Cybersecurity and Infrastructure Security Agency (CISA)

October 29, 2019

Chris Gabbard, CISA
Cybersecurity Advisor Region 5: Minneapolis

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

A secure and resilient critical infrastructure for the American people.

MISSION

Lead the National effort to understand and manage cyber and physical risk to our critical infrastructure.

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

CISA is the Nation’s lead civilian cybersecurity agency and the national coordinator for critical infrastructure security and resilience efforts.

We work with partners to:
DEFEND TODAY and **SECURE TOMORROW**

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

FEDERAL NETWORK PROTECTION

PROACTIVE CYBER PROTECTION

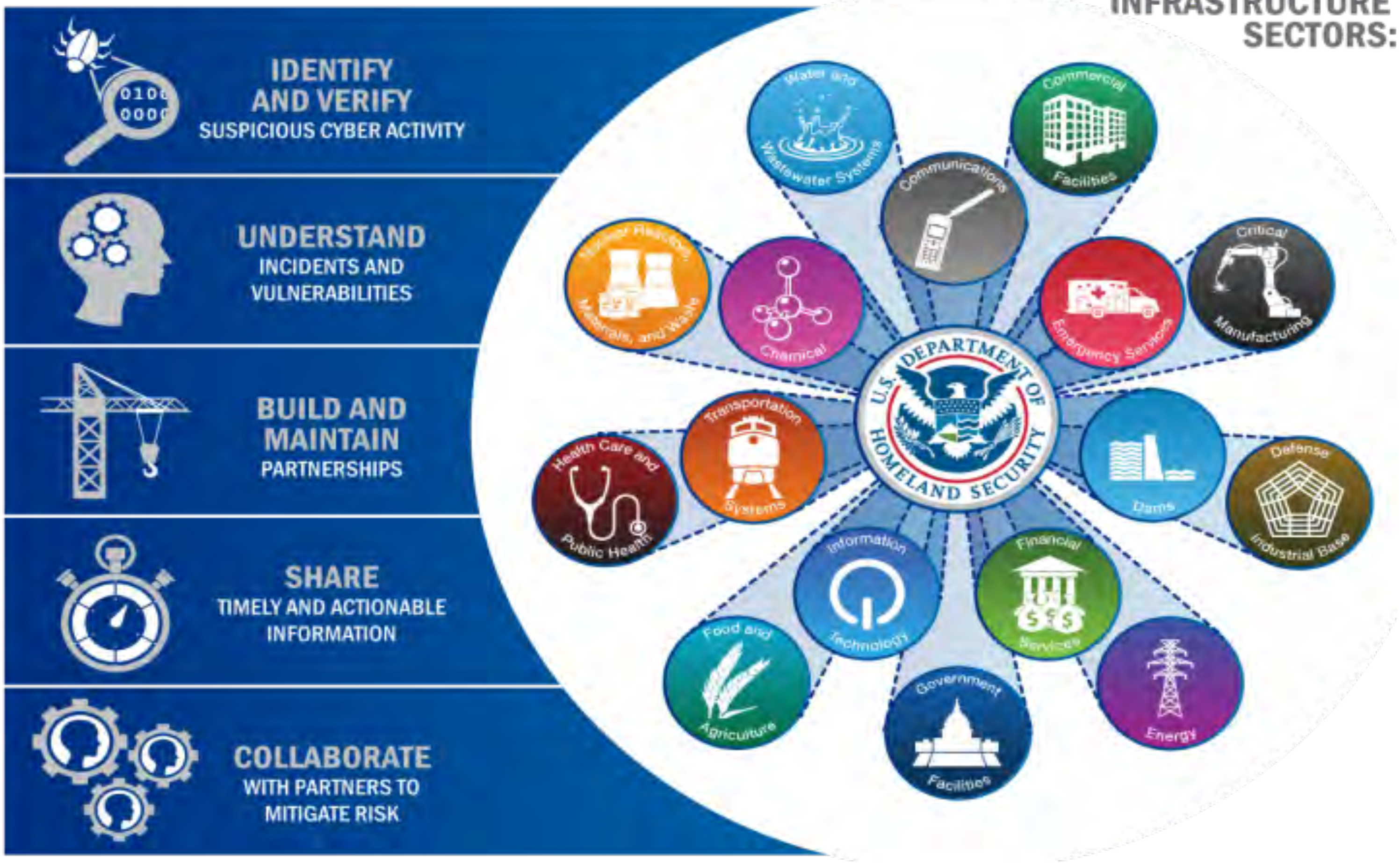
INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS

EMERGENCY COMMUNICATIONS

Serving Critical Infrastructure

KEY ACTIVITIES:

