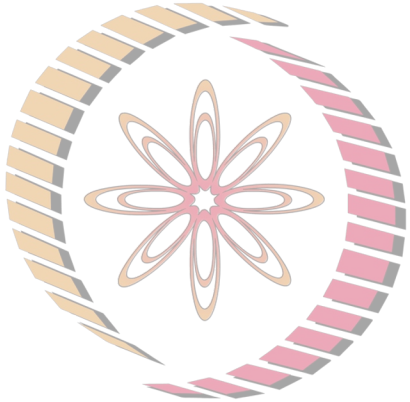
# Cyber Security and Privacy
# MS6880



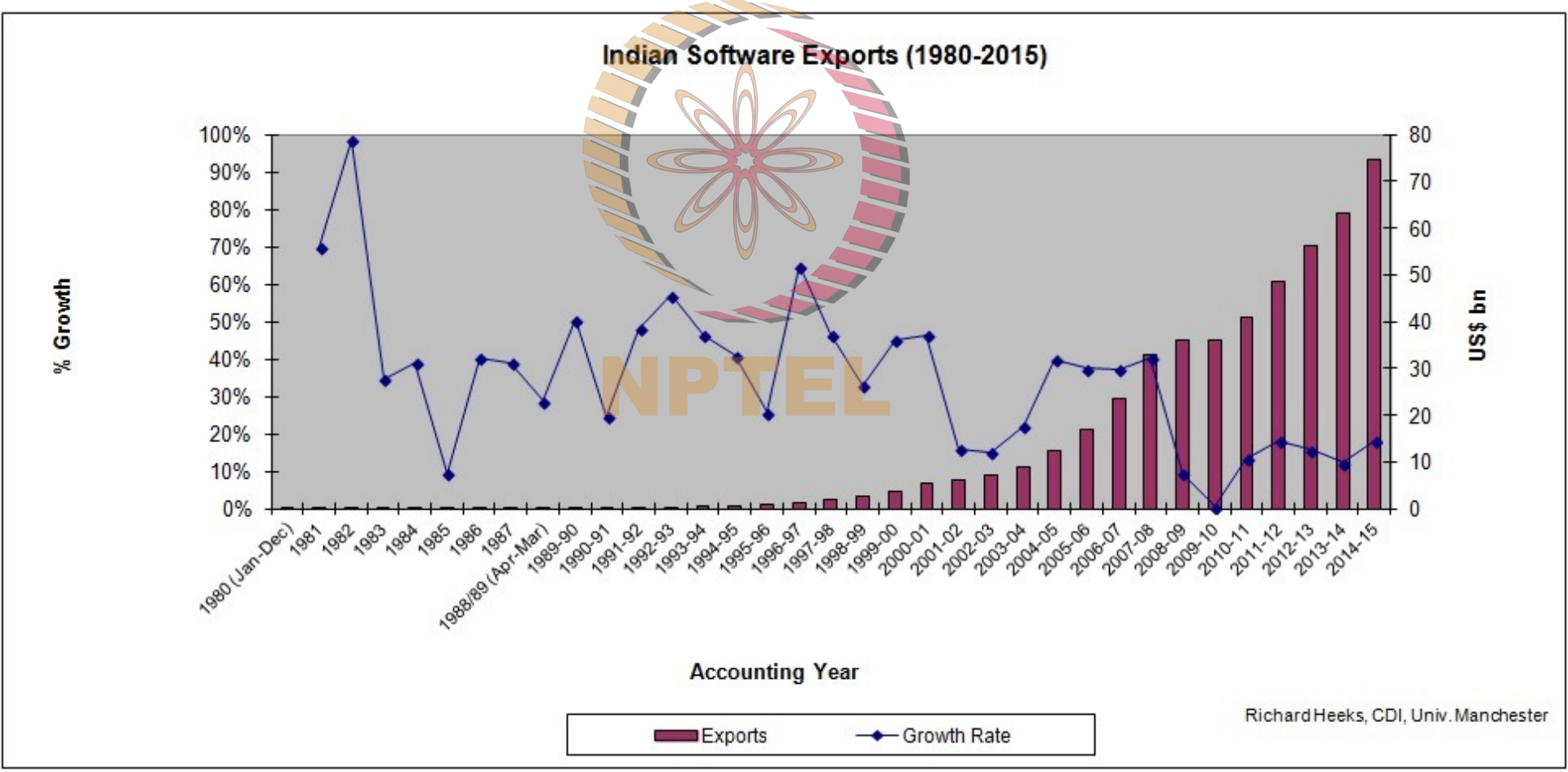
## Cybersecurity policy

Saji K Mathew, PhD
Professor, Management Studies
INDIAN INTITUTE OF TECHNOLOGY MADRAS

# Policy influences progress

- India's policy landmarks
  - Industrial policy: 1949
  - *Entry of foreign players restricted: 1972*
  - New Computer Policy: 1984
  - Policy on Computer Software Export, Development, and Training: 1986
  - Software Technology Park (STP): 1990
  - Economic liberalization: 1991

