

Critical Infrastructure Cybersecurity



Agenda

1. Terminology
2. ICS Incidents Statistics
3. Top Search Engines to Find ICSs
4. US Department of Homeland Security: Seven (7) Strategies to Protect ICSs
5. Defending against Cybersecurity Risks for Critical Infrastructure
6. US National Institute of Standards and Technology(NIST)
- Cybersecurity Framework

Terminology

The official US National Institute of Standards & Technology (NIST) definitions:

- **Critical Infrastructure:** Any technology / asset that is significant to the operations of a society or nation.
- **Industrial Control Systems (ICSs):** Operational technology that automates, controls, or monitors an engineering process.

ICS-CERT for 2015: Incidents by Sectors

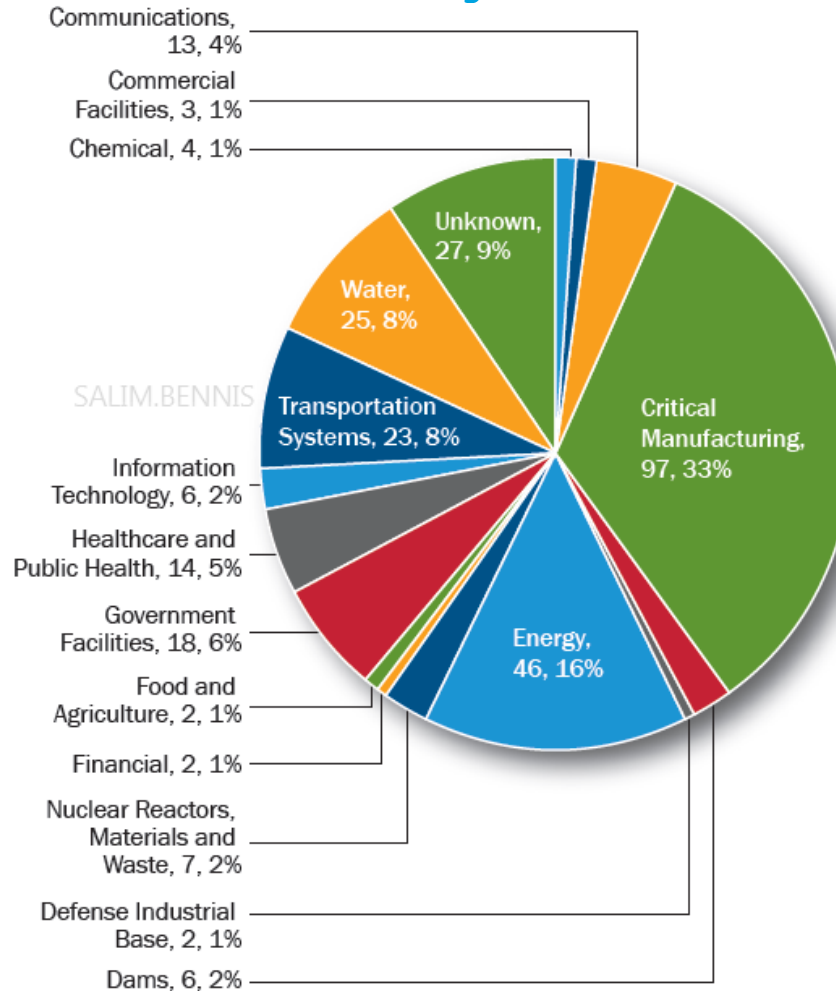


Figure 1. FY 2015 Incidents by Sector, 295 total.

Reference: US Department of Homeland Security - National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team