16 CRITICAL INFRASTRUCTURE SECTORS:



IDENTIFY AND VERIFY SUSPICIOUS CYBER ACTIVITY

UNDERSTAND INCIDENTS AND VULNERABILITIES

BUILD AND MAINTAIN PARTNERSHIPS

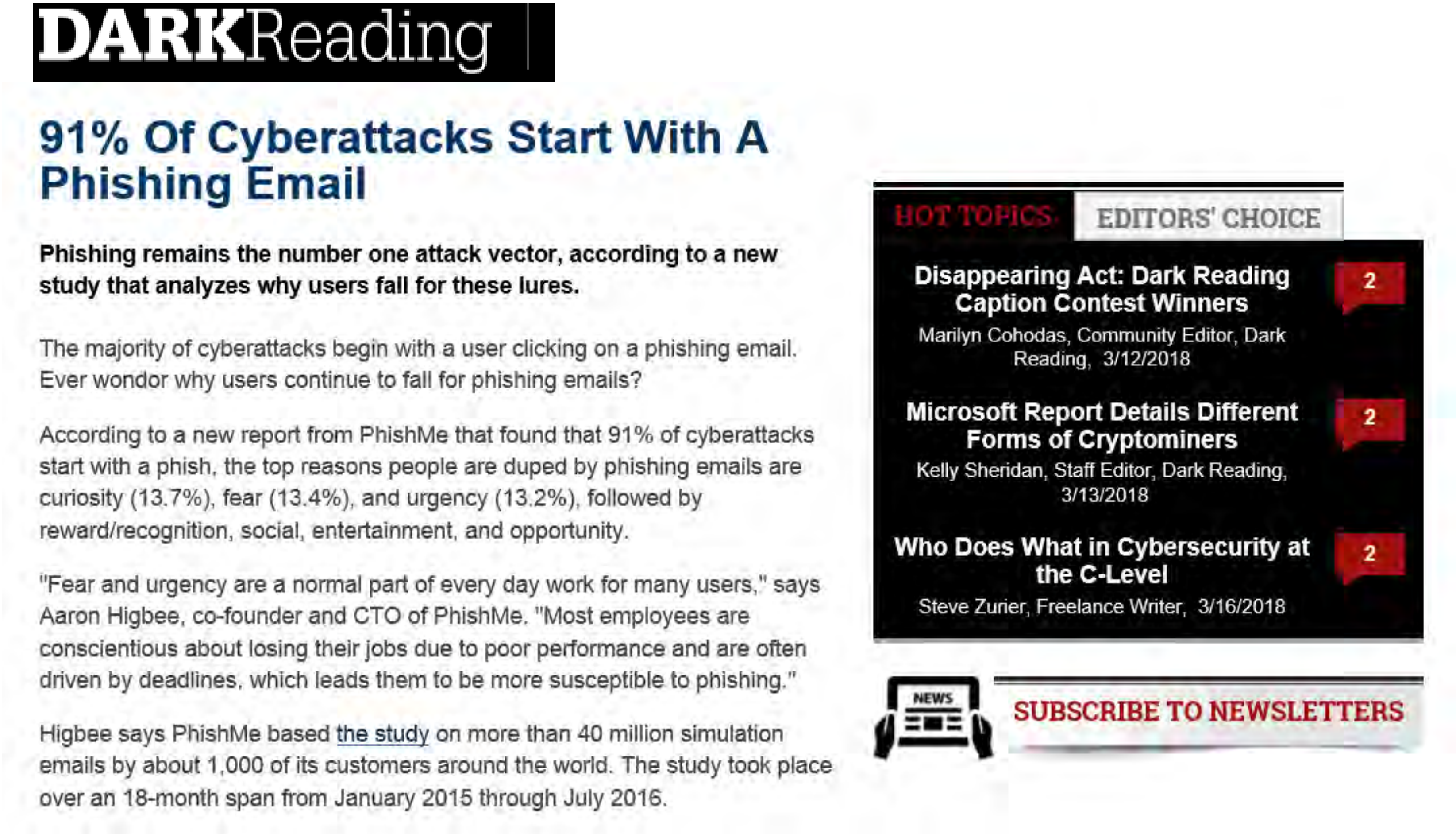
SHARE TIMELY AND ACTIONABLE INFORMATION

COLLABORATE WITH PARTNERS TO MITIGATE RISK

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

Threat Actors Are Sophisticated…

But They Don’t Always Need To Be



DARKReading

91% Of Cyberattacks Start With A Phishing Email

Phishing remains the number one attack vector, according to a new study that analyzes why users fall for these lures.

The majority of cyberattacks begin with a user clicking on a phishing email. Ever wondor why users continue to fall for phishing emails?

According to a new report from PhishMe that found that 91% of cyberattacks start with a phish, the top reasons people are duped by phishing emails are curiosity (13.7%), fear (13.4%), and urgency (13.2%), followed by reward/recognition, social, entertainment, and opportunity.

"Fear and urgency are a normal part of every day work for many users," says Aaron Higbee, co-founder and CTO of PhishMe. "Most employees are conscientious about losing their jobs due to poor performance and are often driven by deadlines, which leads them to be more susceptible to phishing."

