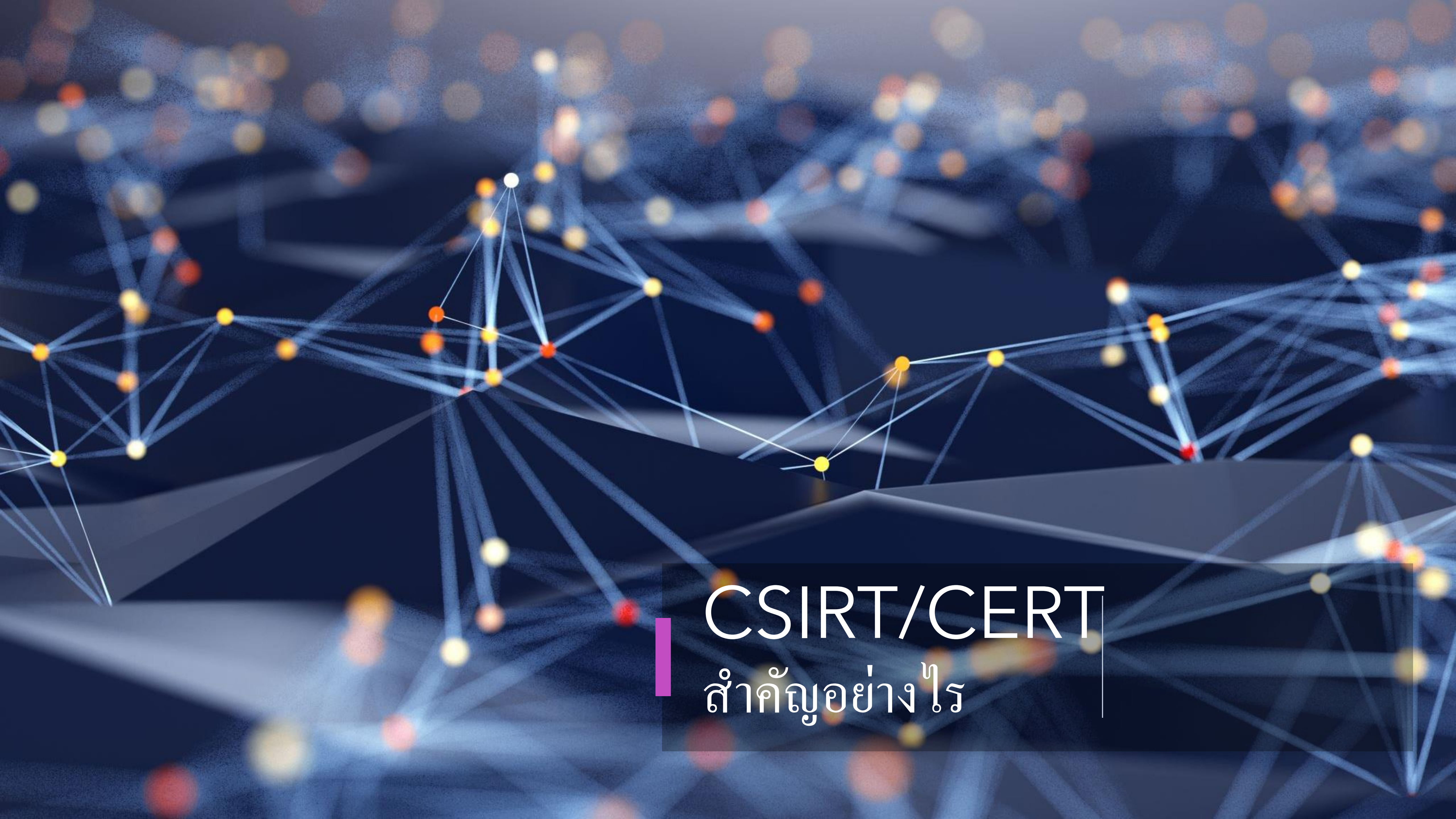


CSIRT/CERT

สำคัญอย่างไร

About me

- Name : Kitisak Jirawannakool
- Facebook : https://www.facebook.com/jkitisak
- Email : jkitisak@gmail.com
- Weblog : https://foh9.blogspot.com
  https://foh9blog.wordpress.com
- Twitter : @kitisak