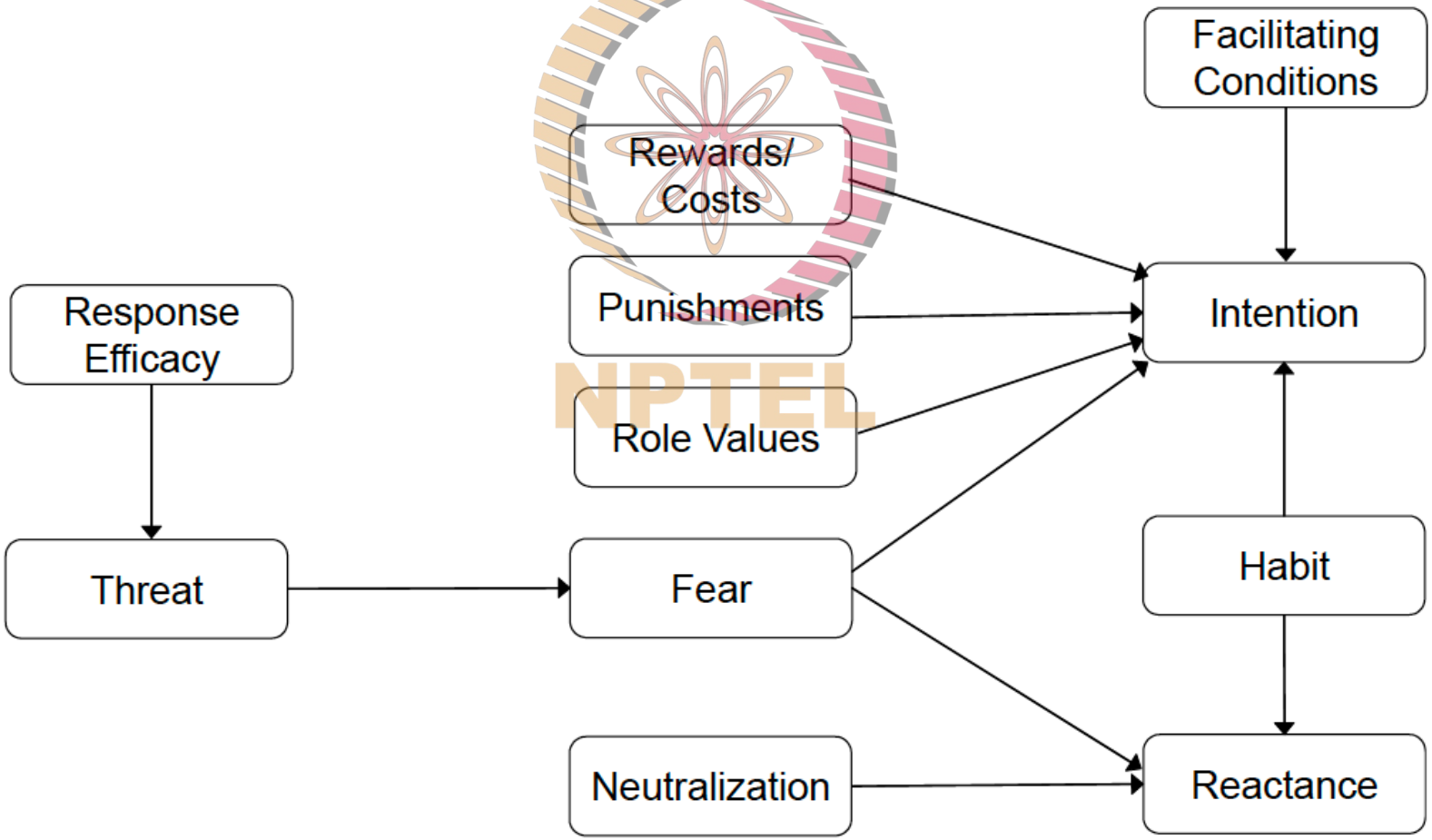
# Policy influences behavior




Source: Richard Heeks, https://ict4dblog.wordpress.com/author/richardheeks/page/4/

# Policy influences individual behavior

(Moody et al., 2018)






**Step 3 of the Unified Model of Information Security Policy Compliance**

# Introduction

- Policy is the essential foundation of an effective information security program
- Some basic rules must be followed when shaping a policy:
  - Never conflict with law
  - Stand up in court
  - Properly supported and administered
  - Contribute to the success of the organization
  - Involve end users of information systems



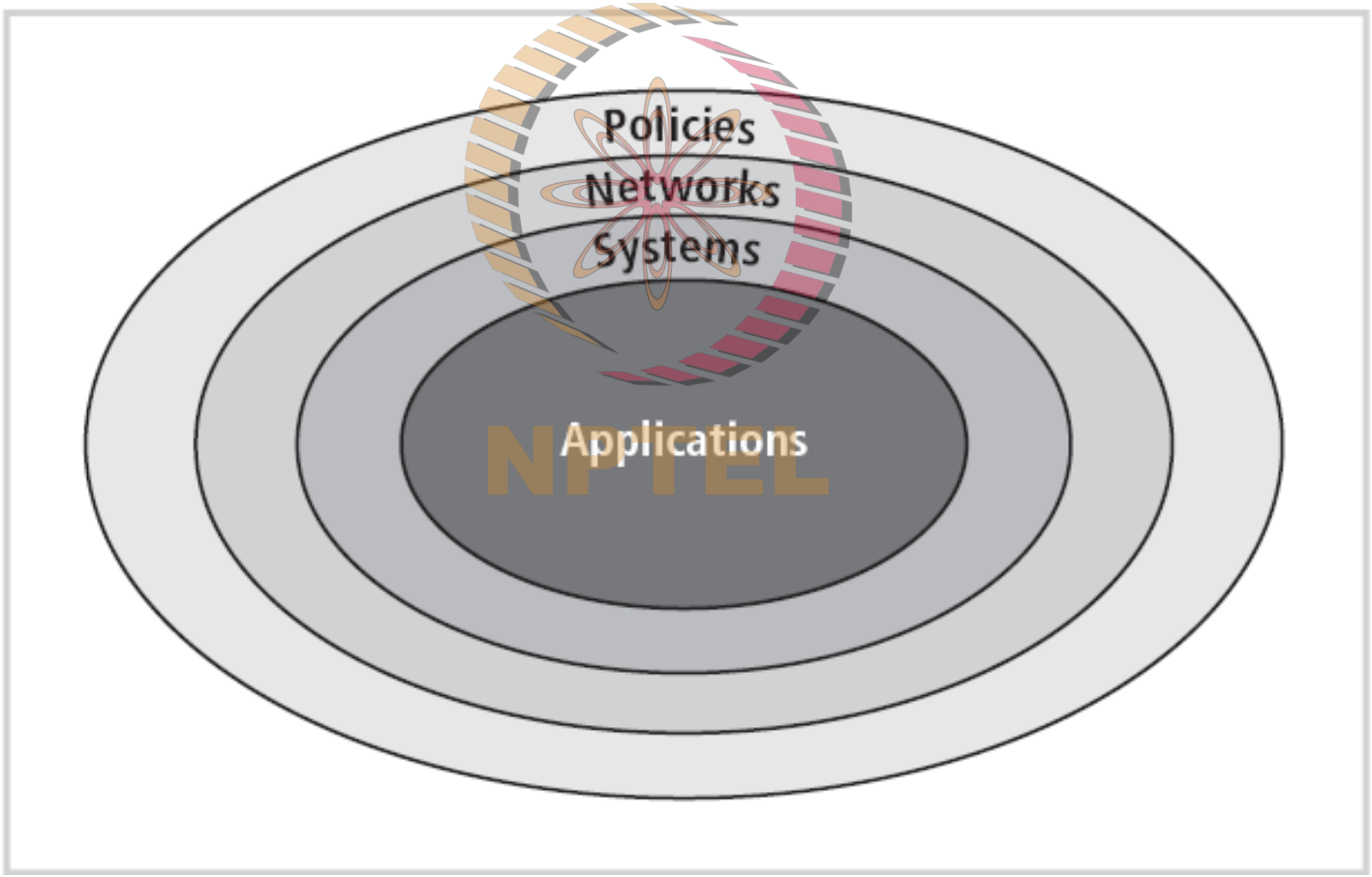
**Warning**. Child abuse is illegal. Creating, possessing, and viewing child pornography content (imagery or video) is prohibited by law. If you see such activity, report it at cybercrime.gov.in. If you are a victim of child abuse, please consider calling Childline for support.
cybercrime.gov.in

