SCAC's 51st Annual Conference

"Preventing and Mitigating Cyberattacks"

AUGUST 6, 2018
HILTON HEAD, SC

Tom Scott

Cyber Resilience Professional

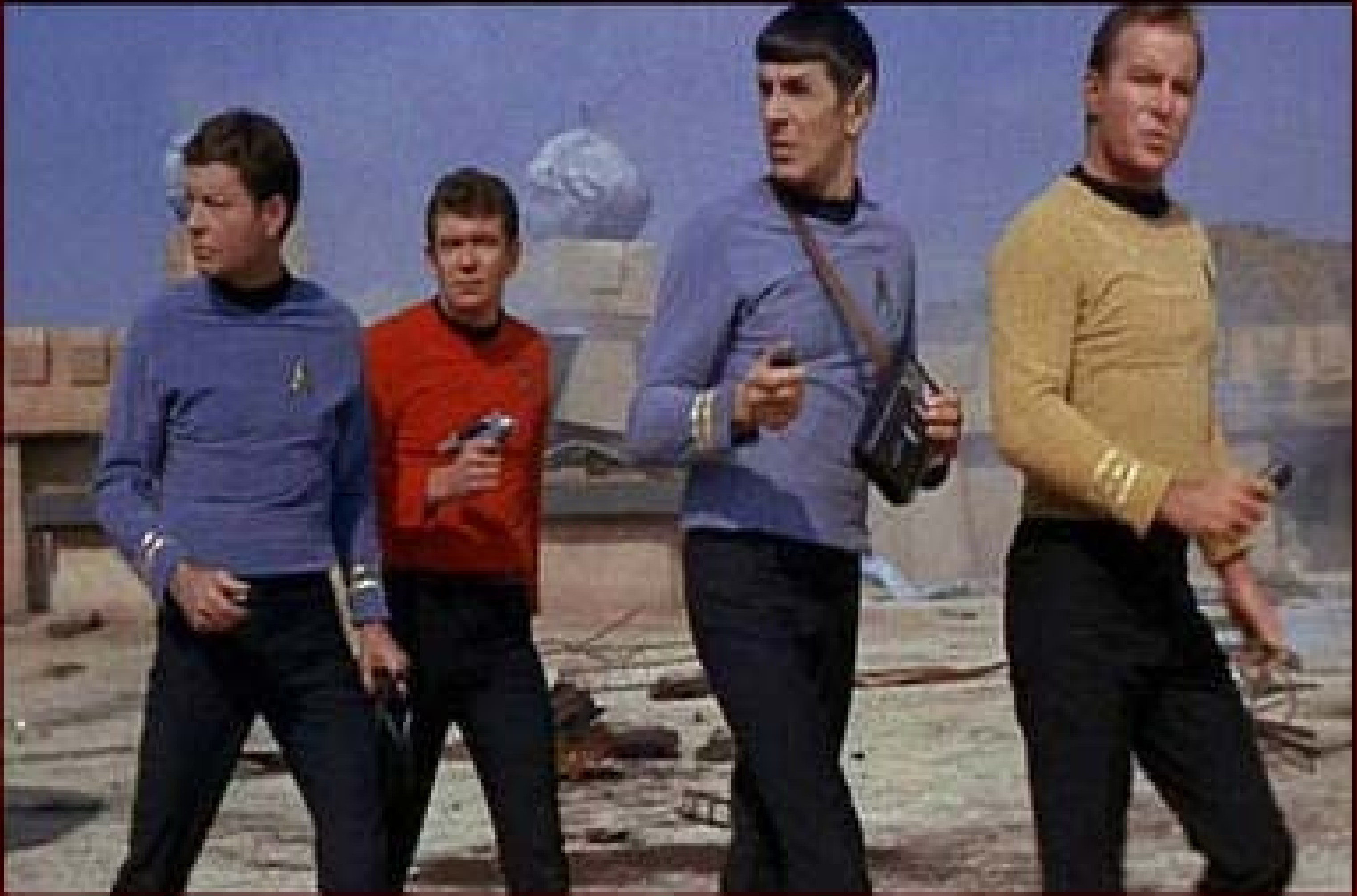
Certified Information Systems Security Professional

Certified Information Systems Auditor

Certified Risk Information Systems Control

Project Management Professional

Certified Critical Infrastructure Manager



EXPENDABILITY

KIRK, SPOCK, MCCOY, AND ENSIGN RICKY ARE BEAMING DOWN TO THE PLANET.
GUESS WHO'S NOT COMING BACK

What is SC Cyber?

SC Cyber is a statewide initiative, based at the University of South Carolina and with partners across all levels of academia, industry, and government, with a mission to develop the talent, techniques, and tools to defend critical, connected infrastructure within the state of South Carolina and the United States. In support of this mission, SC Cyber creates and offers programs for training and workforce development, education, advanced technology development and commercialization, and critical infrastructure protection.

The consortium that is **SC Cyber** is committed to developing is a unified approach to meeting the cybersecurity workforce and education needs in the state of South Carolina. **SC Cyber** carries out this mission by connecting a number of ongoing efforts throughout the state to create dynamic and collaborative partnerships. The consortium is working with cross sector partners ranging from K-12, higher education, workforce development, and the cyber community as a whole.

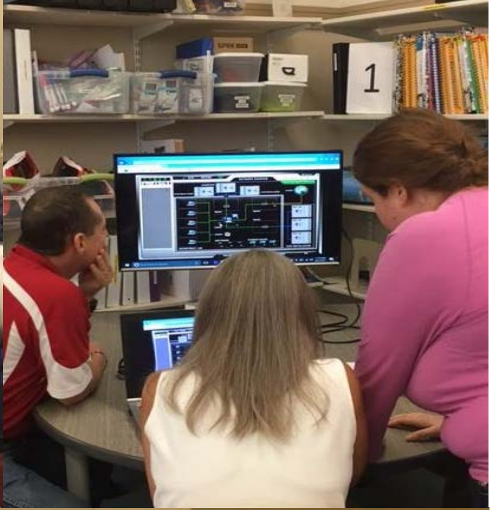
WORKFORCE DEVELOPMENT

EDUCATION

RESEARCH

PROTECTION

KNOWLEDGE MANAGEMENT



DAY OF CYBER CHALLENGE

36
Schools Logged Into Instructor Dashboard

1701
Participating Students

739
Participating Girls

962
Participating Boys

Workforce Development

SC Cyber has identified the development of a workforce as one of the keys to addressing SC's cybersecurity needs.

A well-governed, integrated workforce planning approach, steeped in best practices from governments and businesses, and aligned to the specialty areas of cybersecurity will provide improvements to the ability of organizations Carolina to accurately plan and protect their assets.

SC Cyber includes training new cybersecurity professionals, enhancing the credentialing of professionals, and retraining existing IT key components to developing a cyber workforce. new, in-demand cybersecurity professionals will the supply of cybersecurity workers in South filling a vital need.

PROGRAMS:

- Cyber Internship Program
- NSA "Day of Cyber" School Challenge

ACCOMPLISHMENTS:

- Launched Cyber Career Website
- Initiated First Cyber Internship Program
- Provided $2,500 in grants to SC K-12 Schools

Education

At the K-12 level, **SC Cyber** partners with organizations to enhance curricula already being developed, as well as to provide material support and additional connections to industry mentors, instructors, and specialists. Through partnerships, **SC Cyber** and its statewide collaborators enhances education for teachers and helps them to prepare students to safely participate in the digital world.

At the college and university level, **SC Cyber** primarily provides a repository for sharing among faculty specialists. By providing direct access to specialized, industry-focused educational materials and personnel, **SC Cyber** helps faculty across the state teach students timely, practical skills.

PROGRAMS:

- Cyber Merit Badge Camp
- CyberProtect Workshop
- Annual Cyber Safe Poster Contest
- Free On-Line Cyber Courses

ACCOMPLISHMENTS:

- Created online listing of cyber degree programs across South Carolina institutions
- Trained 40+ professionals in incident response/forensics
- 110 Boy Scouts completed their cyber chip certificate

SCCYBER
UPSTATE KICKOFF
CONFERENCE
sotera
Topics of Discussion
What is the path to becoming a security professional/hacker?
How does being a hacker change your approach to security co
tips do you have for those starting/advancing their securit
pe do you have for businesses hiring security profess
see the future of security research and innovation hea

Research

One of the greatest potential contributions to the security of South Carolina's critical infrastructure is the rapid sourcing, development, testing, and adoption of advanced cybersecurity technology. Given its capabilities, its university and small business partners, and its unique ability to connect early-stage, entrepreneurial teams with corporate or government mentorship, **SC Cyber** has an immense opportunity to accelerate technology development and commercialization among its partners.