#whoami

- Current: Freelance !!!
  - (Next move: KBTG)
- Former : ThaiCERT, G-CERT, and TB-CERT
- OWASP Thailand Chapter co-Leader
- CSA Thailand committee
- Certification and Award
  - COMTIA Security+
  - Asia Pacific Information Security Leader Achievements 2011 (ISLA) by (ISC)2

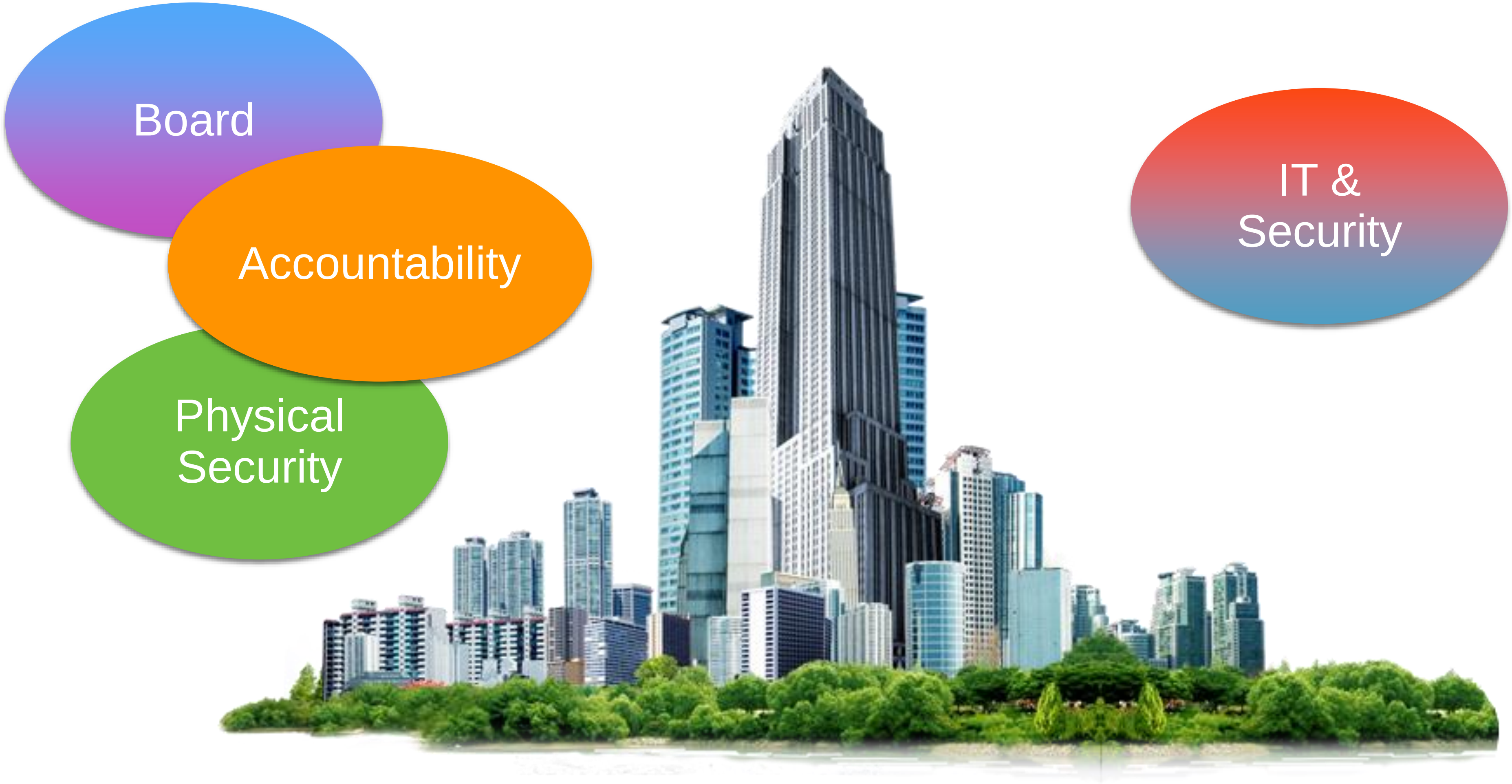
Agenda

- Cyber Threats
- What is CERT/CSIRT/SOC?
- How different?

Cyber Threats Nowadays

- Malware Related
- Data Breaches
- Distributed Denial of Service Attacks
- Web Defacement
- Spam
- Phishing
- Scanning / Attempts
- Content Related

How did it used to be?



