementation Guide

The Transportation Systems Sector Cybersecurity Framework Implementation Guidance and its companion workbook provide an approach for Transportation Systems Sector owners and operators to apply the tenets of the National Institute of Standards and Technology Cybersecurity Framework to help reduce cyber risks. Specifically, organizations may use the implementation guidance to:

- Characterize their current cybersecurity posture.
- Identify opportunities for enhancing existing cyber risk management programs.
- Find existing tools, standards, and guides to support Framework implementation.
- Communicate their risk management issues to internal and external stakeholders.

Organizations that lack a formal cybersecurity risk management program could use the guidance to establish risk-based cyber priorities.

Attachment	Size
Transportation Systems Sector Cybersecurity Framework Workbook	27.59 KB
Transportation Systems Sector Cybersecurity Framework Implementation Guide	456.71 KB



NIST FRAMEWORK

Tiers

Core

Profiles

Implementation Tiers

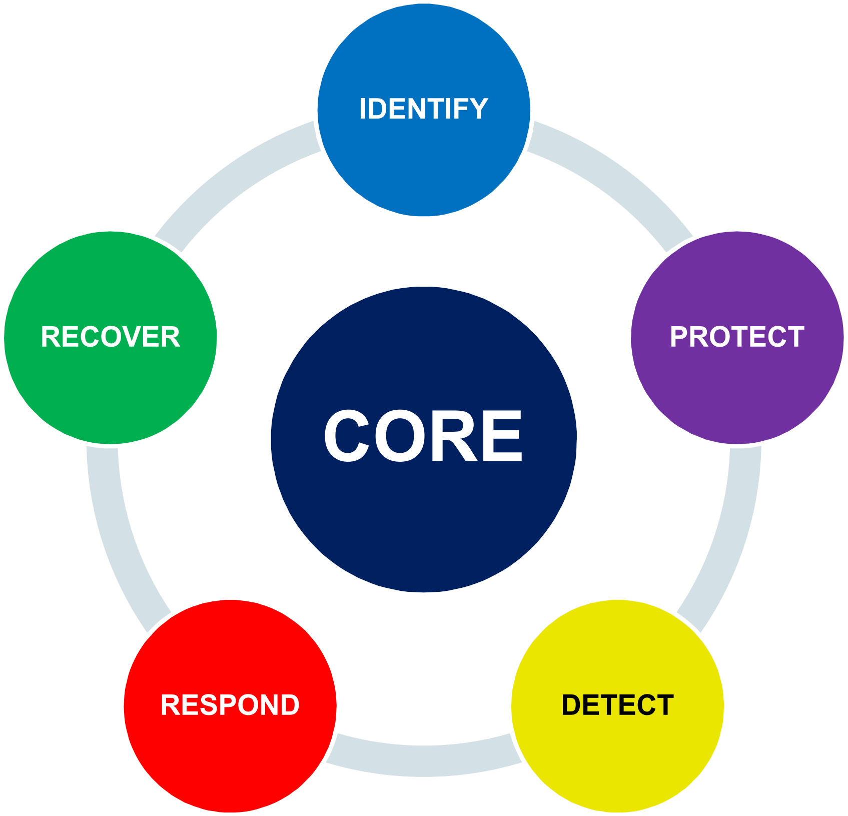
- Framework Implementation Tiers (“Tiers”) provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.

- Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective.
  - Tier 1: Partial
  - Tier 2: Risk Informed
  - Tier 3: Repeatable
  - Tier 4: Adaptive