PROGRAMS:

- Capstone projects
- Internship program

ACCOMPLISHMENTS:

- Secured NSA Grant in partnership with University of South Carolina and Savannah River National Lab
- Created mobile alert app for resilience of transportation infrastructure
- Showcased energy grid research to congressional staff

Protection

SC Cyber works closely with a variety of critical infrastructure partners including the FBI's InfraGard and SLED's Office of Homeland Security. By providing resources such as knowledge and training, these efforts help ensure a stable environment conducive to economic development efforts in the state of SC.

PROGRAMS:

- SC Infrastructure Protection Center
- Maritime Association Security Committee
- Cyber Table-Top Exercise Workshop

ACCOMPLISHMENTS:

- Hosted Homeland Security/SLED Cyber Monitoring Center
- Developed SC InfraGard Member Portal and Website
- Engaged Port/Maritime Cybersecurity Community

Knowledge Management

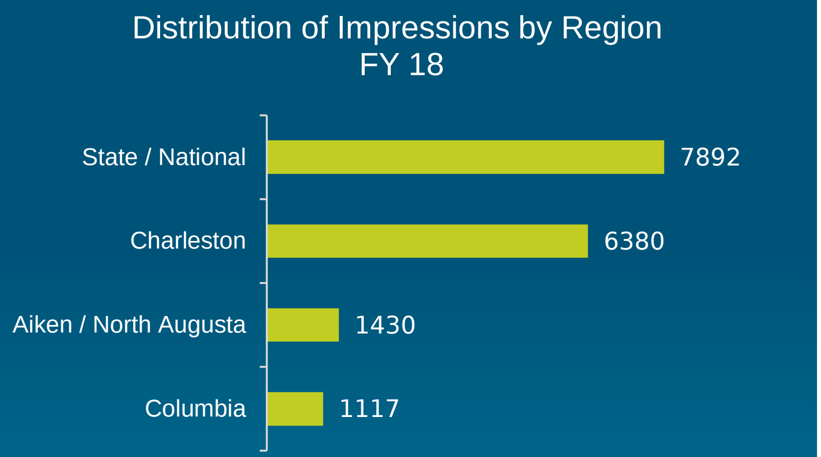
A recurring theme in cyber preparedness is the need for information sharing; this critically important need has been echoed throughout the early meetings of **SC Cyber**. Through real-time communication tools and channels, in-person meetings and exercises, and an Annual Cyber Summit, **SC Cyber** provides mechanisms for partners to collaborate on timely, critical issues facing their respective institutions.

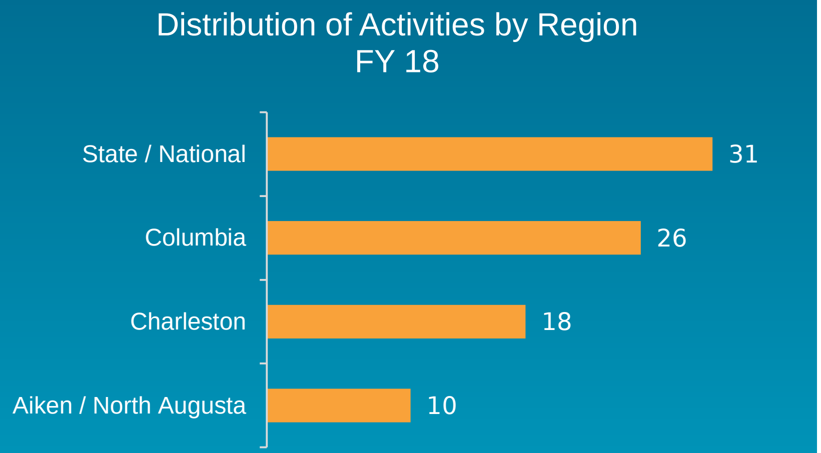
PROGRAMS:

- Annual Cybersecurity Summit for Industry
- SC Government Cybersecurity Symposium
- Cyber Education Symposium
- Cyber Webinar Series
- Cyber Ambassador Outreach Kits

ACCOMPLISHMENTS:

- Hosted 2nd Annual Cybersecurity Summit
- Engaged Civil Air Patrol for Outreach Events
- Presented Cyber Webinar Series Featuring Industry Leaders





FY 18 Geographic Priorities

CYBER EDUCATION & WORKFORCE PIPELINE

AIKEN/NORTH AUGUSTA

SC Cyber announced the expansion of its efforts to include the opening of an office in the North Augusta Municipal Center. Recognizing the rapidly expanding need for a holistic cyber ecosystem in the Central Savannah River area, SC Cyber is working with local leaders and communities to build an educational and workforce pipeline capable of meeting the areas' growing cyber demands.

PORT/MARITIME CYBERSECURITY

CHARLESTON

The Port of Charleston is one of the busiest and fastest growing container ports on the East coast, and it ranked eighth in the nation in 2017 for dollar value of international shipments, with cargo valued at more than $69 billion.

SC Cyber recognizes that due to their international nature, maritime activities are an increasingly attractive target for cybercrime. Maritime cyber crimes could disrupt business both at sea and on shore, causing heavy financial losses, and, worst case, loss of life and major environmental disaster. However, maritime cyber threats are not yet well understood or taken seriously. SC Cyber is working to change that.

The maritime domain is a vast network that must work together to prevent maritime cyber-attacks and manage the impacts of attacks when they occur.

CYBER LAW AND PUBLIC POLICY

COLUMBIA

South Carolina is uniquely poised to take lead in Cyber Public Policy/Law and Insurance.

Focusing on the Statehouse and the need for continued understanding of the software-based economy we live in, SC Cyber is working closely with groups like the SC Bar Technology Committee and the USC School of Law to examine the impact of cyber on public policy.

Membership Engagement

NETWORKING

SC Cyber is dedicated to expanding its membership base and the multiple connections to the vast network of cybersecurity professionals throughout industry, academia, and government.

BENEFITS

By definition, SC Cyber is a collaborative effort. Colloquially, it is best described as a consortium of participating members spanning all levels of academia, industry, and government to include institutions, agencies, companies small and large, nonprofit and community organizations, and individuals with ties to the security of our state.

- Discounted rates for training programs offered through SC Cyber
- Discounted or free admission to workshops and events
- Access to members-only newsletter, lists and information
- Inclusion in SC Cyber member directory
- Eligible to volunteer on committees

4,680

attendees at 14 outreach events

2,970

attendees at 28 presentations

7,550

attendees at 29 partnership and engagement events

2,240

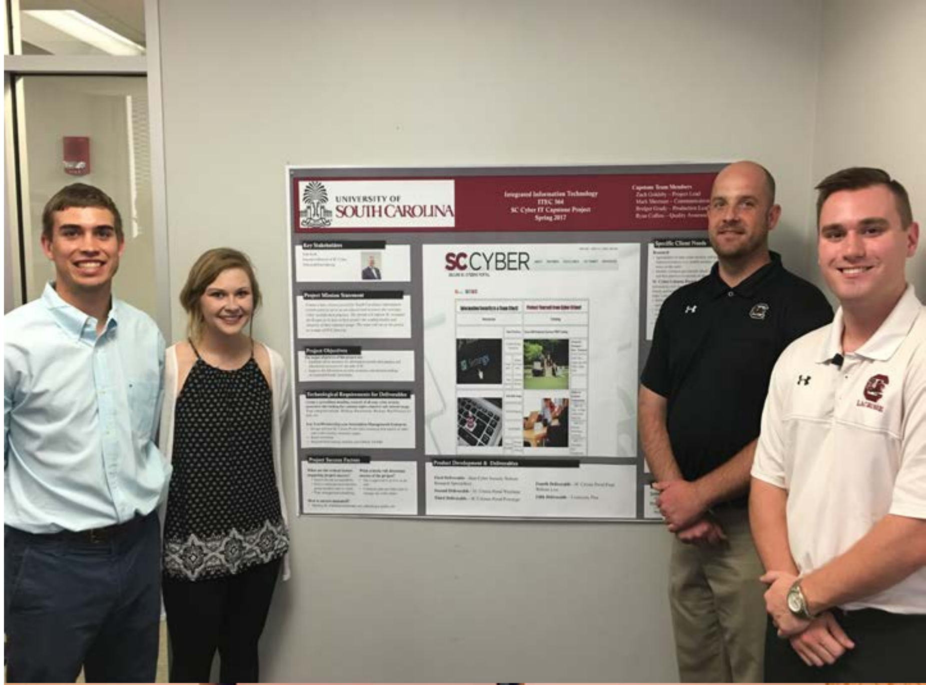
participants at 12 workshops

Student Engagement

UNIVERSITY OF SOUTH CAROLINA SENIOR CAPSTONE PROJECTS & INTERNSHIPS

In conjunction with USC’s College of Engineering and Computing, SC Cyber engaged 3 separate Capstone projects over the past year. These projects are conducted by Senior Information Technology majors, who are given the opportunity to work on real-life projects for clients in the field of IT. In addition to these Capstone projects, SC Cyber’s internship program has given 11 college students the opportunity to gain valuable experience in the Cybersecurity Industry. Each intern is given a specific project to complete over their time as an intern, which allows them to understand how real-life projects are conducted and some of the struggles that come along with completing a project.