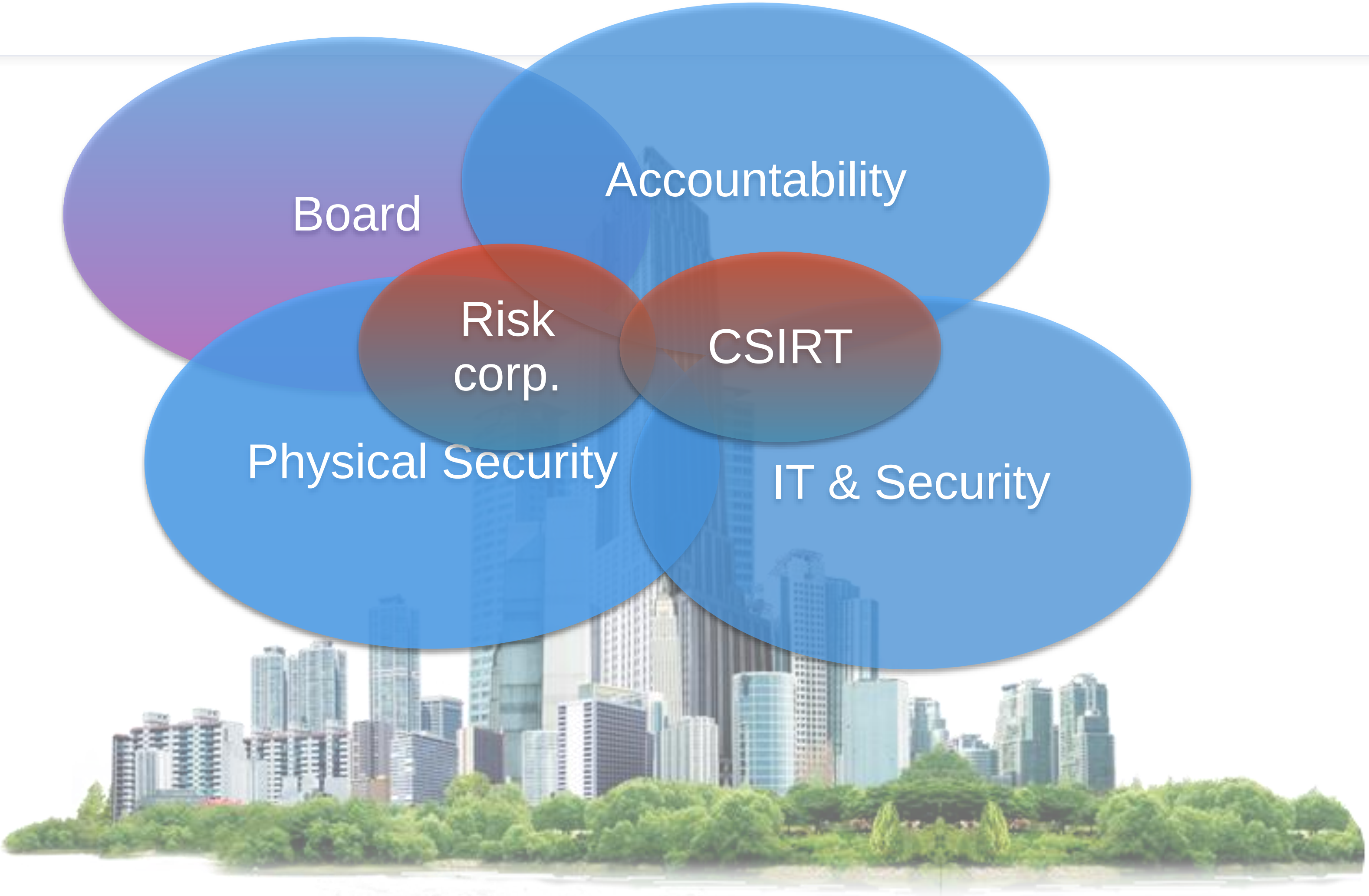
Board

Accountability

Physical Security

IT & Security

… and How it is growing to be?



What are we protecting?