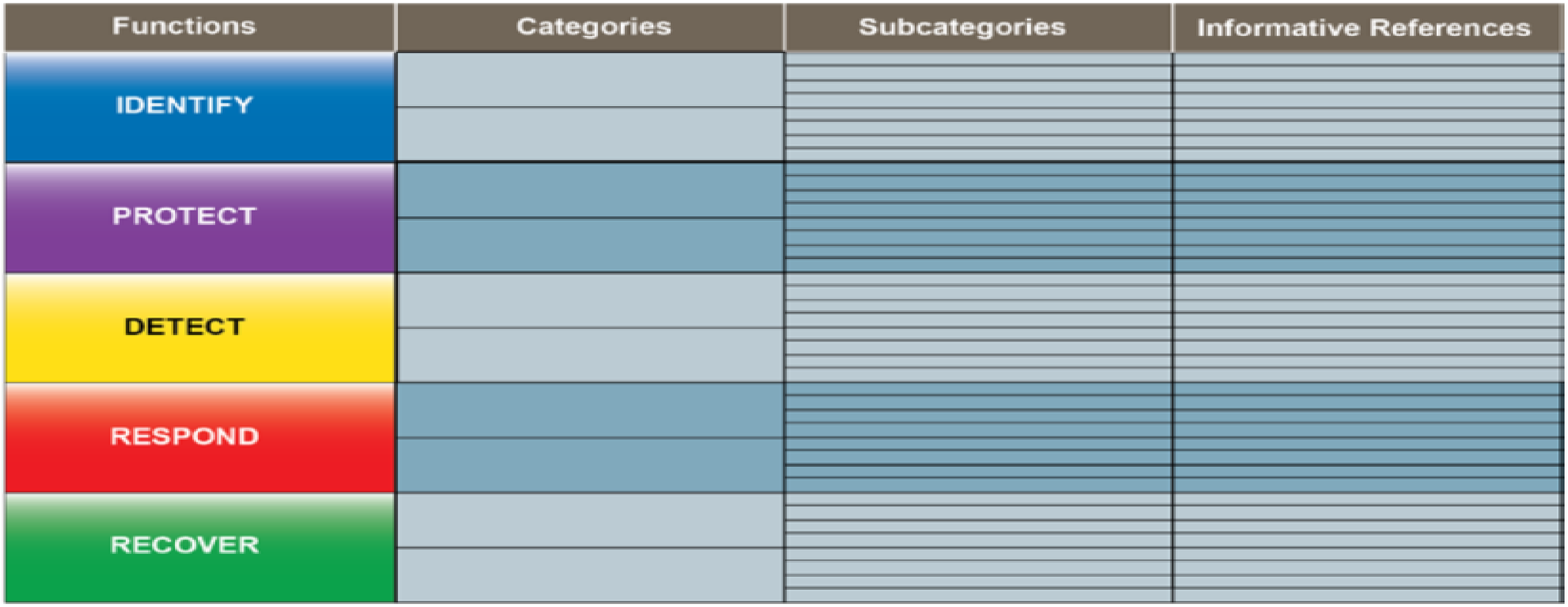
Profiles

- Alignment of Core functions with the business requirements, risk tolerance, and resources of the organization
- Useful in establishing a roadmap to move from “current” profile to “target” profile
- Does not prescribe Profile templates

Framework Core

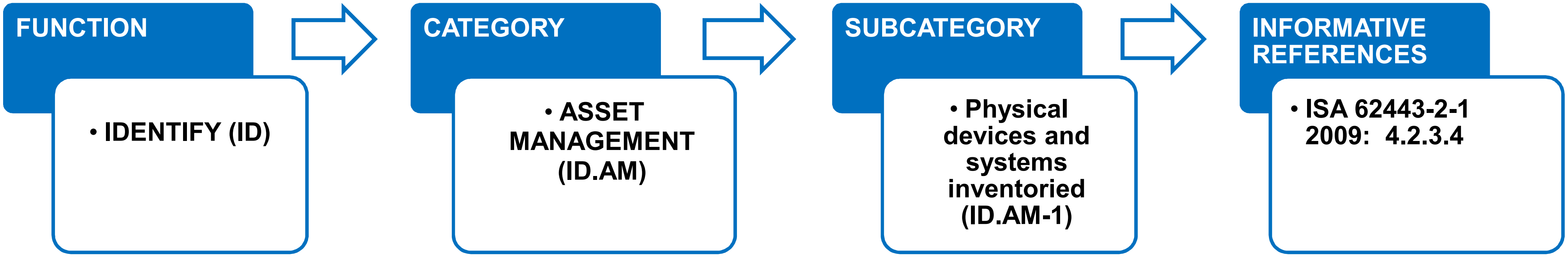


Framework Core



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Linking function to Informative References



FUNCTION

- IDENTIFY (ID)

CATEGORY

- ASSET MANAGEMENT (ID.AM)