Higbee says PhishMe based the study on more than 40 million simulation emails by about 1,000 of its customers around the world. The study took place over an 18-month span from January 2015 through July 2016.

HOT TOPICS | EDITORS' CHOICE

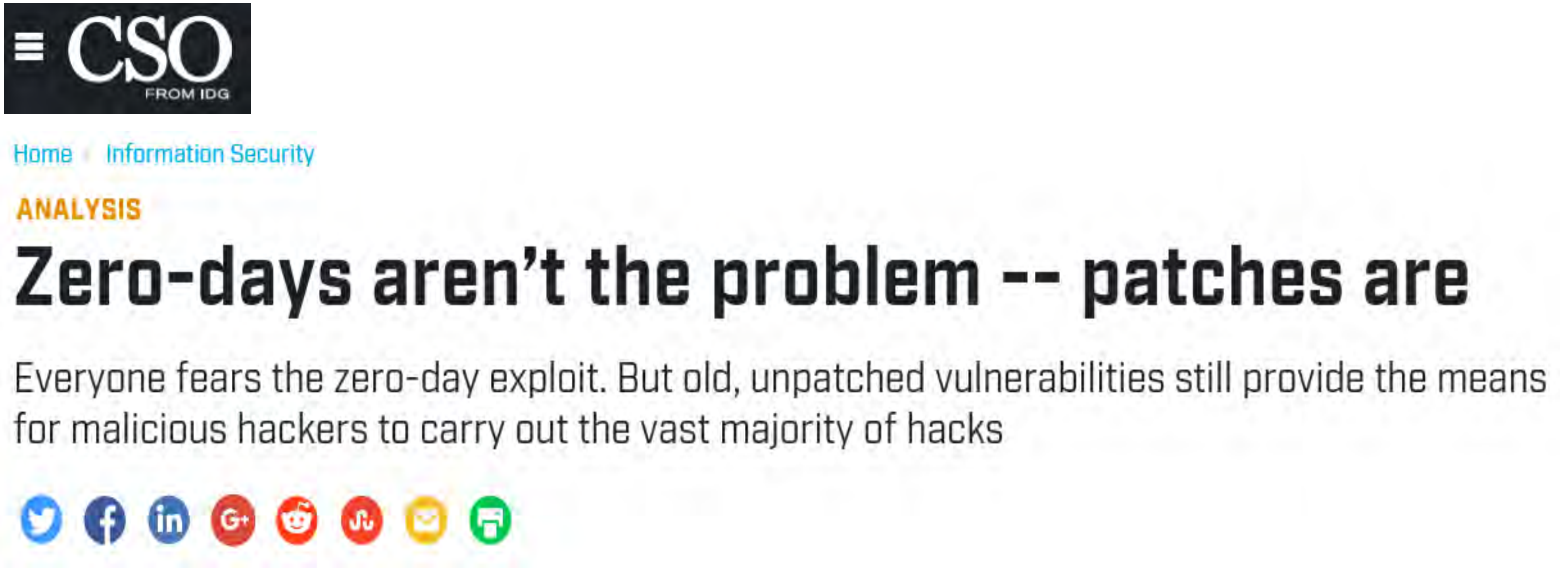
Disappearing Act: Dark Reading Caption Contest Winners 2
Marilyn Cohodas, Community Editor, Dark Reading, 3/12/2018

Microsoft Report Details Different Forms of Cryptominers 2
Kelly Sheridan, Staff Editor, Dark Reading, 3/13/2018

Who Does What in Cybersecurity at the C-Level 2
Steve Zurier, Freelance Writer, 3/16/2018