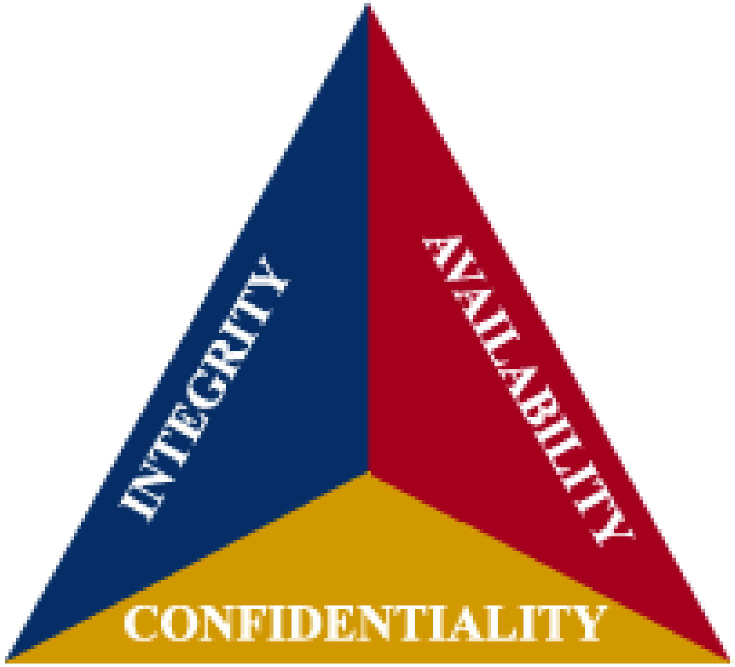
- Primary process
- Customers, Employees, Identities
- Products, Contracts
- Supporting processes
- Reputation
- Information, infrastructure
- Critical infrastructures
- Health, lives

So you need security, right !

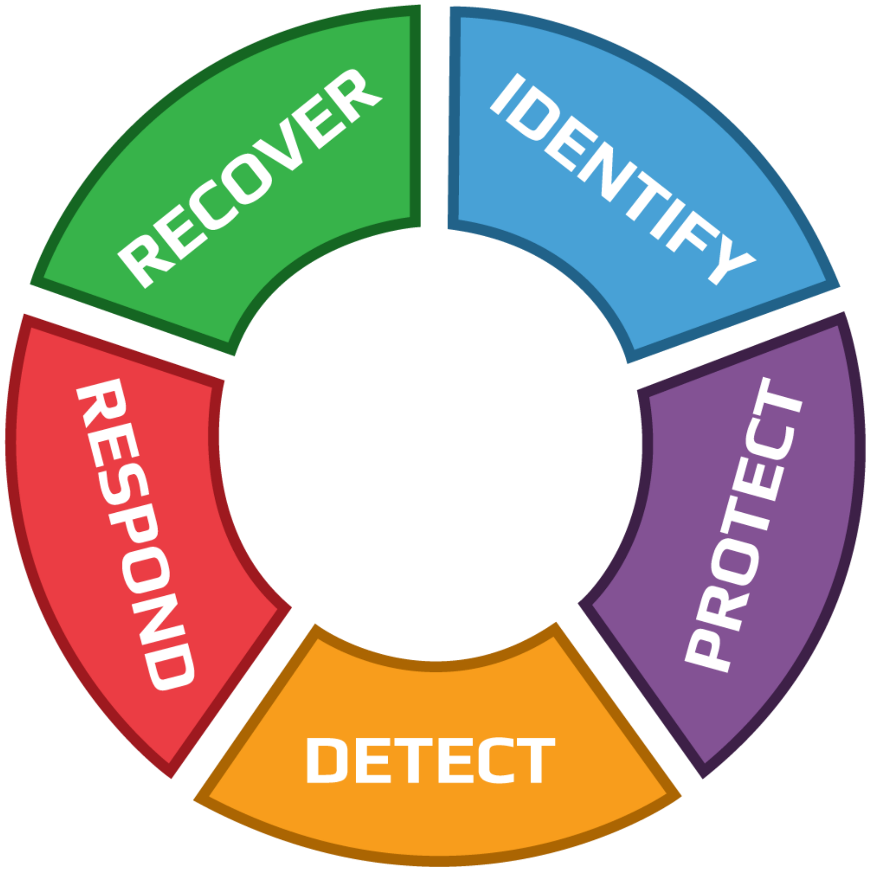
- “Total Security”
    - E.g. TSM (Total Security Management)
  - Risk Management
  - Crisis Management
  - Physical security
  - Information security
    - CISO (Chief Information Security Officer)
    - CSIRT
    - IT department
- Responsible = **board / CEO**