CHILDLINE

1098

Hours: Available 24 hours everyday
Website: http://www.childlineindia.org.in/

# The Bulls-eye Model



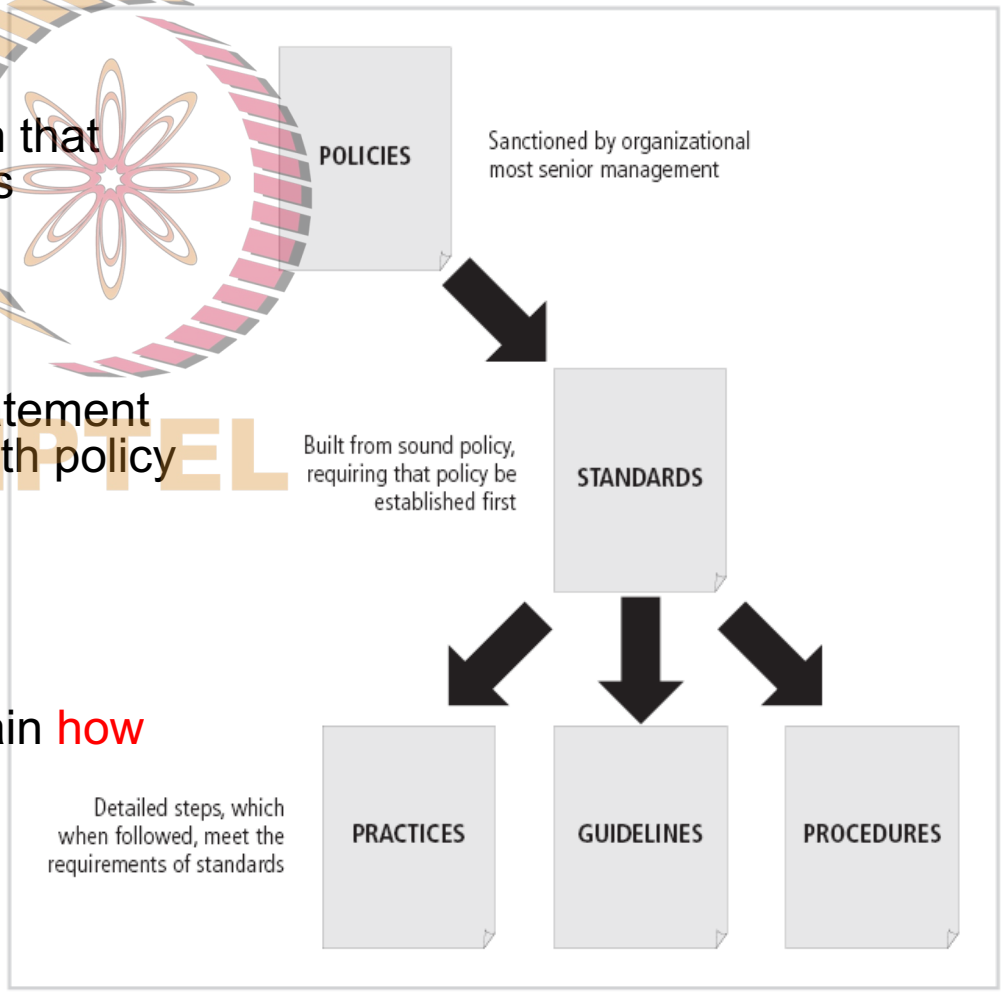

Policies are important reference documents for internal audits and for the resolution of legal disputes about management's due diligence, and policy documents can act as a clear statement of management's intent

# Policies, Standards, & Practices

**Policy** is a plan or course of action that influences and determine decisions

**Standards** are a more detailed statement of what must be done to comply with policy practices

**Procedures and guidelines** explain how employees will comply with policy




Policy must be properly disseminated, read, understood, and agreed-to

Security Education Training Awareness (SETA)

# Policy, Standards, and Practices

- Policies require constant modification and maintenance
- In order to produce a complete information security policy, management must define three types of information security policy:

1. Enterprise information security program policy (EISP)
2. Issue-specific information security policies (ISSP)
3. Systems-specific information security policies (SysSP)

# Enterprise Information Security Policy (EISP)

- Sets strategic direction, scope, and tone for organization's security efforts
- Assigns responsibilities for various areas of information security
- Guides development, implementation, and management requirements of information security program

# Components of the EISP

- Statement of Purpose - What the policy is for
- Information Technology Security Elements - Defines information security
- Need for Information Technology Security - Justifies importance of information security in the organization
- Information Technology Security Responsibilities and Roles - Defines organizational structure
- References Information Technology standards and guidelines

# Issue-Specific Security Policy (ISSP)

- Provides detailed, targeted guidance to instruct the organization in secure use of technology systems, and begins with introduction to fundamental technological philosophy of the organization
- Documents how the technology-based system is controlled; and identifies the processes and authorities that provide this control
- ISSP requires frequent updates
- Serves to *indemnify* the organization against liability for an employee's inappropriate or illegal system use

# ISSP issues/topics

- Contains a statement on the organization's position on an issue
- ISSP topics could include:
  - electronic mail,
  - use of the Internet and the World Wide Web,
  - specific minimum configurations of computers to defend against worms and viruses,
  - prohibitions against hacking or testing organization security controls,
  - home use of company-owned computer equipment,
  - use of personal equipment on company networks,
  - use of telecommunications technologies

# Components of the ISSP

- Statement of purpose
  - Scope and applicability
  - Definition of technology addressed
  - Responsibilities
- Authorized access and usage of equipment
  - User access
  - Fair and responsible use
  - Protection of privacy