ICS-CERT for 2015: Incidents by Attempted Infection Vector

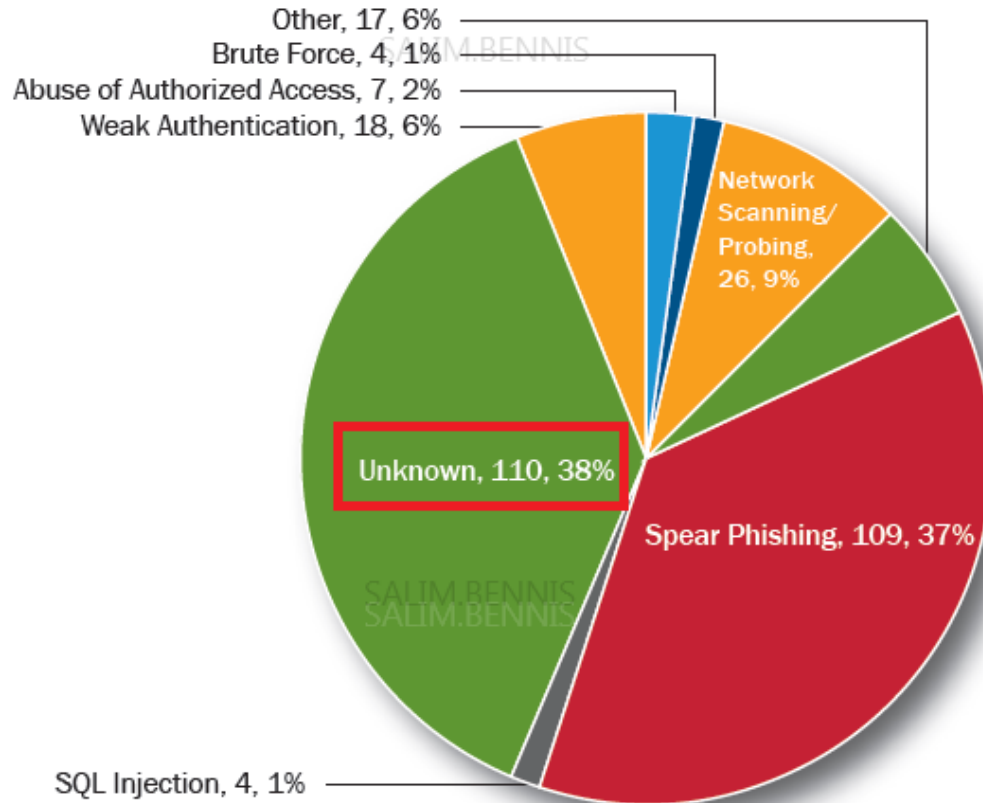


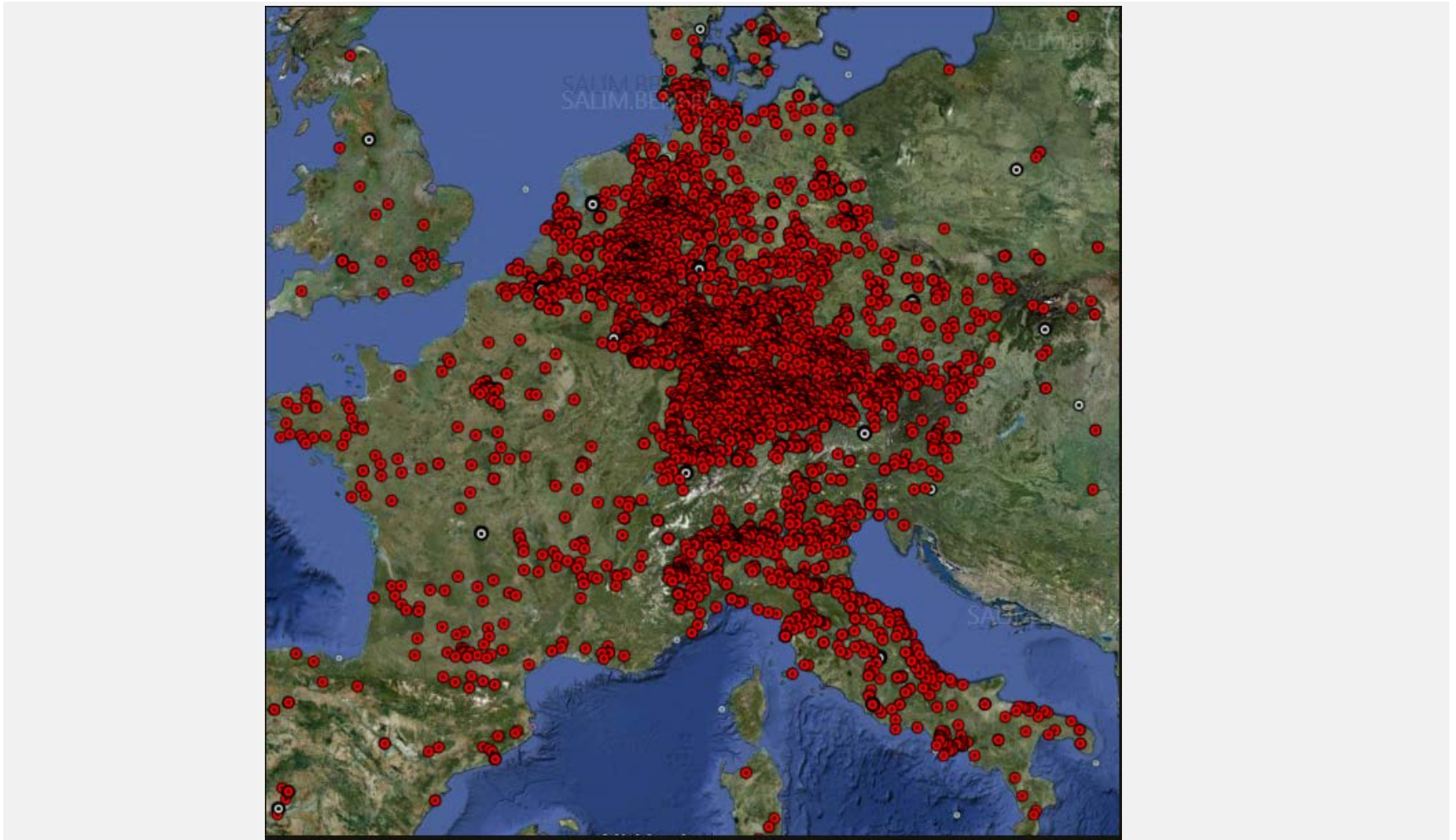
Figure 2. FY 2015 Incidents by Attempted Infection Vector, 295 total.

Reference: US Department of Homeland Security - National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team