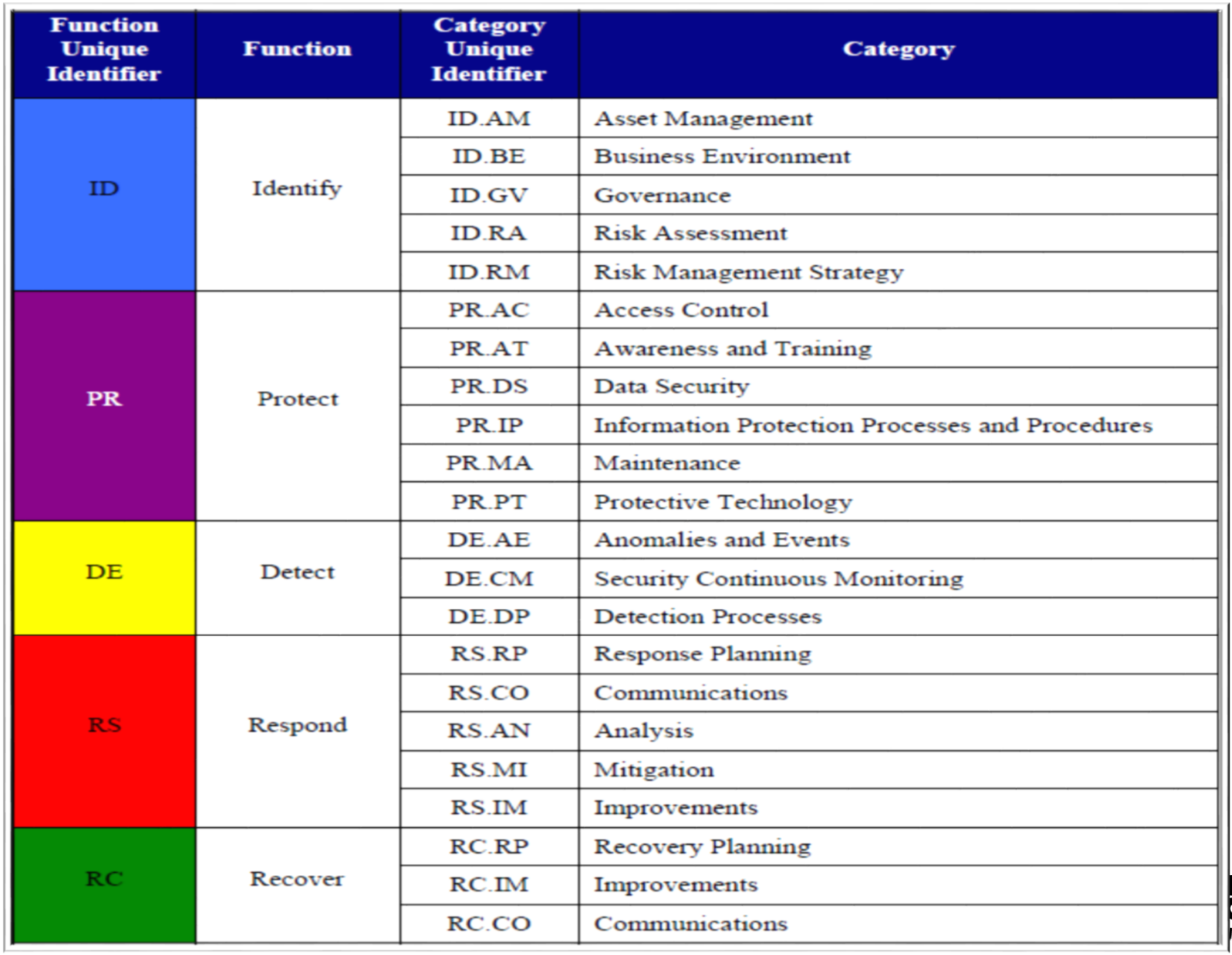
SUBCATEGORY

- Physical devices and systems inventoried (ID.AM-1)