SUBSCRIBE TO NEWSLETTERS

But They Don’t Always Need To Be



CSO FROM IDG

Home / Information Security

ANALYSIS

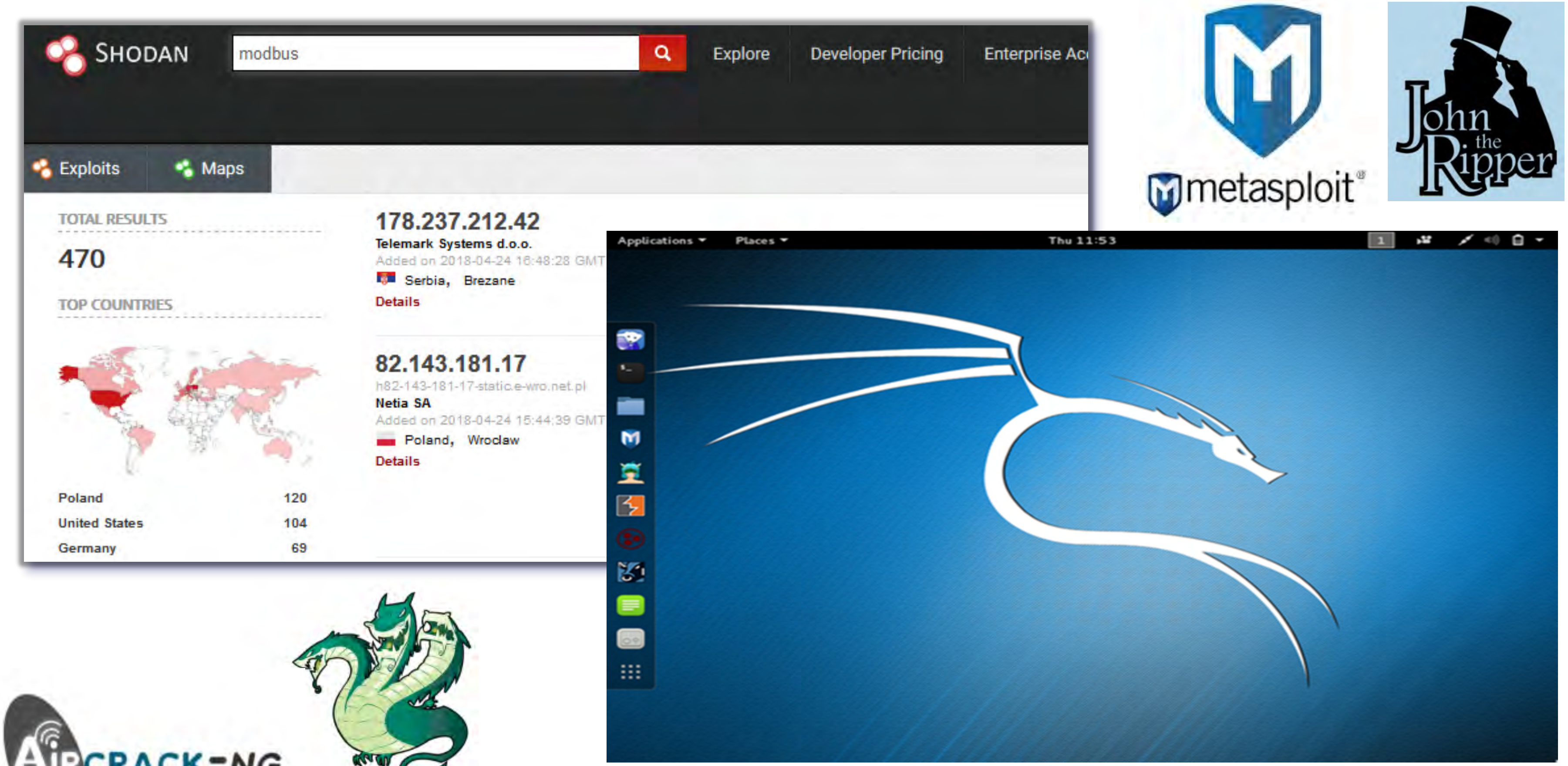
Zero-days aren’t the problem -- patches are

Everyone fears the zero-day exploit. But old, unpatched vulnerabilities still provide the means for malicious hackers to carry out the vast majority of hacks

. . . Most hackers follow the path created by a very few smart ones -- and zero days make up a very small percentage of attacks. It turns out that patching vulnerable software, if implemented consistently, would stop most hackers cold and significantly reduce risk.

Against an Expanding Attack Surface

With Tools Aimed Directly At You



TOTAL RESULTS

470

TOP COUNTRIES

Poland	120
United States	104
Germany	69

178.237.212.42
Telemark Systems d.o.o.
Added on 2018-04-24 16:48:28 GMT
Serbia, Brezane
Details

82.143.181.17
h82-143-181-17-static.e-wro.net.pl
Netia SA
Added on 2018-04-24 15:44:39 GMT
Poland, Wroclaw
Details