# Components of the ISSP (contd)

- Prohibited usage of equipment
  - Disruptive use or misuse
  - Criminal use
  - Offensive or harassing materials
  - Copyrighted, licensed, or other intellectual property
  - Other restrictions
- Systems management
  - Management of stored materials
  - Employer monitoring
  - Virus protection
  - Physical security
  - Encryption

# Components of the ISSP (contd)

- Violations of policy
  - Procedures for reporting violations
  - Penalties for violations
- Policy review and modification
  - Scheduled review of policy and procedures for modification
- Limitations of liability
  - Statements of liability or disclaimers

# Systems-Specific Policy (SysSP)

- Systems-specific policies (SysSPs) are created to function as standards or procedures to be used when configuring or maintaining systems
- SysSPs can be separated into:
  - Management guidance
    - Eg: How to configure a firewall
  - Technical specifications
    - Eg.: Configuration of the firewall

# Management Guidance SysSPs

- Created by management to guide the implementation and configuration of technology
- Applies to any technology that affects the confidentiality, integrity or availability of information
- Informs technologists on management's intent

# Technical Specifications SysSPs

- System administrator's directions on implementing managerial policy
- Each type of equipment has its own type of policies
- There are two general methods of implementing such technical controls:
  - Access control lists
  - Configuration rules

# Access Control Lists

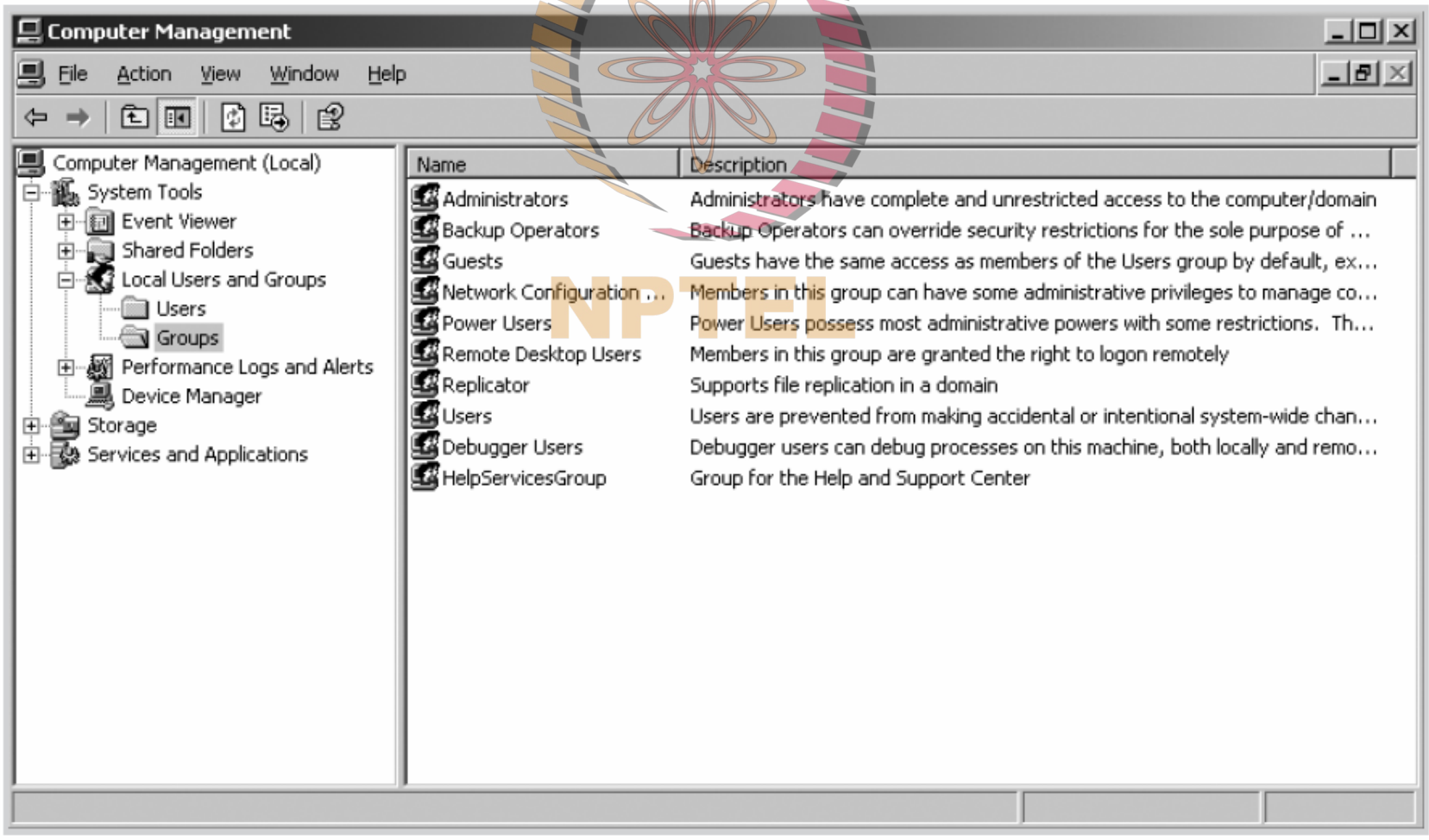
- Include the user access lists, matrices, and capability tables that govern the rights and privileges
- A similar method that specifies which subjects and objects users or groups can access is called a capability table
- These specifications are frequently complex matrices, rather than simple lists or tables
- In general, ACLs enable administrations to restrict access according to user, computer, time, duration, or even a particular file

# ACLs

- In general, ACLs regulate:
  - Who can use the system
  - What authorized users can access
  - When authorized users can access the system
  - Where authorized users can access the system from
  - How authorized users can access the system
  - Restricting what users can access, e.g., printers, files, communications, and applications

  - Set privileges of Read, Write, Create, Modify, Delete, Compare and Copy

# Windows XP ACLs




The list of "built-in" groups specifies which rights individual users have to and within a particular system.

# Configuration Rules

- Configuration rules are the specific configuration codes entered into security systems to guide the execution of the system when information is passing through it
- Rule policies are more specific to the operation of a system than ACLs, and may or may not deal with users directly
- Many security systems require specific configuration scripts telling the systems what actions to perform on each set of information they process

# Firewall Configuration Rules

Rule 7 states that any traffic coming in on a specified link (Comm_with_ Contractor) requesting a Telnet session will be accepted, but logged. This rule also implies that non-Telnet traffic will be denied.