Internet-facing ICSs

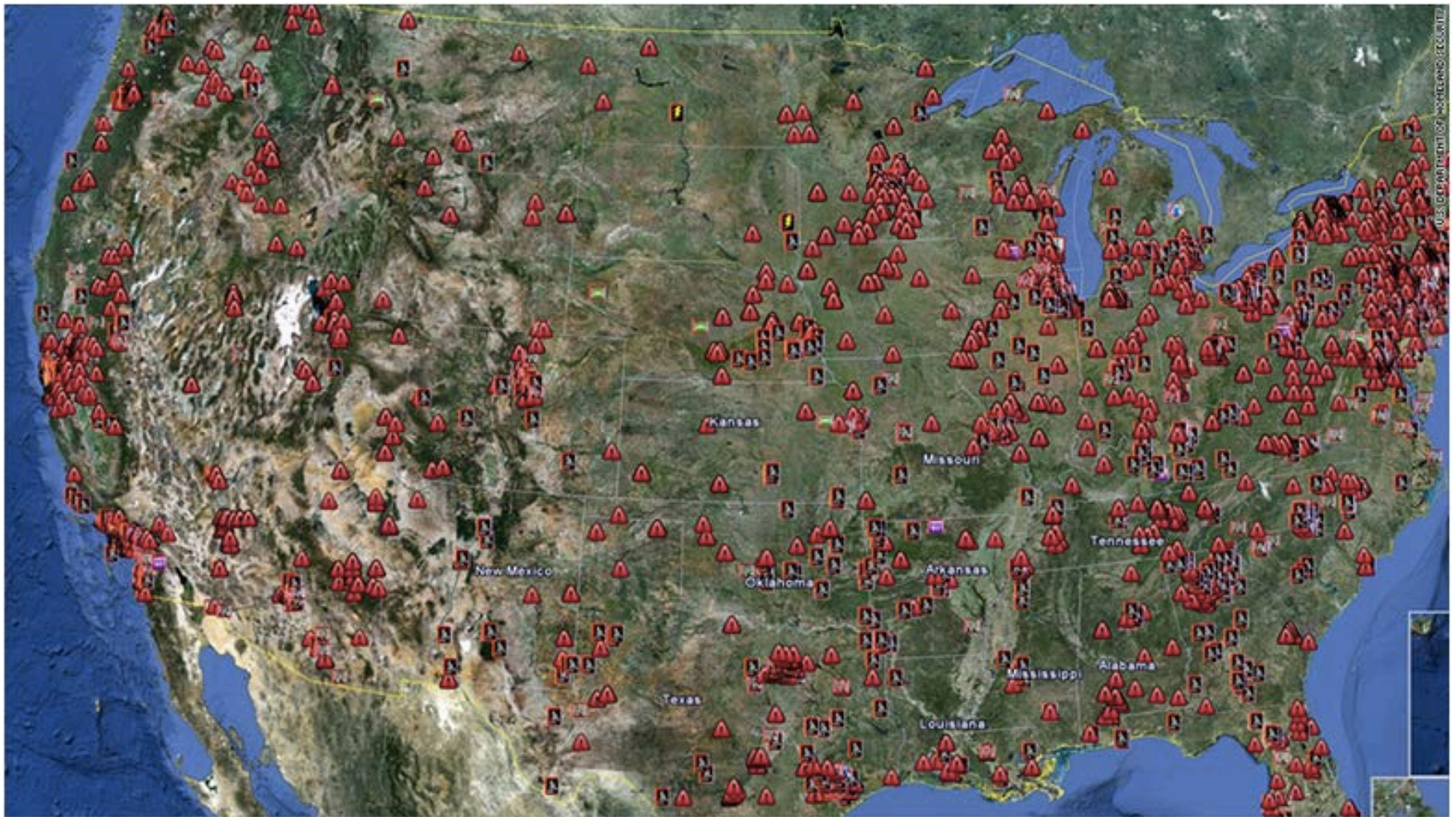
- As of 2014, ICS-CERT was aware of 82,000 cases of ICS hardware or software directly accessible from the public Internet.
- Examples include numerous water utilities, a US Crime Lab, a Dam, the Sochi Olympic stadium.

Internet-Connected ICSs (SCADA) in Europe Alone



Source: <https://cyberarms.wordpress.com/2013/03/19/worldwide-map-of-internet-connected-scada-systems/>

Internet-Connected ICSs Worldwide



Source: The Department of Homeland Security.

Top Search Engines Used

NNIS



JIS




SALIM.BENNIS



SHODAN admin+1234 country:PL

Exploits | **Maps** | Share Search | Download Results

TOP COUNTRIES



Poland 928

TOP CITIES

Czestochowa	323
Warsaw	57
Wroclaw	8
Swinoujscie	7
Torun	3

TOP SERVICES

Kerberos	419
HTTP (8080)	338
HTTP	140
HTTP (81)	7
AndroMouse	5

TOP ORGANIZATIONS

Spoldzielnia Mieszkaniowa Polnoc	411
Orange Polska	125
Netia SA	24
	22

Authentication Required

http://212.96.230.130:88 is requesting your username and password. The site says: "Default: admin/1234"

User Name:

Password:

Cancel OK

Total results: 928

Document Error

213.195.134.91
user.134.91.lan.ekonet.
Netia SA
Added on 2017-02-11 01:31:28 GMT
Poland, Walbrzyz

Details

Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html

Document Error: Unauthorized

83.12.233.99
giz99.intomeldsl.tpnet.pl
Orange Polska
Added on 2017-02-11 01:31:28 GMT
Poland

Details

HTTP/1.1 401 Unauthorized
Server: GoAhead-Webs
Date: Fri Feb 13 11:33:14 1970
WWW-Authenticate: Basic realm="Default: admin/1234"
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html

212.96.230.130

host-212.96.230.130.tvkamp.pl
Spoldzielnia Mieszkaniowa Polnoc
Added on 2017-02-11 01:30:18 GMT
Poland, Czestochowa

Details

HTTP/1.1 401 Unauthorized
Server: GoAhead-Webs
Date: Mon Jan 24 09:26:58 2011
WWW-Authenticate: Basic realm="Default: admin/1234"
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html

Waiting for 212.96.230.130...