1,530	11
Combined Work Hours	Interns Placed



CYBER CAREER SITE

Cybersecurity has emerged as one of the leading creators of jobs and opportunity for all economic sectors. **SC Cyber**’s career site allows job seekers to search for open positions within the cybersecurity field.

CYBER NEWS

Staying up-to-date with the latest cyber attacks ensures that that an organization can take measures to stay protected from those certain attacks. At **SC Cyber**, we make sure our community is aware of the latest cyber news so they can prevent attacks from happening in their organization.

CYBER CALENDAR

Find out about upcoming events and view photo galleries of past events! Using the **SC Cyber** calendar, you can register or purchase tickets for various upcoming events within the cyber community.

HIGHER ED DATABASE

Cybersecurity is a broad field with a number of specialized focus areas. The **SC Cyber** Higher Education Database helps students and educators identify Information Technology programs within the state of South Carolina.

SCIPC RESOURCES

Responding to a need identified through the SLED Office of Homeland Security, **SC Cyber** has created the South Carolina Infrastructure Protection Center (SCIPC) to provide resources to the infrastructure protection community.

EDUCATOR TOOLS

To help educators, **SC Cyber** provides a variety of tools to include presentations on cyberbullying and workforce development. CyberProtect workshop materials are also made available to teachers and educators across the Palmetto State.

Our website serves as a central informational hub to promote SC Cyber’s programs and activities, which include:

- Membership information
- News & Newsletters
- Cyber Calendar
- Webinars
- Resources and Tools
- Lists of Partners/Sponsors
- Contact information

Partners

EDTS CYBER

APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY

mcmillan pazdan smith ARCHITECTURE

SCANA® ENERGY

RPI GROUP

JTi JohnsTek Strategic Technology Engineering

SAIC Redefining Ingenuity™

Edgefield PC

CLEMSON UNIVERSITY SOUTH CAROLINA 1889

TRIDENT TECHNICAL COLLEGE

Dragoon Security Group

SOUTH CAROLINA NATIONAL GUARD

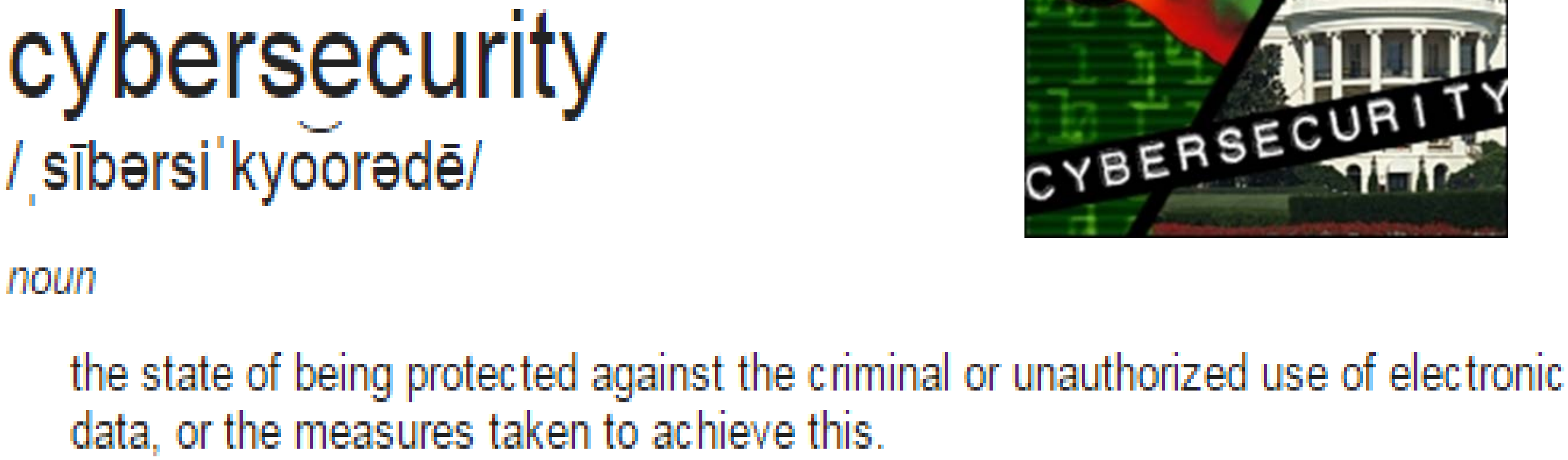
soteria

TeamLogicIT® Your Technology Advisor

KUMA

COLSA CORPORATION

What is Cyber Security?

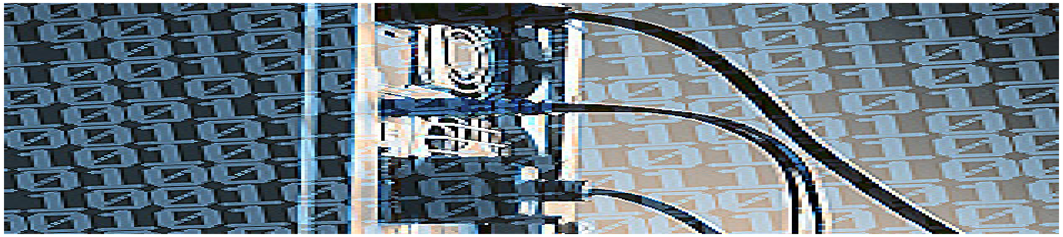


cybersecurity

/ˌsībərsiˈkyo͝orədē/

noun

the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.