Action specifies whether the packet from Source: is accepted (allowed through) or dropped.

Track specifies whether the processing of the specified packet is written to the system logs.

| NO. | SOURCE | DESTINATION | IF VIA | SERVICE | ACTION | TRACK | INSTALL ON | TIME | COMMENT |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Primary_Manage<br>Dallas_Gateway<br>Dallas_internalM<br>Dallas_Radius | All_Intranet_Gat | * Any | dhcp-r<br>NBT<br>bootp | drop | - None | * Policy Targets | * Any | |
| 2 | Primary_Manage<br>Dallas_Gateway<br>Dallas_internalM<br>Dallas_Radius | All_Intranet_Gat | * Any | * Any | drop | Log | * Policy Targets | * Any | |
| 3 | Primary_Manage | All_Intranet_Gat | * Any | * Any | drop | Log | * Policy Targets | * Any | |
| 4 | * Any | Dallas_network | My_Intranet | MSExchange-20<br>sqlnet1<br>sqlnet2<br>sqlnet2-1521<br>sqlnet2-1525<br>sqlnet2-1526 | accept | Log | * Policy Targets | * Any | Remote offices workers can connect to the exchange server, read and post emails. ERP is also allowed. |
| 5 | * Any | * Any | Dallas_internall_ | NBT | accept | - None | * Policy Targets | * Any | Allow the replica alias to do anything VPNed with the Dallas and vice versa. |
| 6 | * Any | * Any | My_Intranet | * Any | accept | - None | * Policy Targets | * Any | Don't log NBT connections to the file server. |
| 7 | * Any | * Any | Comm_with_Cor | telnet | accept | Log | * Policy Targets | * Any | Support from the contractor is allowed only by telnet. |
| 8 | * Any | Dallas_mail1 | * Any | smtp->SMTP_Sc | accept | - None | * Policy Targets | * Any | |

# IDS Configuration Rules

This section defines which security levels are to be used and who is to be notified if that level file is modified.

This section looks for unauthorized modifications to Internet Explorer Registry edits, most likely due to virus or hacker efforts.

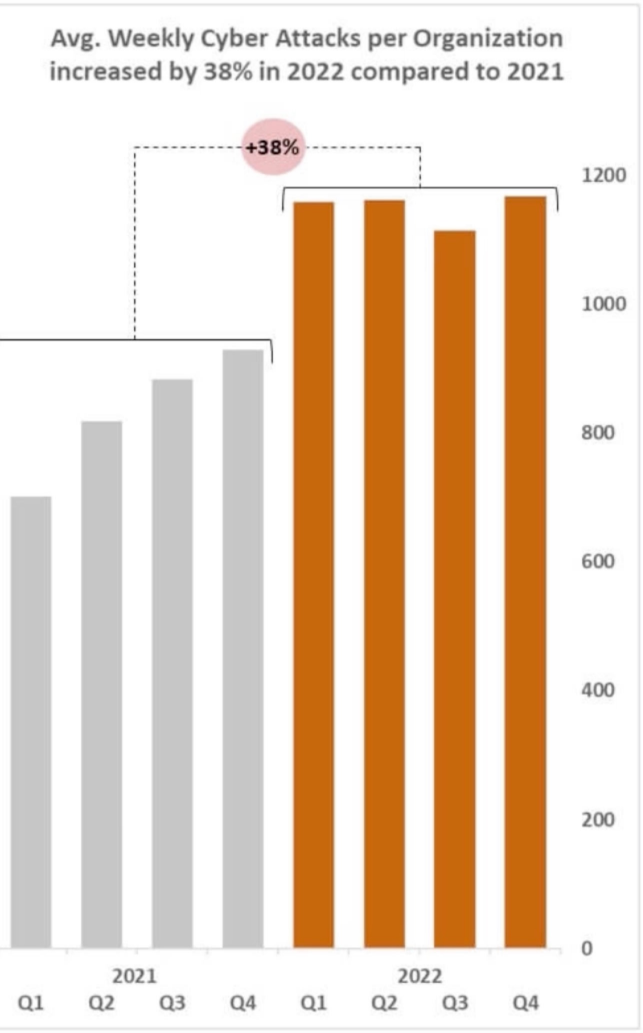
```
##############################################################################
# This Policy was created by the Tripwire Policy Resource Center             #
# Created on: Mon Mar 25 21:54:27 GMT 2002                                   #
#       Copyright (C) 2001, Tripwire Inc. Reprinted with permission          #
##############################################################################
@@section global
SYSTEMDRIVE="C:" ;
BOOTDRIVE="C:" ;
SYSTEMROOT="C:\\Winnt" ;
PROGRAMFILES="C:\\Program Files" ;
IE5="C:\\Program Files\\Plus!\\Microsoft Internet" ;
# Email Recipients # #
SIG_HIGHEST_MAILRECIPIENTS  = "Administrator" ;
SIG_HIGH_MAILRECIPIENTS     = "Administrator" ;
SIG_MED_MAILRECIPIENTS      = "Administrator" ;
SIG_LOW_MAILRECIPIENTS      = "Administrator" ;
# Security Levels # #
SIG_LOW       = 33 ;     # Non-critical files that are of minimal security impact
SIG_MED       = 66 ;     # Non-critical files that are of significant security impact
SIG_HIGH      = 100 ;    # Critical files that are significant points of vulnerability
SIG_HIGHEST   = 1000 ;   # Super-critical files.  Mostly used for the TCB section.
@@section NTFS
{
 rulename = "IE 5.01 Registry keys",
 severity = $ (SIG_HIGHEST),
 emailto  = $ (SIG_HIGHEST_MAILRECIPIENTS),
 recurse  = true
}
{
 $ (HKLM_CCS_SM_CBadApps)                    -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_CRYPT)                              -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_CRYPTINIT)                          -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_CRYPTMSG)                           -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_CRYPTSIGN)                          -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_EventSystem)                        -> $ (REG_SEC_HIGHEST) ;
 $ (HKLM_SW_IE_Setup)                        -> $ (REG_SEC_HIGHEST) ;
```

# Design elements (cont.)

- SETA – Security education, training and awareness program contains
  - Security education
  - Security training
  - Security awareness
- Purpose
  - Improving awareness
  - Developing skills & knowledge
  - Building in-depth knowledge