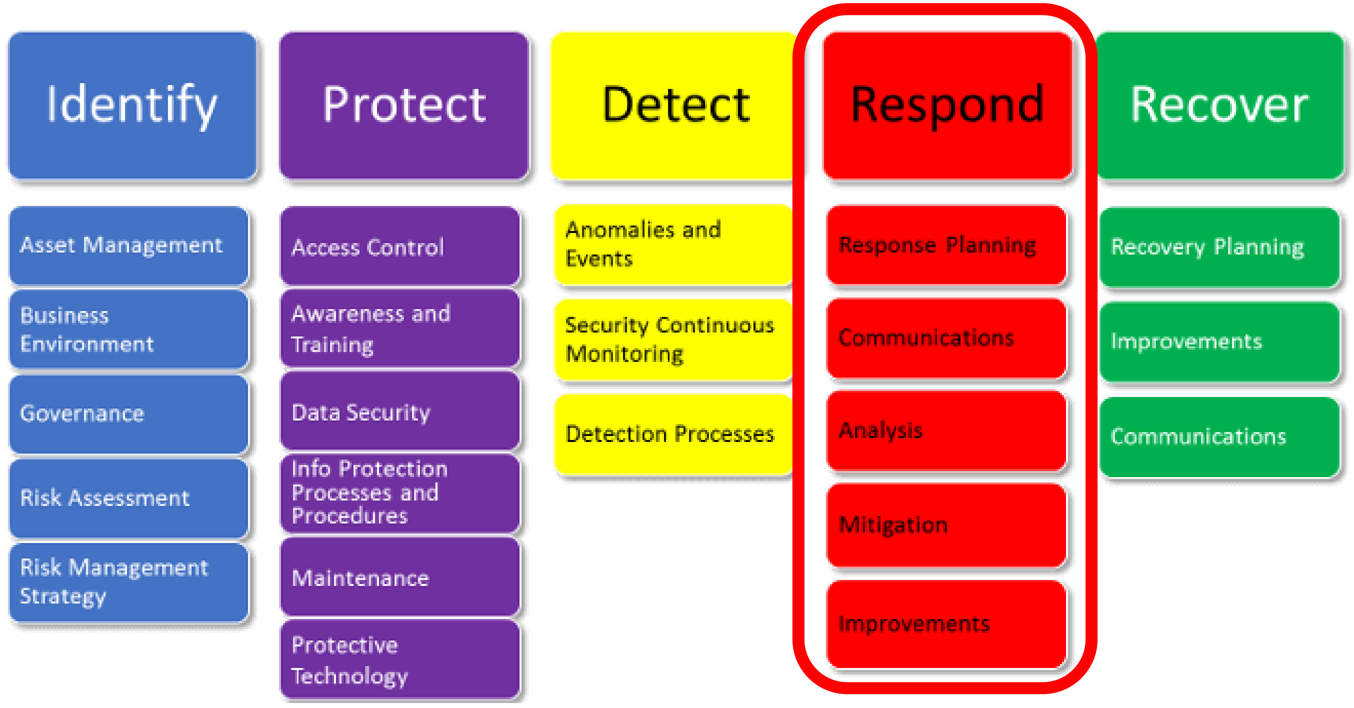
Cyber Security Framework

- How do we think about security?
- Ensuring the CIA
  - Confidentiality, Integrity, Availability
- Collection of activities to address Risk
  - Risk = Threats x Vulnerabilities
  - Dealing with the Known & and Unknown
- People, Process, Technology
- Dynamic & Continuous Approach
  - Including Learning from Incidents
  - Applying Best Current Practices



NIST Cyber Security Framework





Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

But.........

FIRE ALARM
More Security Doesn’t Make You More Secure
Better Management Does.