INFORMATIVE REFERENCES

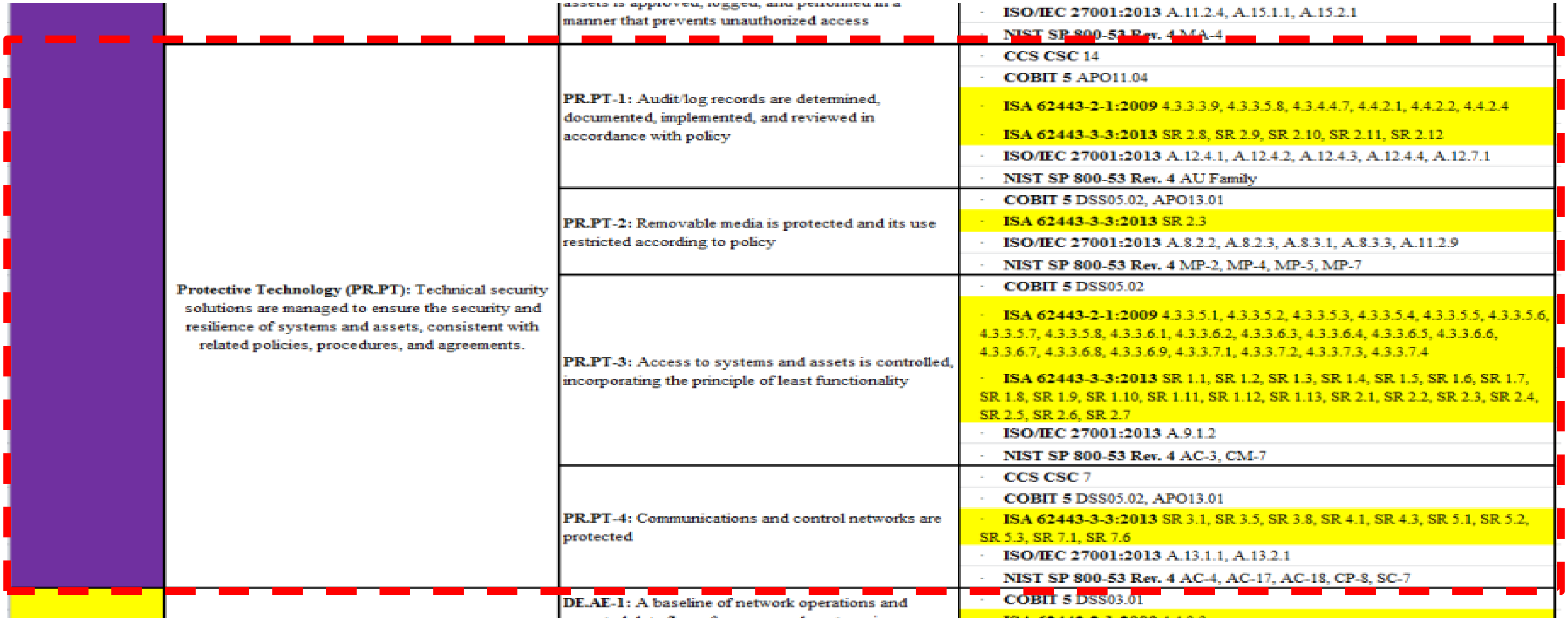
- ISA 62443-2-1 2009: 4.2.3.4

PHŒNIX CONTACT
INSPIRING INNOVATIONS



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

CSF Informative References



		assets is approved, logged, and performed in a manner that prevents unauthorized access	· ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 · NIST SP 800-53 Rev. 4 MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· **CCS CSC** 14 · **COBIT 5** APO11.04 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	· **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 2.3 · **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	· **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	· **CCS CSC** 7 · **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
		DE.AE-1: A baseline of network operations and	· **COBIT 5** DSS03.01

Summary

- Managing cyber risks is now the norm.
- Protecting critical infrastructure, including transportation systems is essential to our country's economic and national security.
- The NIST Cybersecurity Framework provides guidance and informative references for a comprehensive security plan.

Answers for the tough questions…

Could you have done more to prevent this attack?
Just 2 years till retirement!
Because we have a comprehensive security plan we were able to detect the cyber activity early and implement countermeasures quickly to mitigate the event. As a result the impact on public safety and our operations were minimized.

Easy questions for me?

PHOENIX CONTACT
INSPIRING INNOVATIONS

Presenter

Don Dickinson

Senior Business Development Manager – Water Sector

Phoenix Contact USA

e-mail: ddickinson@phoenixcon.com

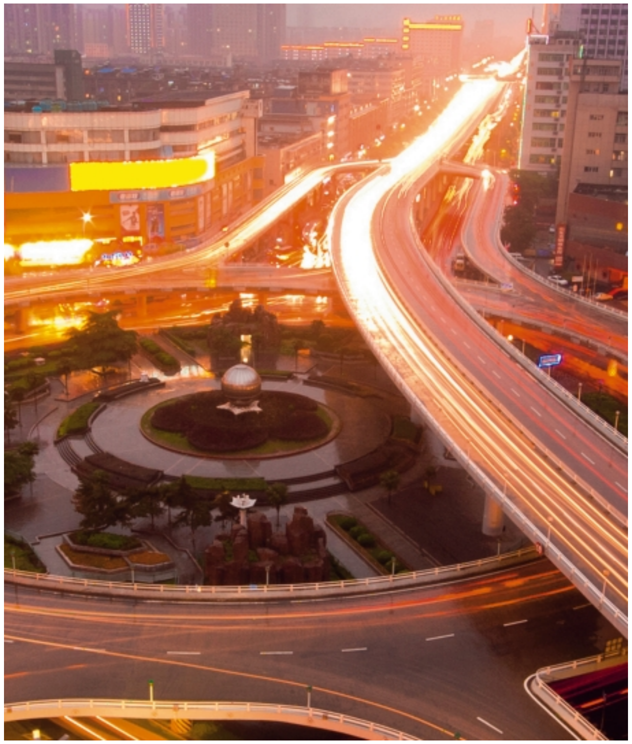
Request white paper: “Cyber White Paper” in Subject Line

Cybersecurity: Going Beyond Protection to Boost Resiliency

PHOENIX CONTACT
INSPIRING INNOVATIONS

ITS Carolinas 2018 Annual Meeting

Cybersecurity: Going Beyond Protection



Thank you

PHOENIX CONTACT
INSPIRING INNOVATIONS