Organized crime

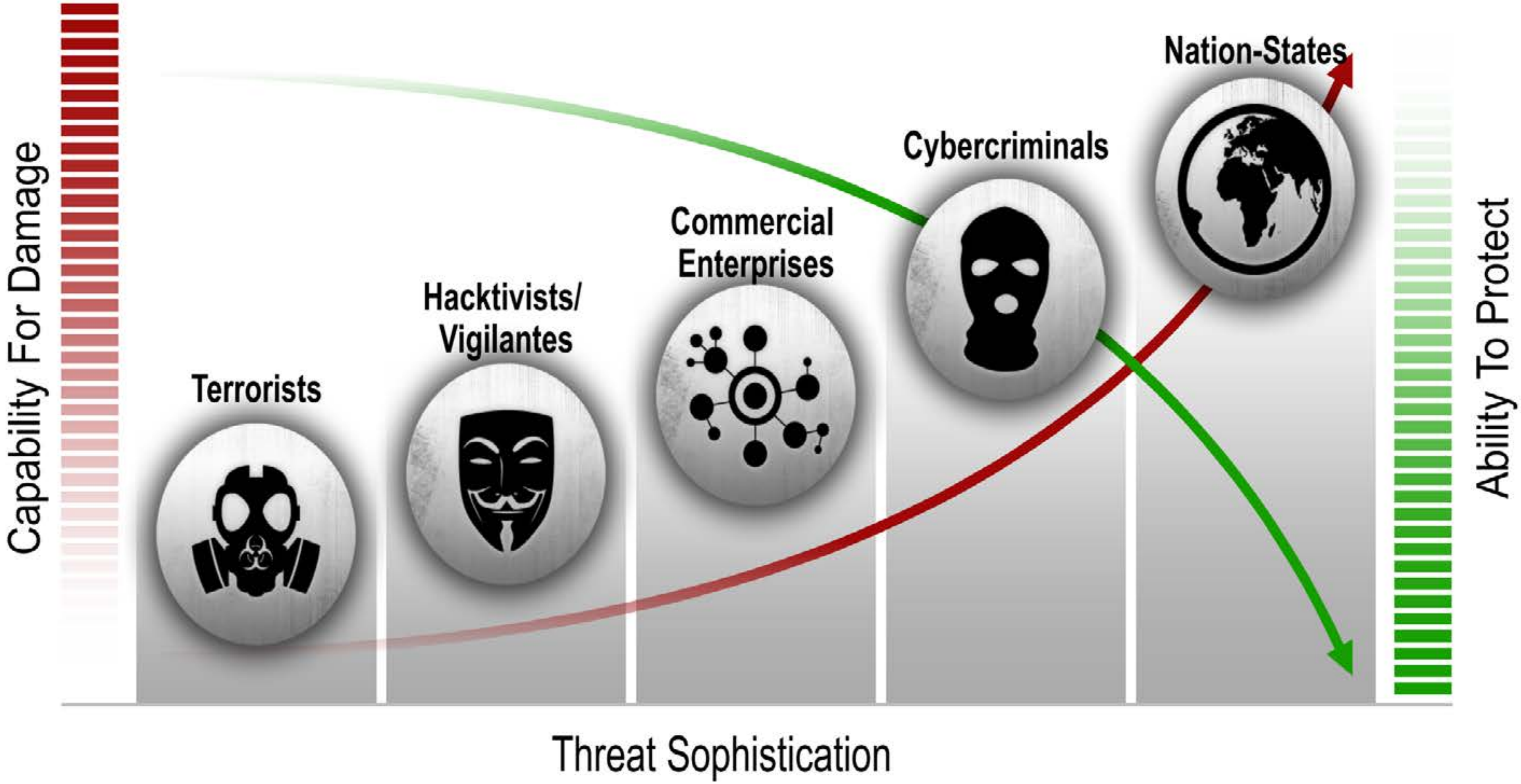
Nation states

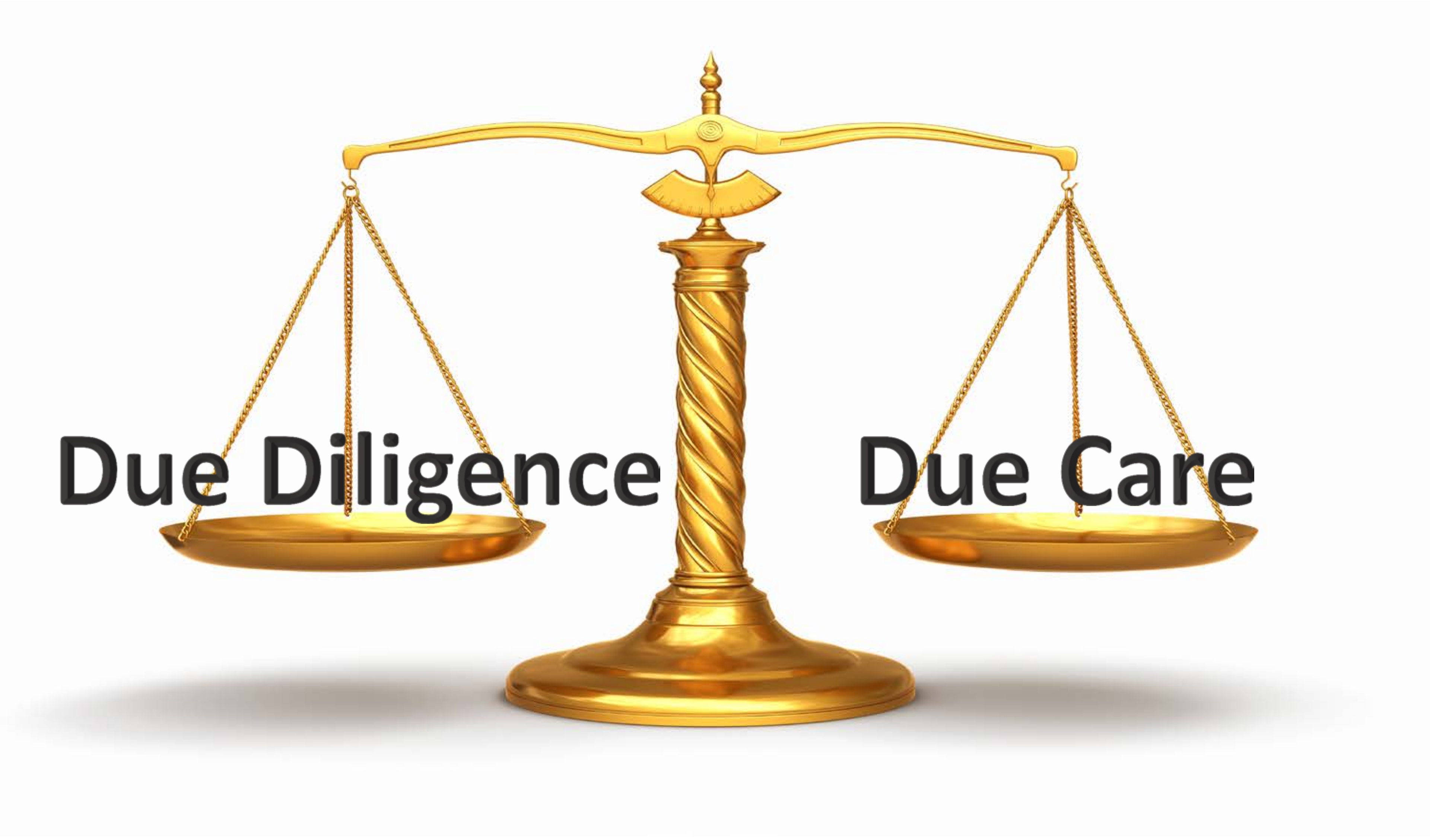
Insiders

Cyber-terrorists / Hacktivists

Others…

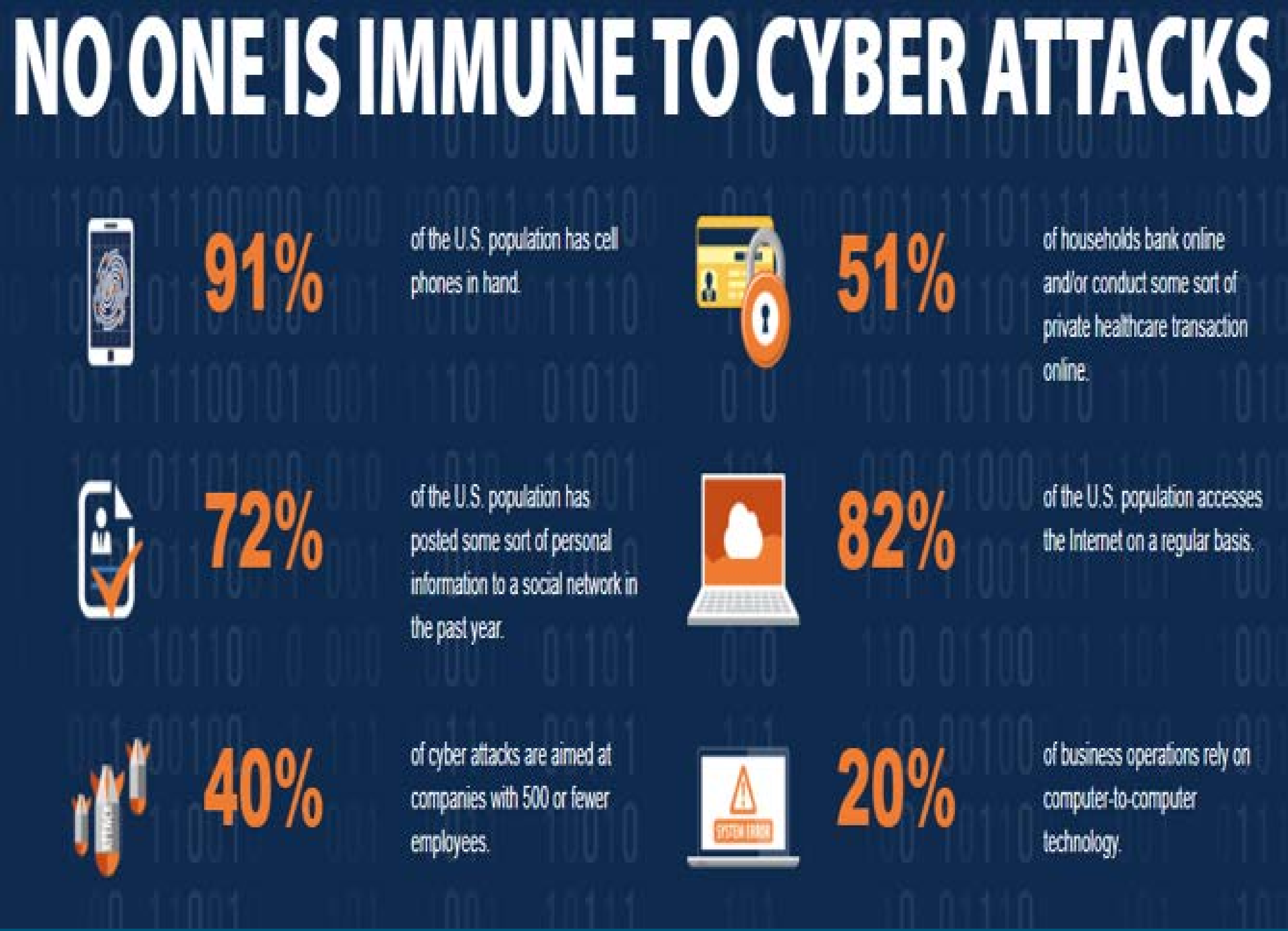
CYBER THREATS





Due Diligence

Due Care



NO ONE IS IMMUNE TO CYBER ATTACKS

91% of the U.S. population has cell phones in hand.