Traditional Incident Response

- Adhoc & Unplanned
- Deal with it as it happens
- Prolonged Recovery Times
- Damage to Company
- Lack of Metrics
- Legal Issues
- Bad Guys/Gals Getting Away

Terminology

- CERT : Computer Emergency Response Team
  - Origin 1988, later trademarked
  - CERT Coordination Center (CERT/CC)
  - Permission to use : http://www.sei.cmu.edu/legal/permission/index.cfm
- CSIRT : Computer Security Incident Response Team
  - Origin 1998 : http://www.cert.org/archive/pdf/csirt-handbook.pdf
  - Free to use !
- CERT/CSIRT name common and popular but misleading

- What's in a name – **you must have this capability !**

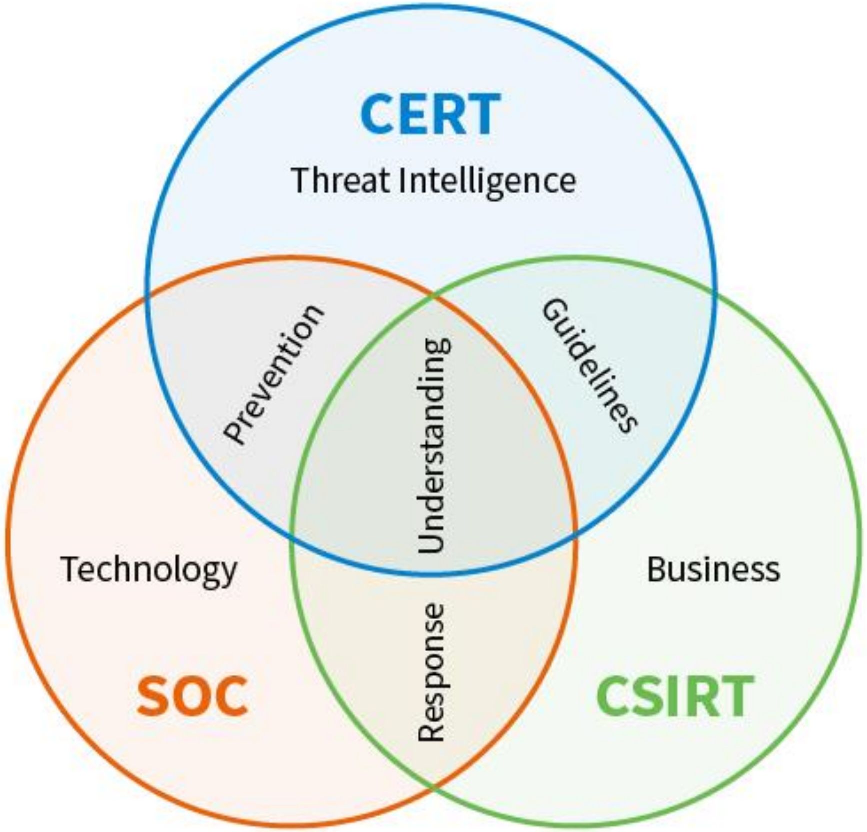
Warning!!!!!