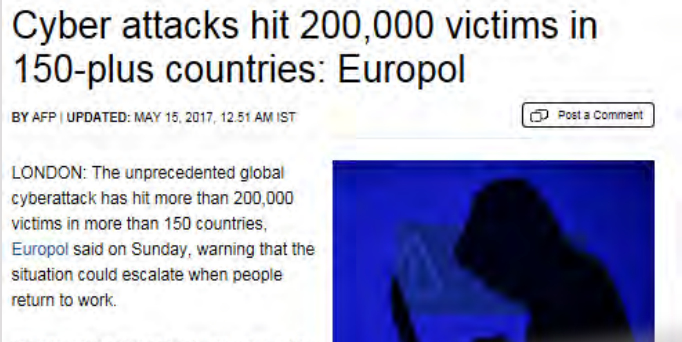
AIRCRACK-NG

netsparker
web application security scanner

w3af
Web Application Attack and Audit Framework

U.S. DEPARTMENT OF HOMELAND SECURITY
CISA
CYBER+INFRASTRUCTURE

Leading to Successful Attacks



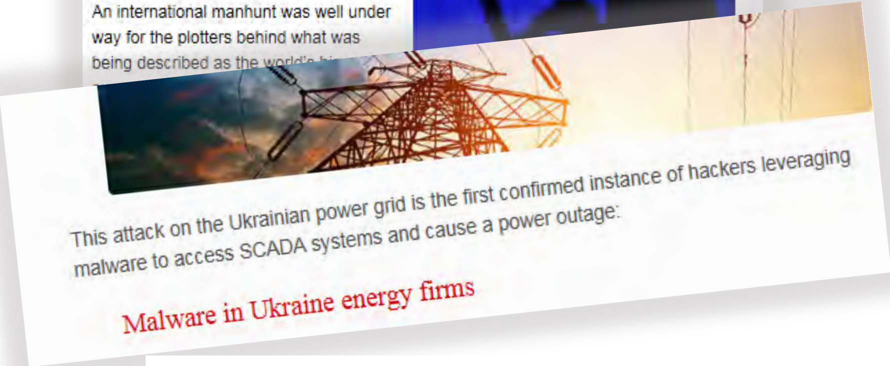
Cyber attacks hit 200,000 victims in 150-plus countries: Europol

BY AFP | UPDATED: MAY 15, 2017, 12.51 AM IST

Post a Comment

LONDON: The unprecedented global cyberattack has hit more than 200,000 victims in more than 150 countries, Europol said on Sunday, warning that the situation could escalate when people return to work.

An international manhunt was well under way for the plotters behind what was being described as the world's bi

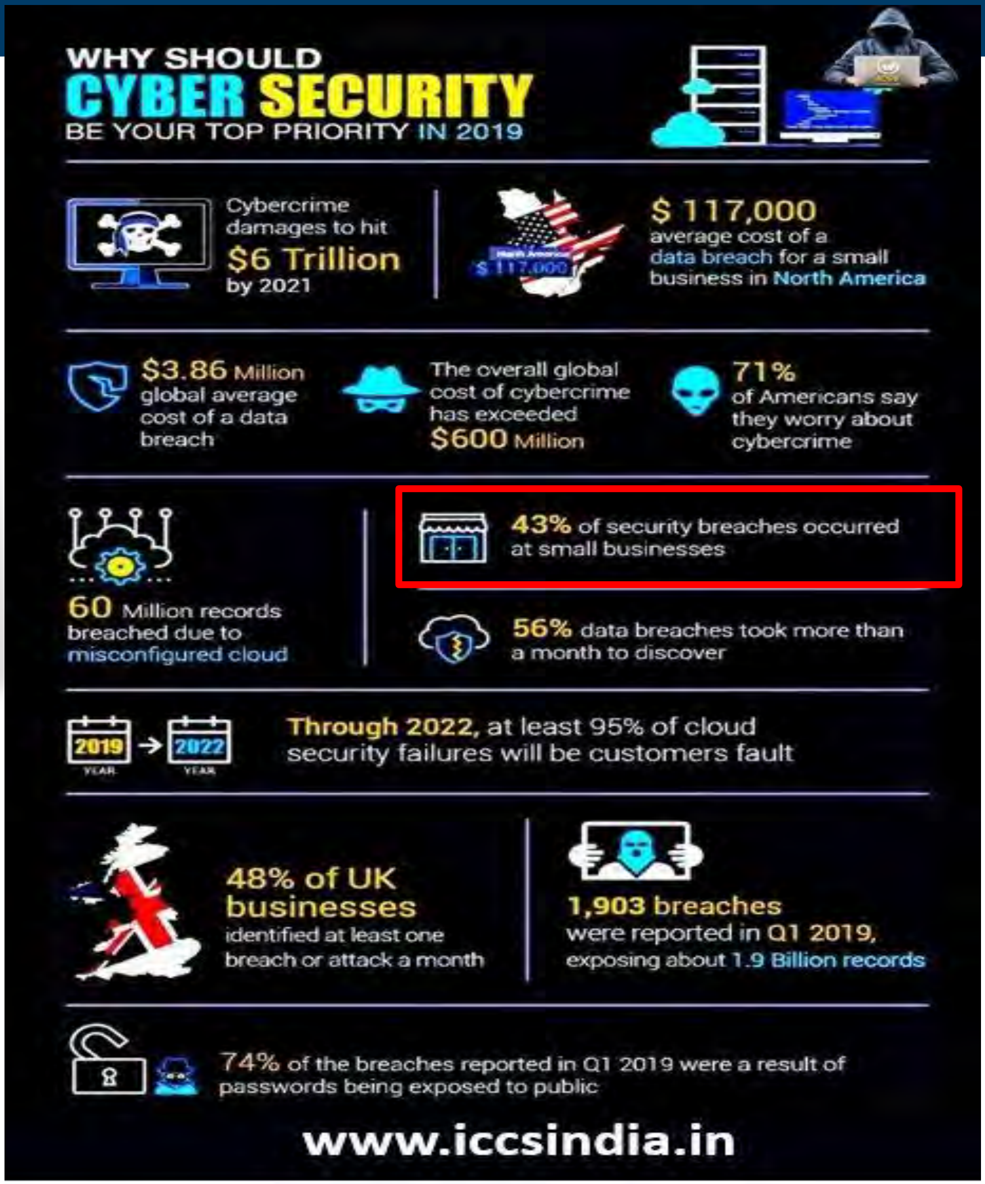


This attack on the Ukrainian power grid is the first confirmed instance of hackers leveraging malware to access SCADA systems and cause a power outage:

Malware in Ukraine energy firms

The New York Times

Hackers Are Holding Baltimore Hostage: How They Struck and What's Next



WHY SHOULD CYBER SECURITY BE YOUR TOP PRIORITY IN 2019

Cybercrime damages to hit $6 Trillion by 2021

$ 117,000 average cost of a data breach for a small business in North America

$3.86 Million global average cost of a data breach

The overall global cost of cybercrime has exceeded $600 Million

71% of Americans say they worry about cybercrime

60 Million records breached due to misconfigured cloud

43% of security breaches occurred at small businesses

56% data breaches took more than a month to discover

Through 2022, at least 95% of cloud security failures will be customers fault

48% of UK businesses identified at least one breach or attack a month

1,903 breaches were reported in Q1 2019, exposing about 1.9 Billion records

74% of the breaches reported in Q1 2019 were a result of passwords being exposed to public

www.iccsindia.in

CISA
CYBER+INFRASTRUCTURE

Cyber Risk Management Considerations

- The challenges continue to grow
- An efficient approach to managing risk helps you serve your customers and stakeholders
- Avoid “paralysis by analysis”
  - Manage your cybersecurity posture against established standards
  - Develop an improvement plan and take action
  - Manage improvements and work on “operational resilience” to address ongoing change and shifting threats.

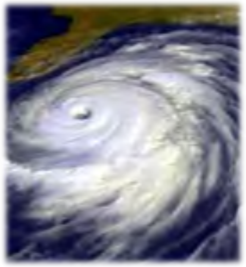
Bring “the Business” into Cybersecurity

Actions of People

```
A fatal exception
000059F8. The curr
* Press any key to
* Press CTRL+ALT+D
  lose any unsaved
```

Systems and Technology Failures

Failed Internal Processes



External Events

In highly complex, Internet-dependent, technically enabled organizations, cybersecurity is a **business** problem.

Cyber impacts/risks are not just disruptions of technology, but of the **business missions** that rely on the supporting technology.

Approaching cybersecurity as an **operational business risk brings** cybersecurity into the organization’s risk management process.

CISA
CYBER+INFRASTRUCTURE

Resilience Defined

"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"

- Presidential Policy Directive 21
February 12, 2013

Protect (Security)	**Sustain (Continuity)**
Perform (Capability)	**Repeat (Maturity)**

Resilience Emerges From What You Do

- Consider your health.
  - How do you become healthy?
  - Can you buy good health?
  - Can you “manufacture” good health?
- You can’t buy it in a product.
- *Good health* and *resilience* are both emergent properties.
- They develop – or emerge – from what we do.

Operational Resilience in Practice

Operational resilience emerges from what we do, such as:

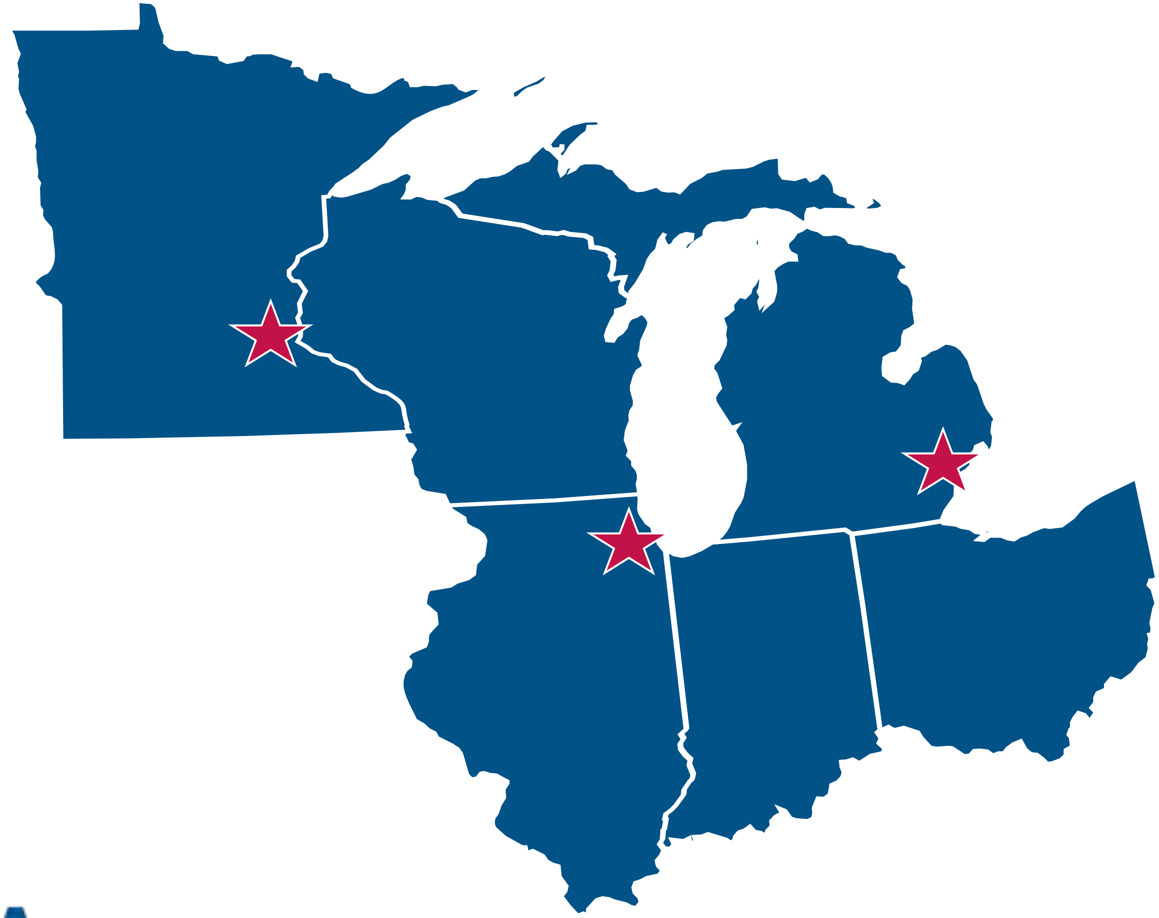
- Identifying critical services and mitigating risks,
- Planning for and managing vulnerabilities and incidents,
- Performing service-continuity processes and planning,
- Managing IT operations,
- Managing, training, & deploying people,
- Protecting and securing important assets, and
- Working with external partners.

CISA is with you

The Department of Homeland Security is honing its focus on how it helps state and local governments and small and medium businesses in the area of cyber security amid a number of recent ransomware attacks and continued threats to critical infrastructures

- Jeanette Manfra, assistant Director for Cybersecurity with the Cybersecurity and Infrastructure Security Agency

CSA Deployed Personnel- Region 5



★ **CSA Offices**

Cybersecurity Advisor Program

In support of the CISA mission, Cybersecurity Advisors:

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.

Sampling of Cybersecurity Offerings

- **Preparedness Activities**
  - Information / Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices
  - Cybersecurity Evaluations
    - Cyber Resilience Reviews (CRR™)
    - Cyber Infrastructure Surveys
    - Phishing Campaign Assessment
    - Vulnerability Scanning
    - Risk and Vulnerability Assessments (aka "Pen" Tests)
    - External Dependency Management Reviews
    - Cyber Security Evaluation Tool (CSET™)
    - Validated Architecture Design Review (VADR)

- **Response Assistance**
  - Remote / On-Site Assistance
  - Malware Analysis
  - Hunt and Incident Response Teams
  - Incident Coordination

- **Cybersecurity Advisors**
  - Assessments
  - Working group collaboration
  - Best Practices private-public
  - Incident assistance coordination

- **Protective Security Advisors**
  - Assessments
  - Incident liaisons between government and private sector
  - Support for National Special Security Events

Range of Cybersecurity Assessments

STRATEGIC
(C-Suite Level)

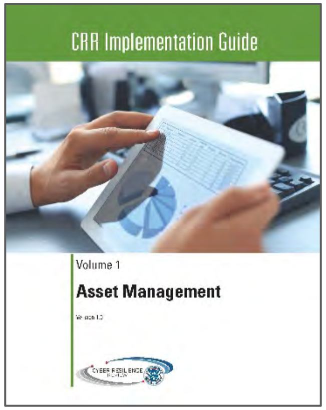
- Cyber Resilience Review (Strategic) ---------------------------
- External Dependencies Management (Strategic)-----------
- Cyber Infrastructure Survey (Strategic) ------------------------
- Cybersecurity Evaluations Tool (Strategic/Technical)-----
- Phishing Campaign Assessment (Technical)----------------
- Vulnerability Scanning / Hygiene (Technical)----------------
- Validated Architecture Design Review (Technical) ---------
- Risk and Vulnerability Assessment (Technical)-------------

TECHNICAL
(Network-Administrator Level)

Criticality of Periodic Assessments

- Periodic assessments are essential for resilience, helping you:
  - Measure your cybersecurity efforts
  - Manage improvements over time