72% of the U.S. population has posted some sort of personal information to a social network in the past year.

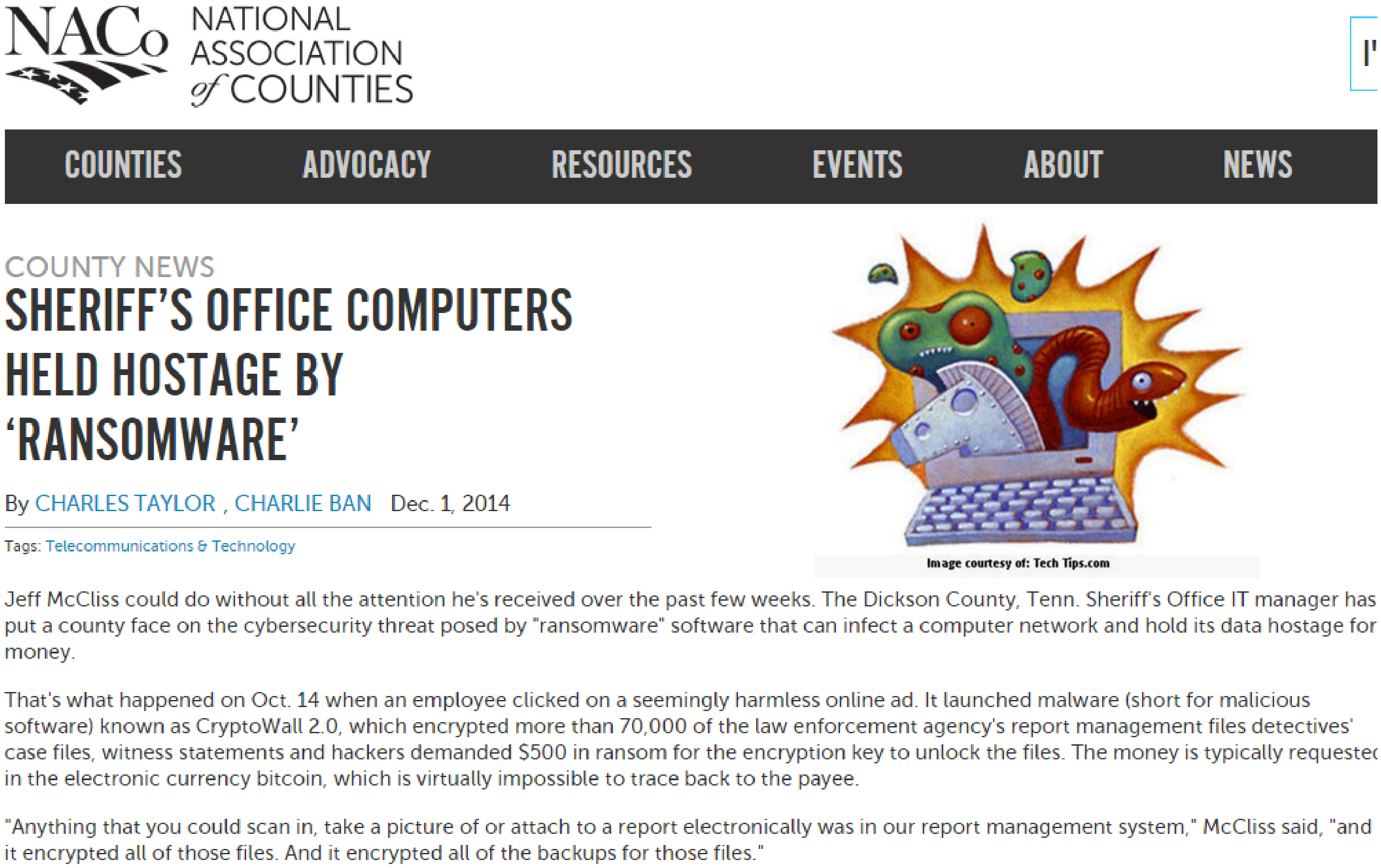
40% of cyber attacks are aimed at companies with 500 or fewer employees.

51% of households bank online and/or conduct some sort of private healthcare transaction online.

82% of the U.S. population accesses the Internet on a regular basis.

20% of business operations rely on computer-to-computer technology.

Could this happen to you?



COUNTY NEWS

SHERIFF'S OFFICE COMPUTERS HELD HOSTAGE BY 'RANSOMWARE'

By CHARLES TAYLOR , CHARLIE BAN Dec. 1, 2014

Tags: Telecommunications & Technology

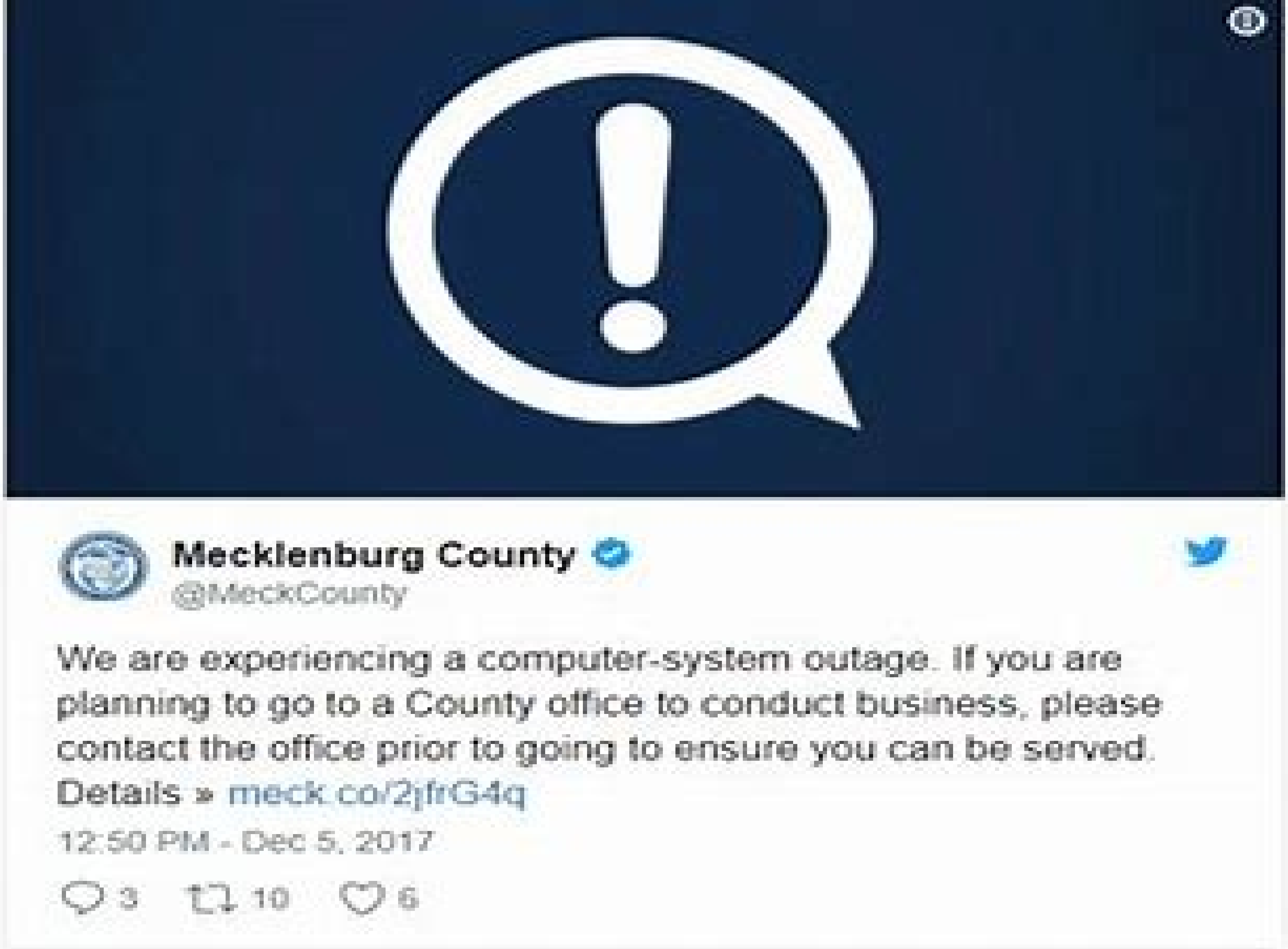
Image courtesy of: Tech Tips.com

Jeff McCliss could do without all the attention he's received over the past few weeks. The Dickson County, Tenn. Sheriff's Office IT manager has put a county face on the cybersecurity threat posed by "ransomware" software that can infect a computer network and hold its data hostage for money.