US Department of Homeland Security - Seven (7) Strategies to Protect ICSs

Of the 295 ICS incidents reported in the US in 2015, 98% could have been thwarted or detected using one the following strategies:

Seven Strategies to Defend ICSs

Implement Secure Remote Access – 1%

Monitor and Respond – 2%

Manage Authentication – 4%



Implement Application Whitelisting – 38%

Ensure Proper Configuration/Patch Management – 29%

Reduce your Attack Surface Area – 17%

Build a Defendable Environment – 9%

Where do we go from here?

Defending against Cybersecurity Risks (more than just ICSs)

- To better address Cybersecurity risks, the President of the United States issued Executive Order 13636, “[Improving Critical Infrastructure Cybersecurity](#)” on February 12, 2013, which established that “it is the Policy of the United States to enhance the security and resilience of the Nation’s [critical infrastructure](#) and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.”
- In enacting this policy, the Executive Order calls for the development of a voluntary [risk-based Cybersecurity Framework](#) - a set of industry standards and best practices to [help organizations manage cybersecurity risks](#).
- The resulting [Framework](#), created through collaboration between government and the private sector, uses a common language to address and [manage cybersecurity risk](#) in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

What Comprises Critical Infrastructure

Critical infrastructure spans the following sixteen (16) sectors:

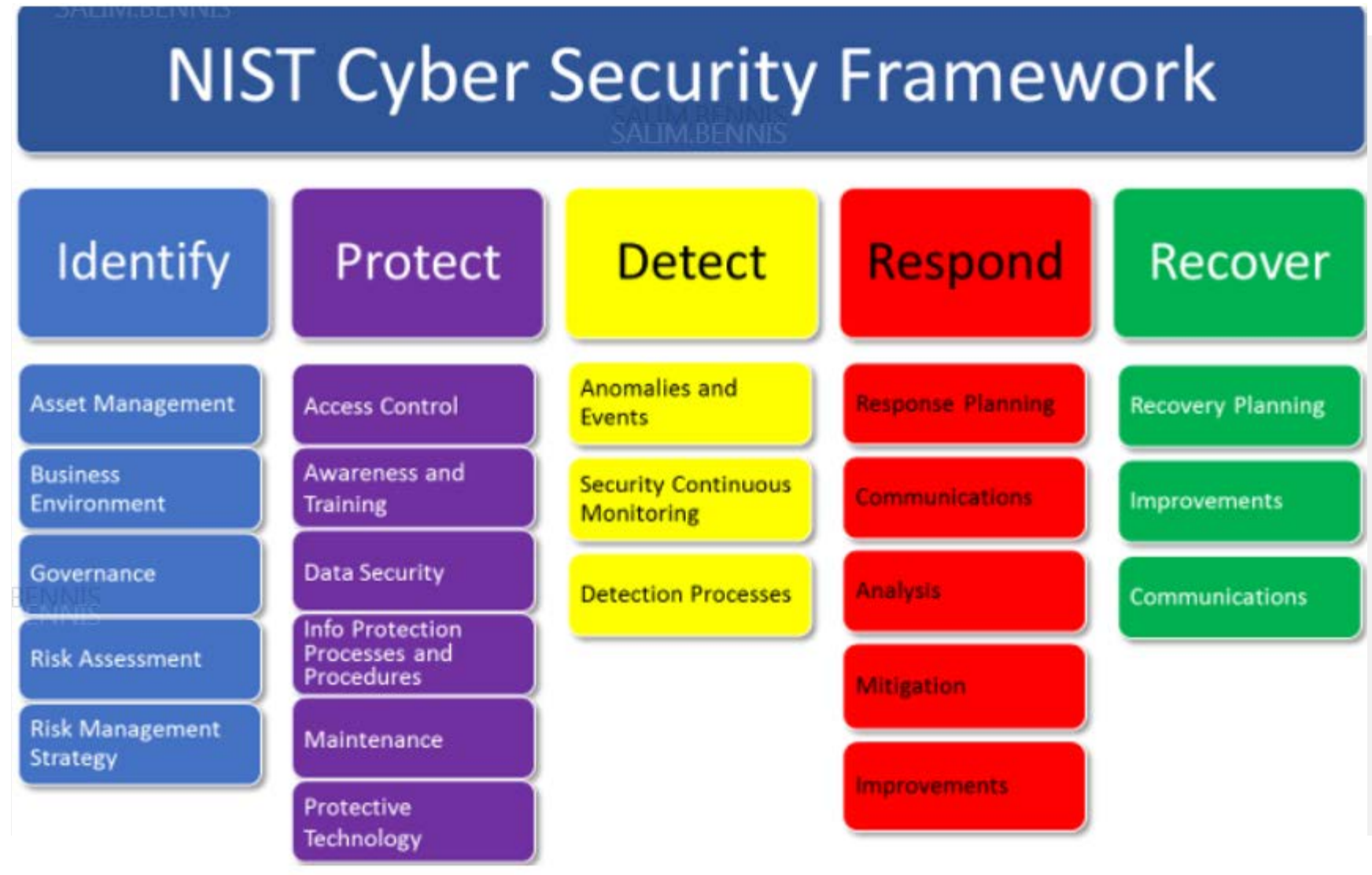
- | | |
|-----------------------------|--|
| 1. Chemicals | 9. Financial services |
| 2. Commercial facilities | 10. Food industry |
| 3. Communications | 11. Government facilities |
| 4. Critical manufacturing | 12. Healthcare & public health |
| 5. Dams | 13. Information technology |
| 6. Defense industrial bases | 14. Nuclear reactors, materials, & waste |
| 7. Emergency services | 15. Transportation systems |
| 8. Energy | 16. Water & wastewater systems |