# INTERNET INSECURITY

BOYA LOKESH - MS21A010
SAYAN BHOWMICK- MS21A060
VIJAY KUMAR - MS21A073




## Key Statistics:

- Global volume of cyberattacks reached an all-time high in Q4 with an average of 1168 weekly attacks per organization.
- Top 3 most attacked industries in 2022 were Education/Research, Government and Healthcare.
- North America (+52%), Latin America (+29%) and Europe (+26%) showed largest increases in cyberattacks in 2022, compared to 2021.
- USA saw a 57% increase in overall cyberattacks in 2022, UK saw a 77% increase and Singapore saw a 26% increase



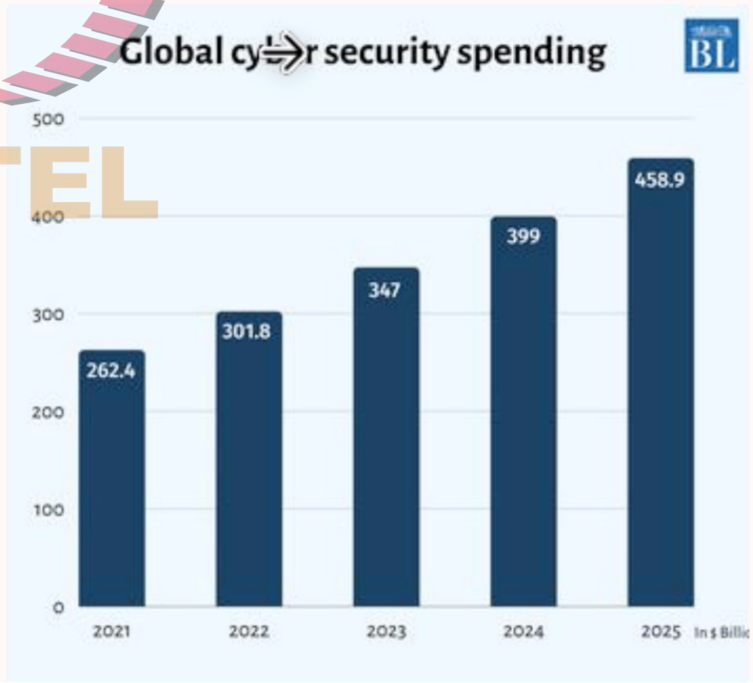
## Does investing in latest cyber defense mechanisms guarantee a success in preventing malware attacks??

**NO AMOUNT OF SPENDING ON DEFENSES WILL SHIELD YOU COMPLETELY FROM HACKERS. IT'S TIME FOR ANOTHER APPROACH.**

# A Staggering growth of global cyber security expenditure

## Global cyber security spending to touch $460 billion by 2025: Kaspersky

- Global cyber security spending has been growing at an average of 15 per cent in the last few years and the annual spending is projected to reach nearly $460 billion by 2025.
- According to Kaspersky, cyber security spending in 2021 was pegged at $262.4 billion, while it is projected to cross the $300-billion mark in 2022.
- Cumulative spending from 2021 to 2025 is set to touch a staggering $1.5 trillion.



# Cyberattacks on critical infrastructure: Increasing complexity and challenges

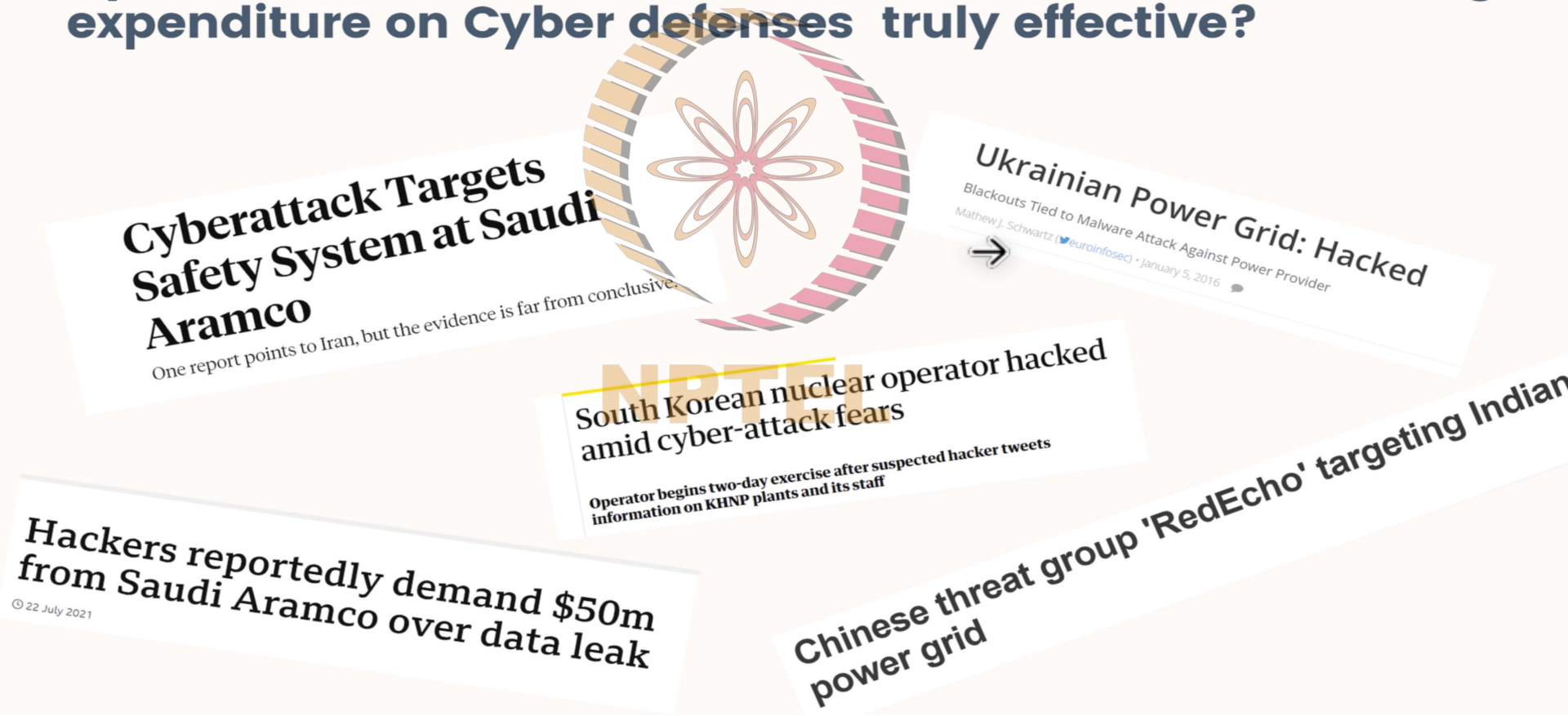
### What are critical infrastructures?