That's what happened on Oct. 14 when an employee clicked on a seemingly harmless online ad. It launched malware (short for malicious software) known as CryptoWall 2.0, which encrypted more than 70,000 of the law enforcement agency's report management files detectives' case files, witness statements and hackers demanded $500 in ransom for the encryption key to unlock the files. The money is typically requestec in the electronic currency bitcoin, which is virtually impossible to trace back to the payee.

"Anything that you could scan in, take a picture of or attach to a report electronically was in our report management system," McCliss said, "and it encrypted all of those files. And it encrypted all of the backups for those files."

MECKLENBURG COUNTY
MAY 20,1775
NORT
INA



Mecklenburg County

@MeckCounty

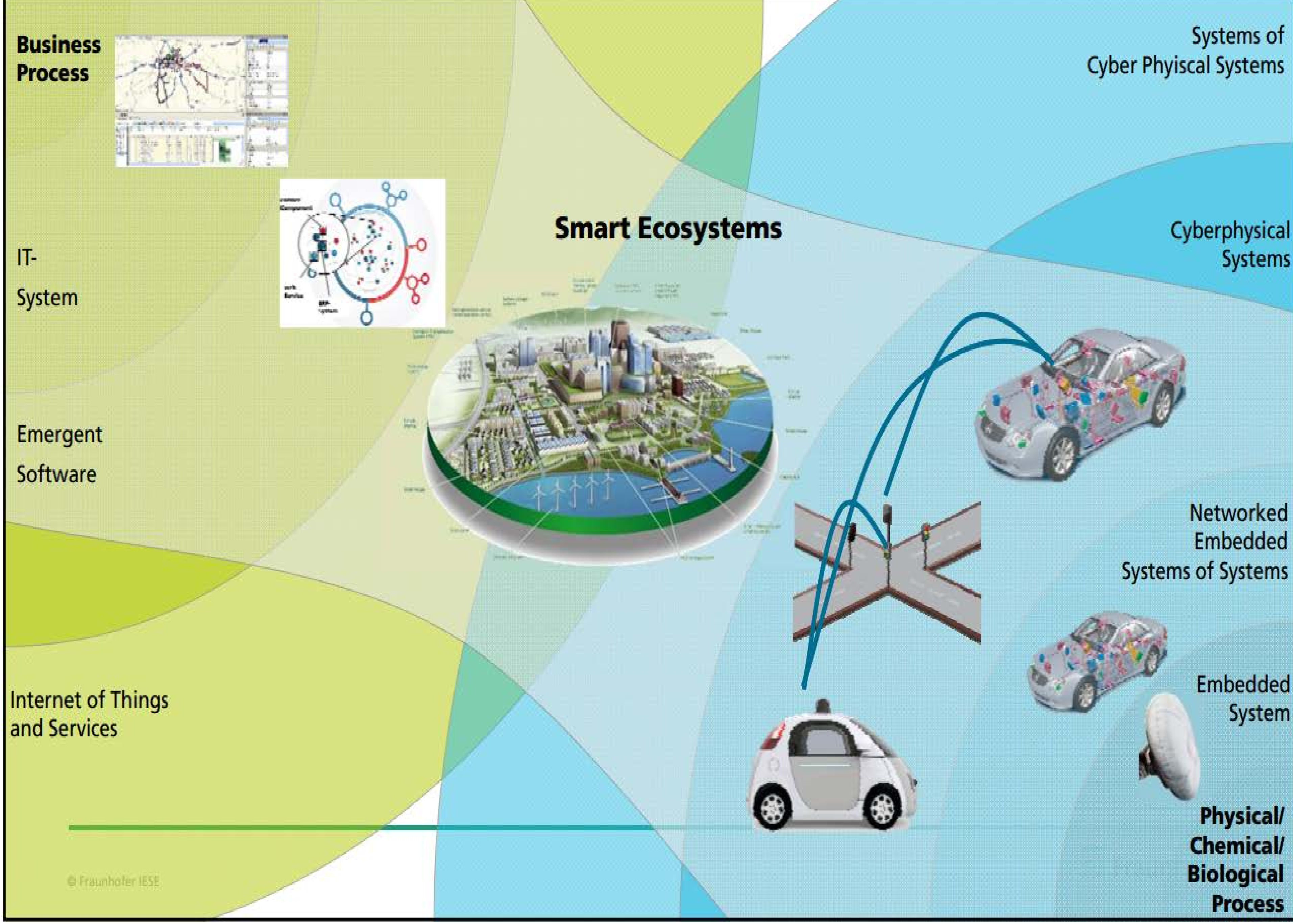
We are experiencing a computer-system outage. If you are planning to go to a County office to conduct business, please contact the office prior to going to ensure you can be served. Details » meck.co/2jfrG4q

12:50 PM - Dec 5, 2017

3 10 6

I shall infect network servers with something called "Ransomware" and hold an organization's data hostage for...