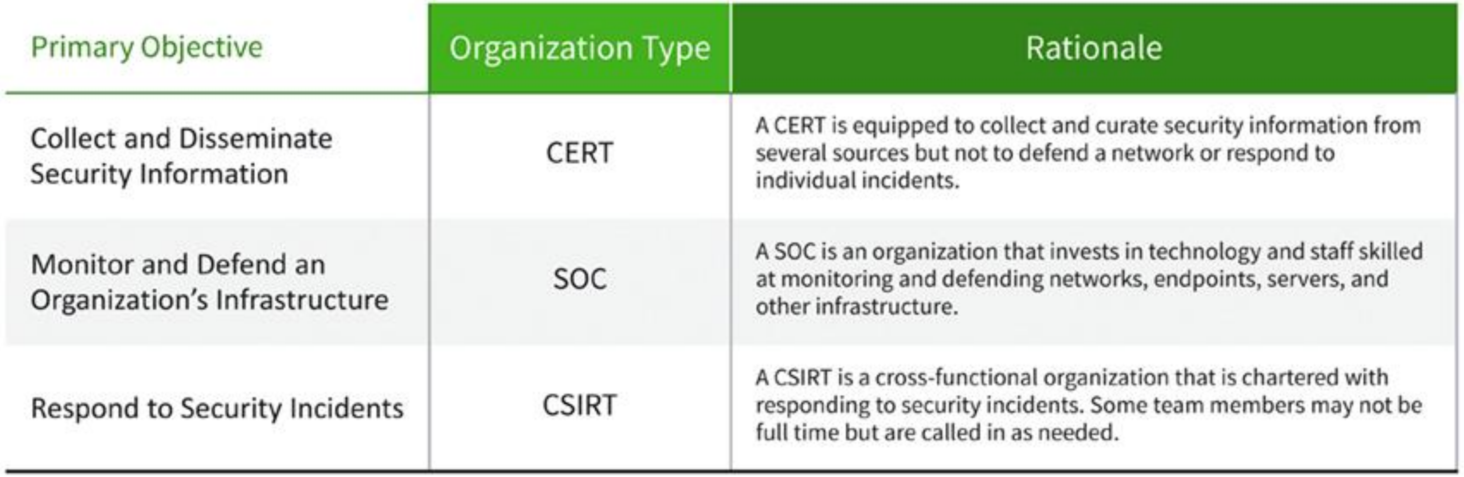
CERT/CSIRT

≠

SOC

How ‘s different?





Primary Objective	Organization Type	Rationale
Collect and Disseminate Security Information	CERT	A CERT is equipped to collect and curate security information from several sources but not to defend a network or respond to individual incidents.
Monitor and Defend an Organization’s Infrastructure	SOC	A SOC is an organization that invests in technology and staff skilled at monitoring and defending networks, endpoints, servers, and other infrastructure.
Respond to Security Incidents	CSIRT	A CSIRT is a cross-functional organization that is chartered with responding to security incidents. Some team members may not be full time but are called in as needed.

https://www.exabeam.com/incident-response/csirt/

The CSIRT Organization

- Defining the CSIRT Organization
- Mission Statement
  - High level definition of what the team will do
- Constituency
  - Whose incidents are we going to be handling or responsible for
  - And to what extent
- CSIRT position / location in the Organization
- Relation to other teams (or organizations)

Different kinds of CSIRTs

- The type of activities, focus and capabilities may be different
- Some examples
  - National CSIRTs
  - Sector based CSIRTs
  - Vendor CSIRTs
  - (Network & Content) Providers Teams
  - Organization CSIRTs

Possible Activities

- Alerts & Warnings
- **Incident Handling**
- Vulnerability Handling
- Artifact Handling
- Announcements
- Technology Watch
- Audits/Assessments
- Configure and Maintain Tools/Applications/Infrastructure
- Security Tool Development

- Intrusion Detection
- Information Dissemination
- Risk Analysis
- Business Continuity Planning
- Security Consulting
- Awareness Building
- Education/Training
- Product Evaluation

No one does all of these !

List from CERT/CC :http://www.cert.org/csirts/services.html

Why we need CSIRT?

- Get notified
- Reduce Impact of Security Incident
- Understand the (root) cause
- Do Something About It

Get notified

- How can other CERTs/CSIRT contact you?
  - Incidents
  - Source of Security Incidents
  - Suspicious activities
  - Threat Information
- Whois db and other
- Will you do something about it?
  - Awareness, Capabilities, Policies & Procedures
- All of the above: Preparedness

Reduce Impact of Security Incident

- Timeliness
- Security Incidents have affect constituent's
  - Operation, Business, Image / Brand, and Safety
- Understand the (root) cause
  - Advise / Alert the constituents
- Reduce cost required to fix