- Energy sector.
- Telecommunication sector.
- Critical manufacturing sector.
- Transportation sector.
- Water treatment.

### Complexity of critical infrastructures:

- Critical infrastructure, like power generation and distribution, is becoming more complex and reliant on networks of connected devices.
- Failure of one critical infrastructure can result in a devastating chain reaction, failing the entire system.

# Cyberattacks on critical infrastructure: is increasing expenditure on Cyber defenses truly effective?



# Cyberattack – A perennial problem for Saudi Aramco


In 2012, threat actors wiped data from approximately thirty-five thousand computers belonging to Saudi Aramco, one of the world's largest oil companies. Malware called Shamoon stole passwords, wiped data, and prevented computers from rebooting.

Malicious software attacked a safety system at Saudi Aramco, the world's largest oil company on december, 2017. The attack was designed to cause the safety controllers to stop working to trigger an explosion in the plant.

On July, 2021, Aramco again fell victim to an extortionist attempt where the company data got leaked by one of its third party contractor. Hackers demanded a whopping 50 miilion dollar to delete the 1000 GB sized data.

# Cyberattack on power grid: A war tactic??


- On April,2022 amid Russia-Ukraine war, the Ukrainian government claimed that it narrowly averted a serious cyberattack on their power grid.
- Hackers targeted Ukraine's largest energy companies to shut down power plants which could have triggered a blackout had they suceeded.
- Sourced revealed that it was part of a war tactic by Russia as a blackout would have made their invasion of Ukraine easier.

# Digital transformation – Capability vs Vulnerability

- Rapid digitalisation of industrial control system have made plant assets more vulnerable to cyber attacks.
- IoT, AI-ML and cloud technologies have made decision making faster and efficient rendering them indispensable in the age of hypercompetition.





- Industries are dealing with terabytes of data on a regular basis which makes defending of cyber threats highly complex.
- Growing sophistication has made a well coordinated cyber attack almost impossible to counter.

# Does fast pace of digital transformation requires increased security ?



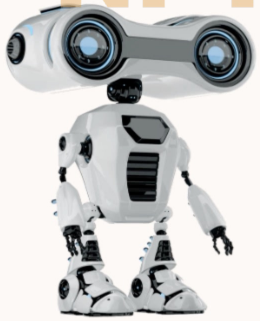

Whatever a company's vision for the future, it must include digital transformation in order to grow


- Make better decisions, faster
- Employees need modern tools to be effective
- Everyone expects an on-demand service

# Growing Vulnerability - issues and challenges

- The pace of digital transformation continues to accelerate with the growth of automation.
- The propagation of and growing dependency on digital technologies poses a threat.
- Vendors who create and know them best don't fully understand their vulnerabilities.





- Automation considered as a way to remove risks posed by fault-prone humans, but it just replaces those risks with others

- Business leaders have been unable to resist the allure of digital technologies and the many benefits they provide
- Leaders spend more and more every year on new security solutions and high-priced consultants

# Cyber Hygiene



Set of practices organizations and individuals perform regularly to maintain the health and security of users, devices, networks and data

## Benefits

- Protect customer data
- Meet compliance requirements
- Locate unmanaged assets

# Regular Approaches of Cyber Hygiene

- Buying and deploying the latest defensive hardware & software tools.
- Regularly training employees to recognize and avoid phishing emails.
- Creating “air gaps” — separating important systems from other networks and the internet .
- Building a large cybersecurity staff supplemented with various services and service providers to do all of the above

## Organizations adhere to best-practices

- Mandating employees to use complex passwords and change them frequently.
- Encrypting data and installing new security patches.
- Segmenting networks by placing firewalls between them.
- Limiting access to sensitive systems.

NO MATTER HOW GOOD YOUR COMPANY'S CYBER HYGIENE IS, A TARGETED ATTACK WILL PENETRATE YOUR NETWORKS AND SYSTEMS.

## Limitations

- Ineffective against well coordinated , targeted and persistent threats posed by sophisticated adversaries.
- Creating comprehensive inventories of the company's hardware and software assets in asset-intensive industries such as energy, transportation, etc is typical.
- Security upgrades usually require that systems be shut down for installation, but that's not always feasible.

# INL'S RADICAL IDEA

## DIfferent Approach

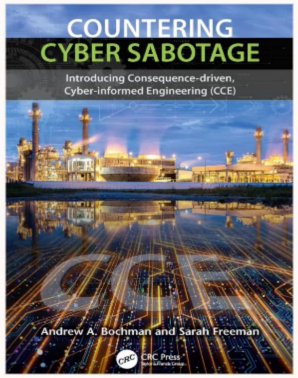
- Identify the most essential processes and functions.
- Reduce or eliminate the digital Pathways attackers could use to reach them.
- Shift away from full reliance on digital connectivity