40 BITCOINS



Business Process

IT-System

Emergent Software

Internet of Things and Services

Smart Ecosystems

Systems of Cyber Phyiscal Systems

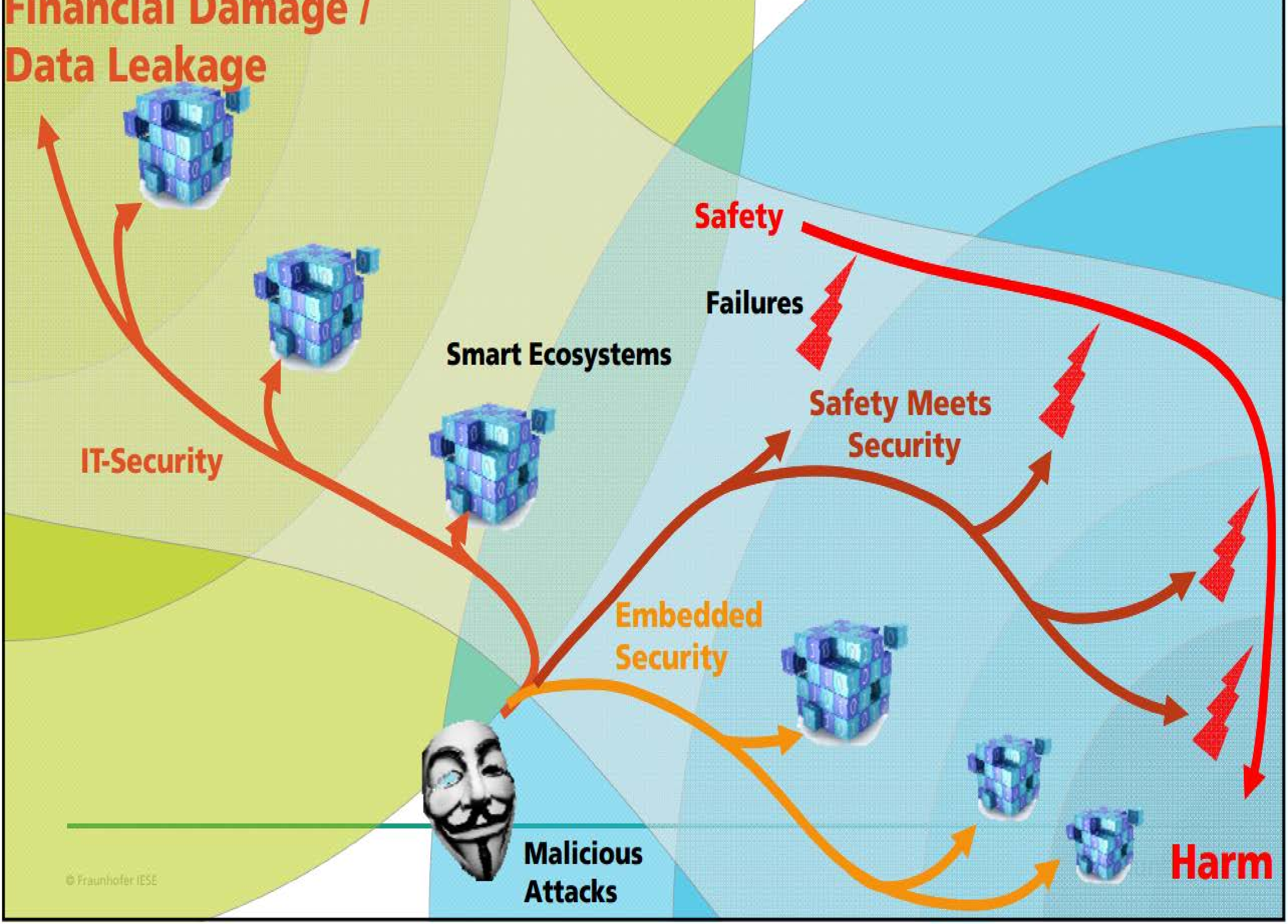
Cyberphysical Systems

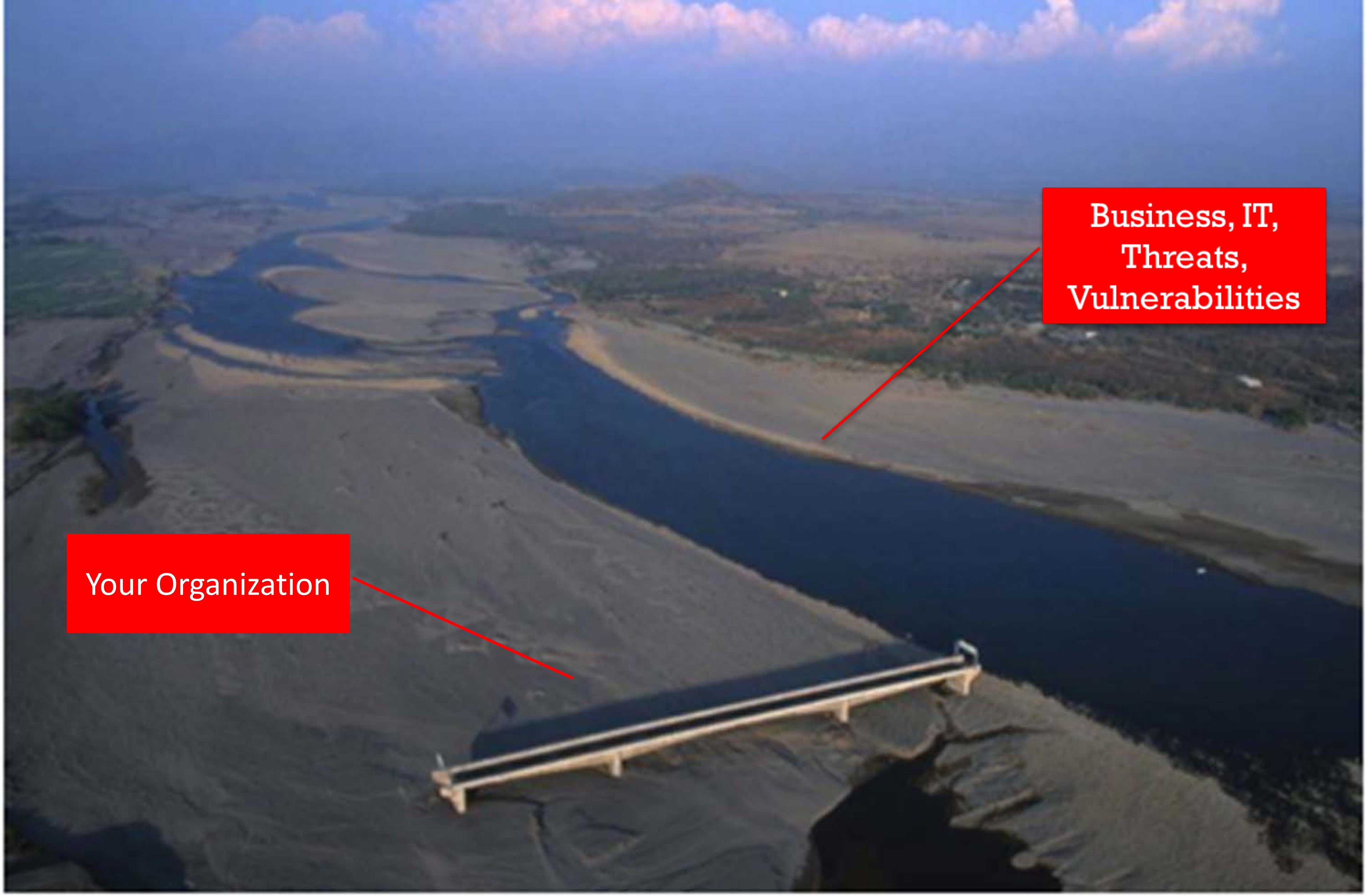
Networked Embedded Systems of Systems

Embedded System

Physical/ Chemical/ Biological Process

© Fraunhofer IESE


Financial Damage /
Data Leakage
Safety
Failures
Smart Ecosystems
Safety Meets
Security
IT-Security
Embedded
Security
Malicious
Attacks
Harm
© Fraunhofer IESE

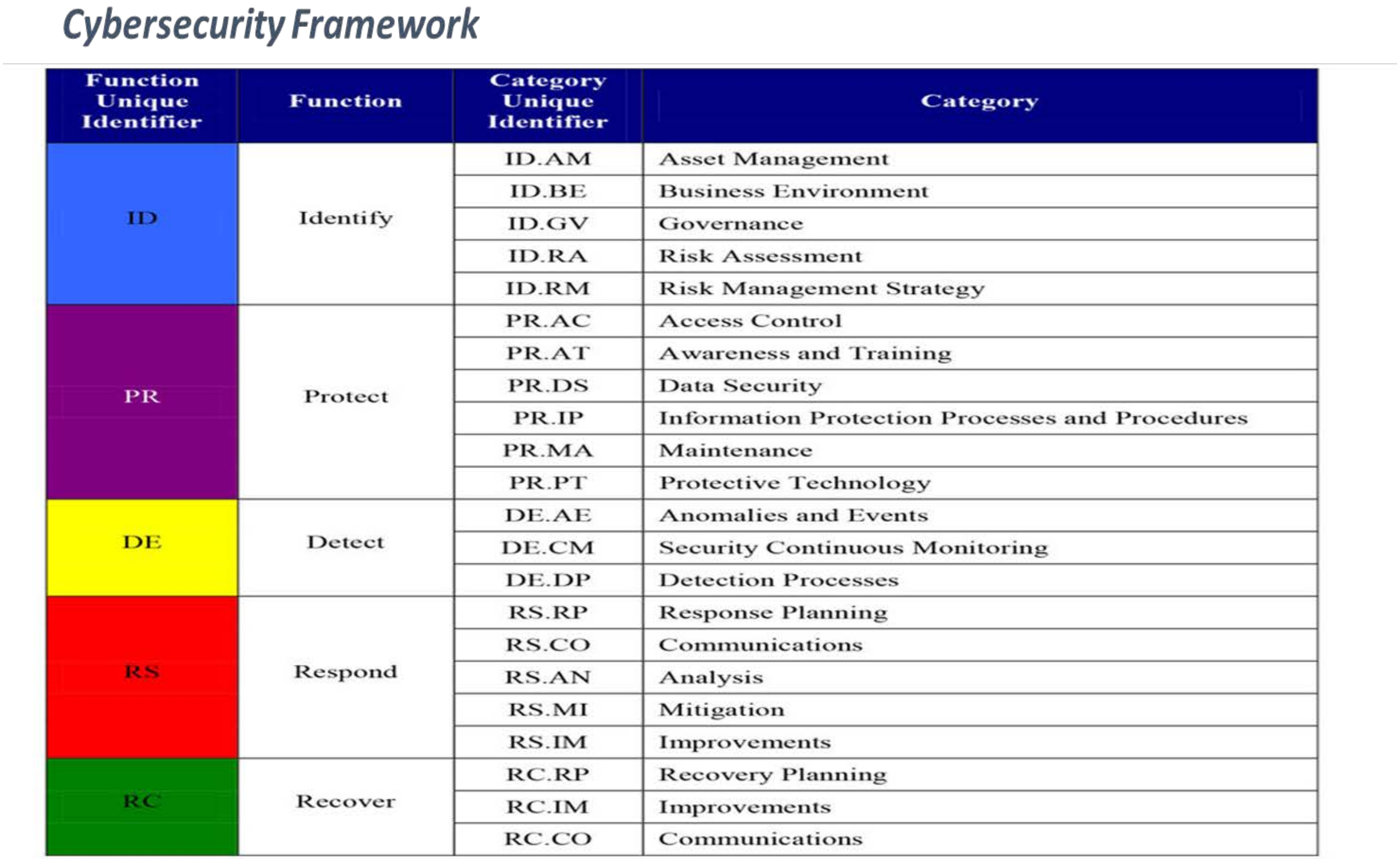


Business, IT, Threats, Vulnerabilities
Your Organization

MANAGING YOUR RISK(S)