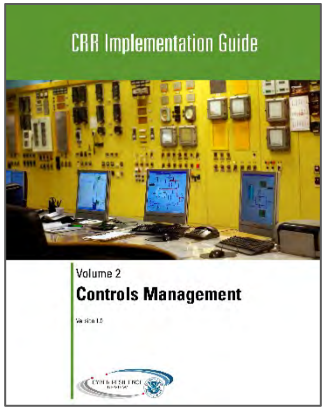
Available Resource Guides


CRR Implementation Guide

Volume 1

Asset Management

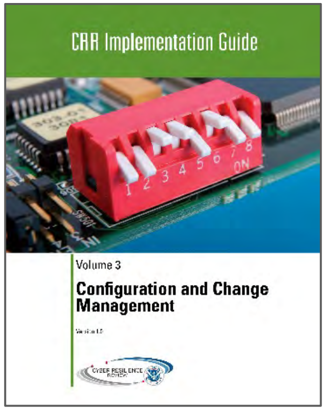
Version 1.0


CRR Implementation Guide

Volume 2

Controls Management

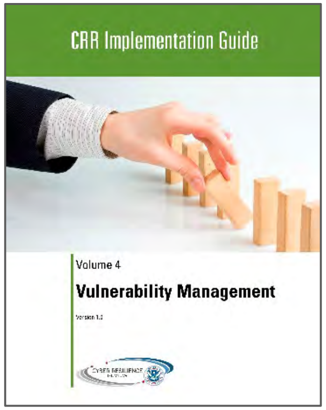
Version 1.0


CRR Implementation Guide

Volume 3

Configuration and Change Management

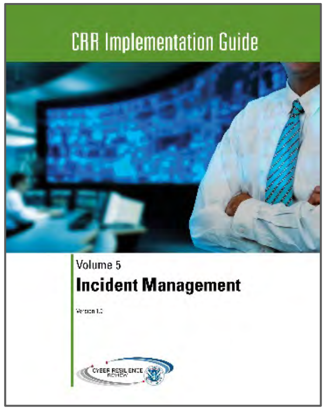
Version 1.0


CRR Implementation Guide

Volume 4

Vulnerability Management

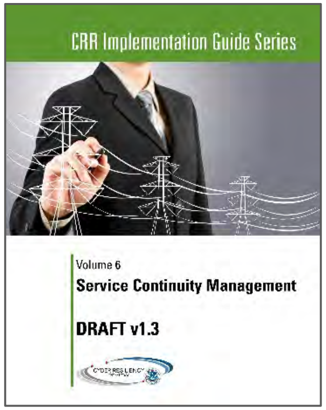
Version 1.0


CRR Implementation Guide

Volume 5

Incident Management

Version 1.0


CRR Implementation Guide Series

Volume 6

Service Continuity Management

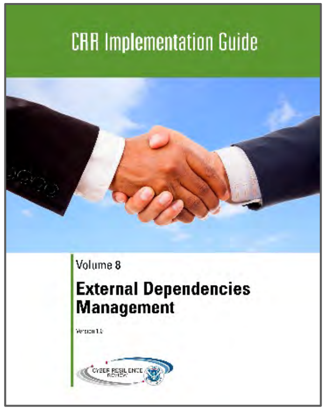
DRAFT v1.3

CRR Implementation Guide

Volume 7

Risk Management

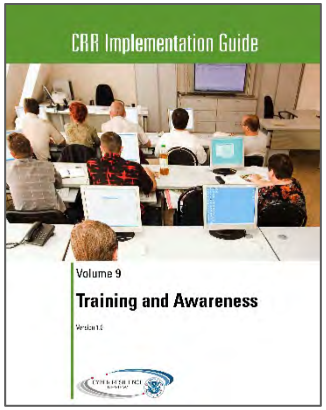
Version 1.0


CRR Implementation Guide

Volume 8

External Dependencies Management

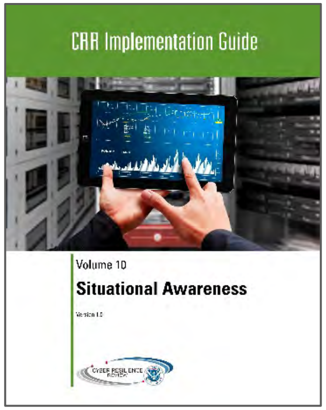
Version 1.0


CRR Implementation Guide

Volume 9

Training and Awareness

Version 1.0


CRR Implementation Guide

Volume 10

Situational Awareness

Version 1.0

C3VP Resources

- us-cert.gov/ccubedvp

CISA
CYBER+INFRASTRUCTURE

Questions?

CSA Contact Information	
Chris Gababrd Cyber Security Advisor	**Christopher.Gabbard@hq.dhs.gov** **612-716-3044**
CyberAdvisor	**Cyberadvisor@hq.dhs.gov**