Components of the Cybersecurity Framework

The Framework Core defines standardized cybersecurity activities, desired outcomes, and applicable references, and is organized by five continuous functions:

- **Identify** - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect** - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect** - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** - Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover** - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Categories of the Cybersecurity Framework



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
PR.AC-1 Manage Identities and Credentials for Authorized Devices	PR.AT-1 Inform and Train all Users	PR.DS-1 Protect Data-at-Rest	PR.IP-1 Create and Maintain Baseline Configuration of Information Technology/Industrial Control Systems	PR.MA-1 Timely Perform and Log Maintenance and Repair of Organizational Assets with Approved and Controlled Tools	PR.PT-1 In Accordance with Policy, Determine, Document, Implement, and Review Audit/Log Records
PR.AC-2 Manage and Protect Physical Access to Assets	PR.AT-2 Privileged Users Understand Roles and Responsibilities	PR.DS-2 Protect Data-in-Transit	PR.IP-2 Implement System Development Life Cycle to Manage Systems	PR.MA-2 Approve, Log, and Perform Remote Maintenance of Organizational Assets in Manner to Prevent Unauthorized Access	PR.PT-2 Protect and Restrict Use of Removable Media According to Policy
PR.AC-3 Manage Remote Access	PR.AT-3 Third-Party Stakeholders Understand Roles and Responsibilities	PR.DS-3 Formally Manage Assets throughout Removal, Transfers, and Disposition	PR.IP-3 Implement Configuration Change Control Processes		PR.PT-3 Incorporate Principle of Least Functionality to Control Access to Systems and Assets
PR.AC-4 Manage Access Permissions Incorporating Principles of Least Privilege and Separation of Duties	PR.AT-4 Senior Executives Understand Roles and Responsibilities	PR.DS-4 Maintain Adequate Capacity to Ensure Availability	PR.IP-4 Periodically Conduct, Maintain and Test Information Backups		
PR.AC-5 Protect Network Integrity Incorporating Network Segregation where Appropriate	PR.AT-5 Physical and Information Security Personnel Understand Roles and Responsibilities	PR.DS-5 Implement Protections against Data Leaks	PR.IP-5 Meet Policy and Regulations Regarding Physical Operating Environment for Organizational Assets		
		PR.DS-6 Use Integrity Checking Mechanisms to Verify Software, Firmware, and Information Integrity	PR.IP-6 Destroy Data According to Policy		PR.PT-4 Protect Communications and Control Networks

Thank You