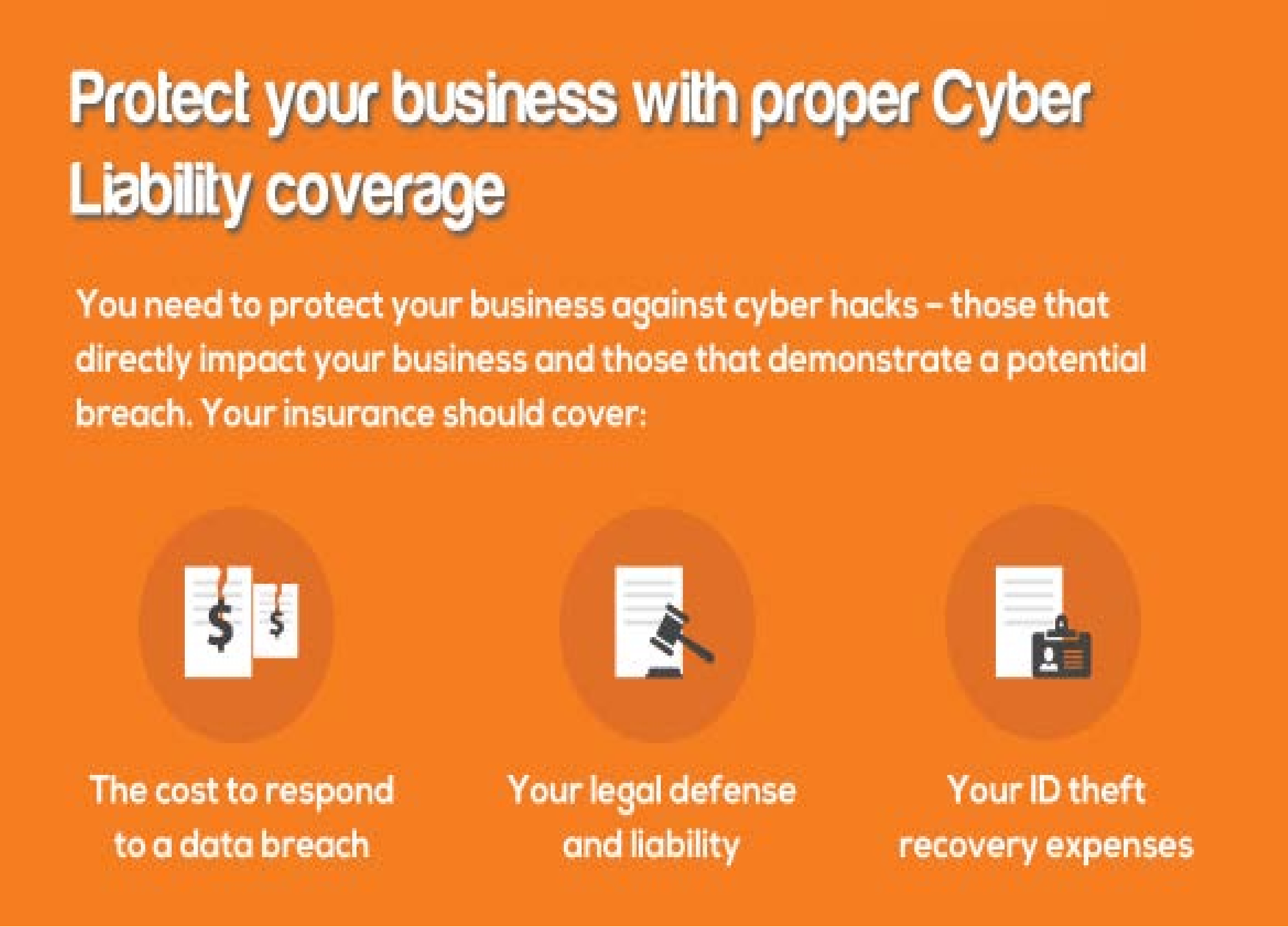
Determine the value of your information

NIST Cyber Security Framework (CSF)



Cybersecurity Framework

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



Protect your business with proper Cyber Liability coverage

You need to protect your business against cyber hacks – those that directly impact your business and those that demonstrate a potential breach. Your insurance should cover:

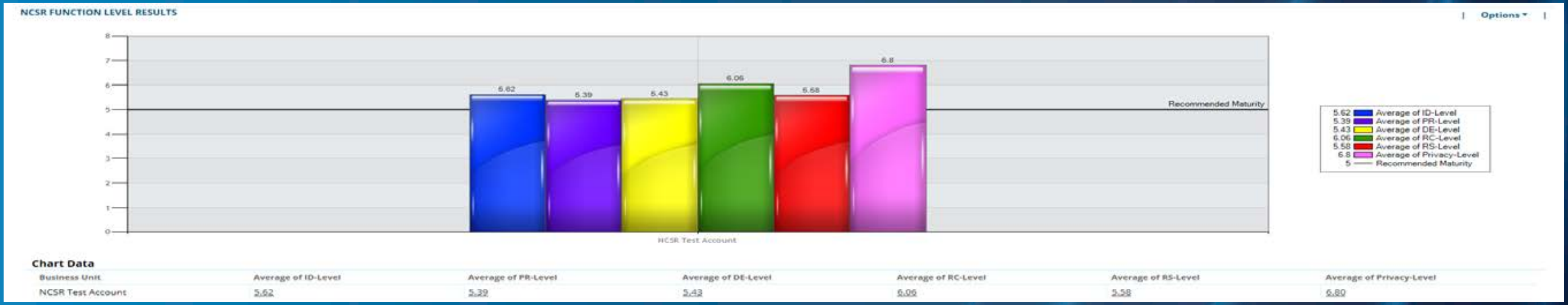
- The cost to respond to a data breach
- Your legal defense and liability
- Your ID theft recovery expenses

NATIONWIDE
CYBER SECURITY
REVIEW

MS-ISAC
Multi-State Information
Sharing & Analysis Center

NACO National Association of Counties
The Voice of America's Counties

NASCIO
Representing Chief Information
Officers of the States



NCSR FUNCTION LEVEL RESULTS

| Options ▾ |
8
7
6
5
4
3
2
1
0
5.62
5.39
5.43
6.06
5.68
6.8
Recommended Maturity
NCSR Test Account
5.62 🟦 Average of ID-Level
5.39 🟪 Average of PR-Level
5.43 🟨 Average of DE-Level
6.06 🟩 Average of RC-Level
5.58 🟥 Average of RS-Level
6.8 🟪 Average of Privacy-Level
5 — Recommended Maturity

Chart Data

Business Unit	Average of ID-Level	Average of PR-Level	Average of DE-Level	Average of RC-Level	Average of RS-Level	Average of Privacy-Level
NCSR Test Account	5.62	5.39	5.43	6.06	5.58	6.80

TLP: WHITE

MS-ISAC

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial, and tribal (SLTT) governments.

TLP: WHITE

Our Membership

Members include:

- All 50 states & Territories
- All 78 DHS-recognized Fusion Centers
- Over 1,100 Local and Tribal governments (representing over 48% of the U.S. population)

State, Local, Tribal, and Territorial

departments, cities, towns, police department, ports, airports, schools, transit associations, and more

24x7 Security Operations Center

Central location to report any cyber security incident

24/7 support for:

- ✓ Network Monitoring Services
- ✓ Research and Analysis

24/7 analysis and monitoring of:

- ✓ Threats
- ✓ Vulnerabilities
- ✓ Attacks

24/7 reporting:

- ✓ Cyber Alerts & Advisories
- ✓ Web Defacements
- ✓ Account Compromises
- ✓ Hacktivist Notifications

24 / 7 / 365 Monitoring & analysis of ~100 billion logs

<u>Phone</u>: 1-866-787-4722

<u>Email</u>: soc@msisac.org

SecureSuite Update

Department of Homeland Security

Cyber Capabilities/Entities

- National Cybersecurity and Communications Integration Center (NCCIC) (contact: NCCIC@hq.dhs.gov)

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (contact: ics-cert@hq.dhs.gov ; 877-776-7585)

- National Coordinating Center for Communications (NCC)
  (contact: NCC@hq.dhs.gov 703-235-5080)

- United States Computer Emergency Readiness Team (US-CERT) (contact: info@us-cert.gov 888-282-0870)

- National Infrastructure Coordinating Center
  (contact: NICC@hq.dhs.gov)

SC

CYBER

FOUNDING SPONSORS

1801

UNIVERSITY OF
SOUTH CAROLINA

South Carolina
Department of Commerce
Just right for business.

1225 Laurel Street, Suite 114 Columbia, SC 29201
www.sccyber.org