Do Something About It

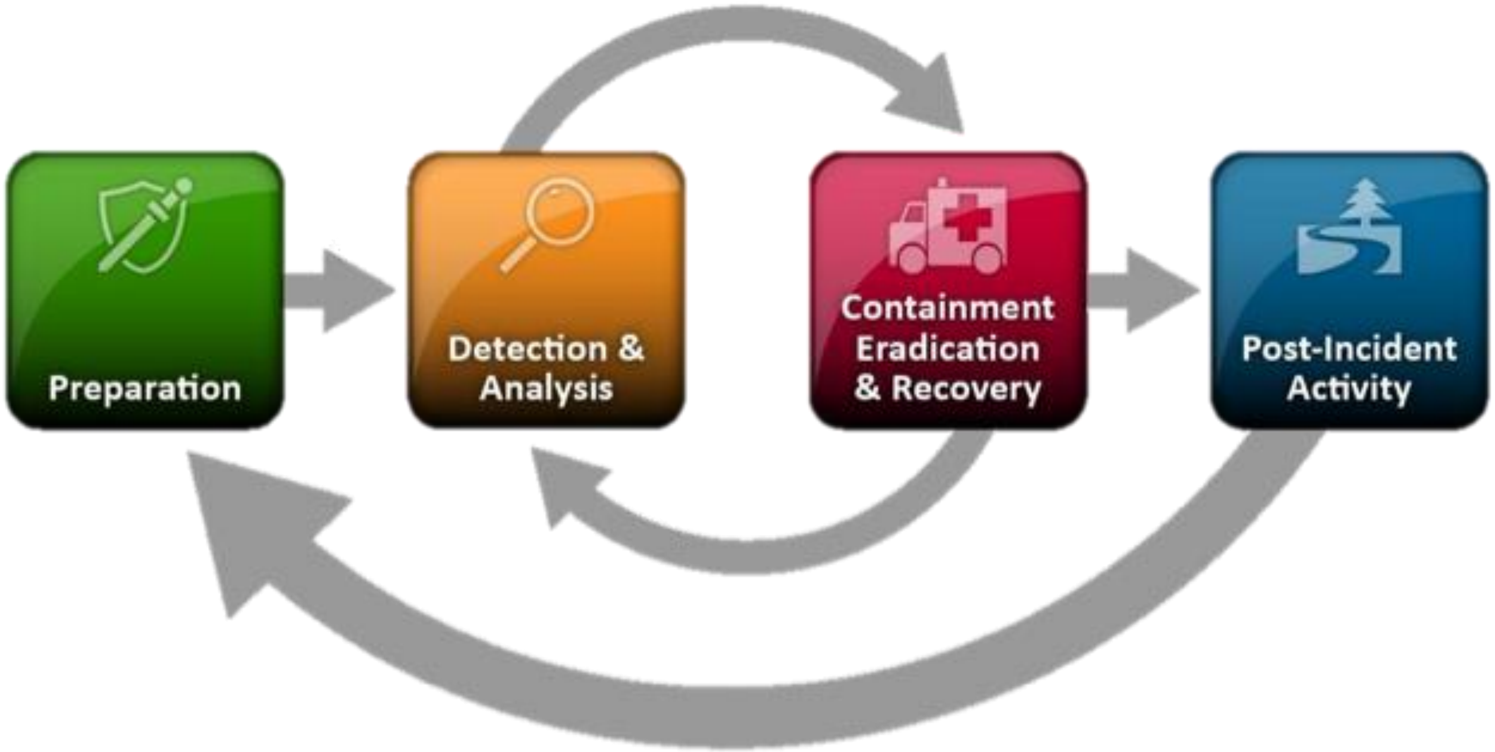
- Remediation
  - Analysis, Collaboration, and Escalation
- DDoS Example
  - Fixing / removing vulnerable hosts
  - Fixing / removing vulnerable services
  - BCP 38 / Source Address Validation
  - Continuous Monitoring
- Join industry-wide initiatives

Resource Considerations

- People, Process and Technology Requirements
- People
    - Resources for:
        - Handling Incidents Reports (Dedicated?)
        - Technical Analysis & Investigation
    - What kinds of skills are required ?
        - Familiarity with technology
        - Familiarity with different types of security incidents
        - Non-Technical skills - Communication, Writing
        - Trustworthiness

- Process & Procedures
    - Generally, from the beginning of incident till when we resolve the incident
    - Including lessons learned & improvement of current policies or procedures
    - Must be clear so that people know what do to
    - Importance
- Specific Procedures for Handling Specific types of Incidents
    - Malware Related, DDoS, Web Defacement, Fraud, Data Breach, …..

Incident Response Process



Source: Special Publication 800-61* Computer Security Incident Handling Guide Figure 3-1 * https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Collaboration & Information Sharing

- Bad guys work together, Good guys should too!
- Make yourself known, establish trust, collaborate and learn from others
- Association of CSIRTS
  - Sector based – Financial sector (TB-CERT, TCM-CERT, and TI-CERT)
  - National CSIRTs groups (in some countries)
  - Regional – APCERT, OIC-CERT, TF-CSIRT
  - Global – FIRST.org
- Closed & Trusted Security Groups
  - NSP-SEC
  - OPS-TRUST
- Getting Feeds about your constituencies (and sharing with them)
  - ShadowServer Foundation
  - Team Cymru
  - Honeynet Project

Key success factors for handling the incidents and working with other CSIRT/CERTs

- Trust
  - Share information /incidents/ resources
  - Control all information by using TLP
- Collaboration
  - Members/ Constituencies
  - Other CERTs in Thailand
  - Other CIIs
  - Communities

Q&A