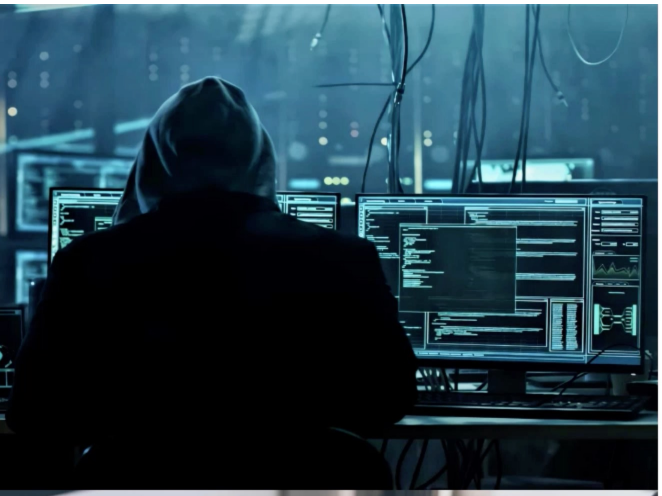
## Idaho National Lab's

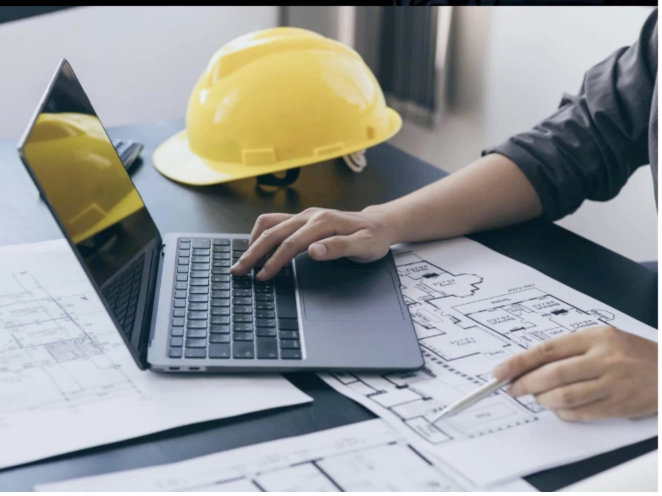
- stepwise concept approach
- Consequence-driven, Cyber-Informed Engineering [CCE] methodology.
- Companion Framework-Cyber Informed Engineering {CIE}

**ANDREW BOCHMAN**
**Idaho National Laboratory**
**Senior grid strategist ,National and Homeland Security at Idaho National Lab.**

- **Provides strategic guidance on critical infrastructure security to senior U.S. and international governments and industries.**
- **Hes Ex US Air Force ,**
- **Was global energy and utilities security lead at IBM and is a cybersecurity subject matter expert listed with the U.S. State Department**





## CCE

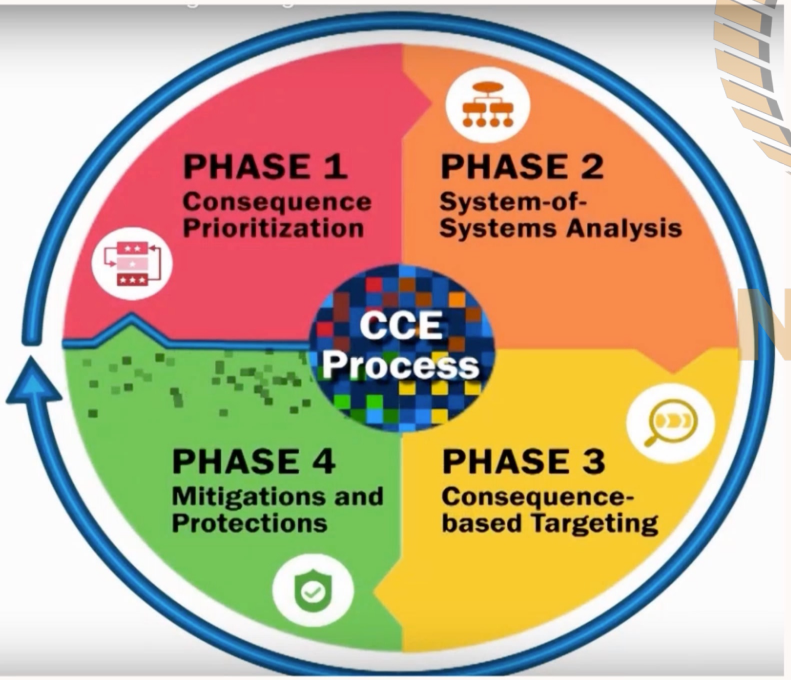
- Consequence Driven Cyber Informed Engineering
- Objective-Change in cyber risk perception of hierarchy.
- Target- licensed Implementation by service firms by 2020.

## CIE

- Cyber Informed Engineering →
- Companion Framework
- Similar to CCE in many respects.
- Objective-Integrating cyber risk mitigations across the entire engineering life cycle.

- **Challenge from Engineering perspective** - understanding impact of cyber-attacks across the entire product and program lifecycle.
- **Evolving nature of cyber threats-** impacts design, development, deployment, and operational phases of all systems.
- CCE and CIE processes teaches to heed and incorporate cyber security aspects at design stage of the components themselves.

# 4 STEPS




## Implementation

- CCE master — INL & INL trained personnel.
- Corporate Hierarchy-Heads of Regulatory compliance,litigation, and mitigating risks & CEO, COO,CFO.
- People who oversee core operational functions.
- Safety system experts , operators and engineers familiar with the companies critical processes .
- Cyber experts and process engineers who know how systems and equipment can be misused

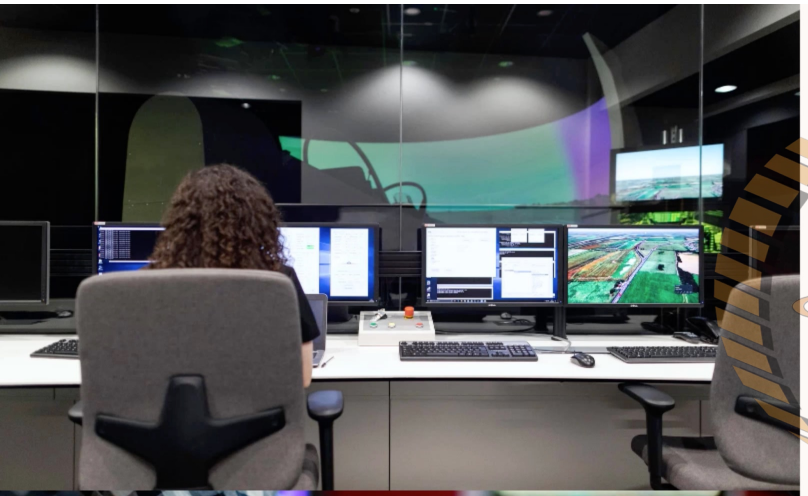


## The Process

- Identify “Crown Jewel” Processes
- Map the Digital Terrain
- Illuminate the Likely Attack Paths
- Generate Options for Mitigation and Protection

# Recommendations

- Learn to think like your adversaries
  - internal team to war game scenarios.
  - Assess defensive strength of critical targets.
  - Team of experts - control and safety systems, and operational networks.
- Notwithstanding consistently high levels of cyber hygiene, you must prepare for a breach
  - Cyber Safety Culture-Create culture like of elite chemical factories and nuclear power plants.
  - Employee Awareness- From senior to the most junior, awareness of glitch/abnormality recognition and SOP to be followed .
- Contingency Planning -
  - Support critical systems functioning
  - Continuity of essential operations-reduced level if required
  - Switch to analogous/digitally air gapped-backup system not to rely on digital technologies.
  - Air gapped from network — particularly the internet.



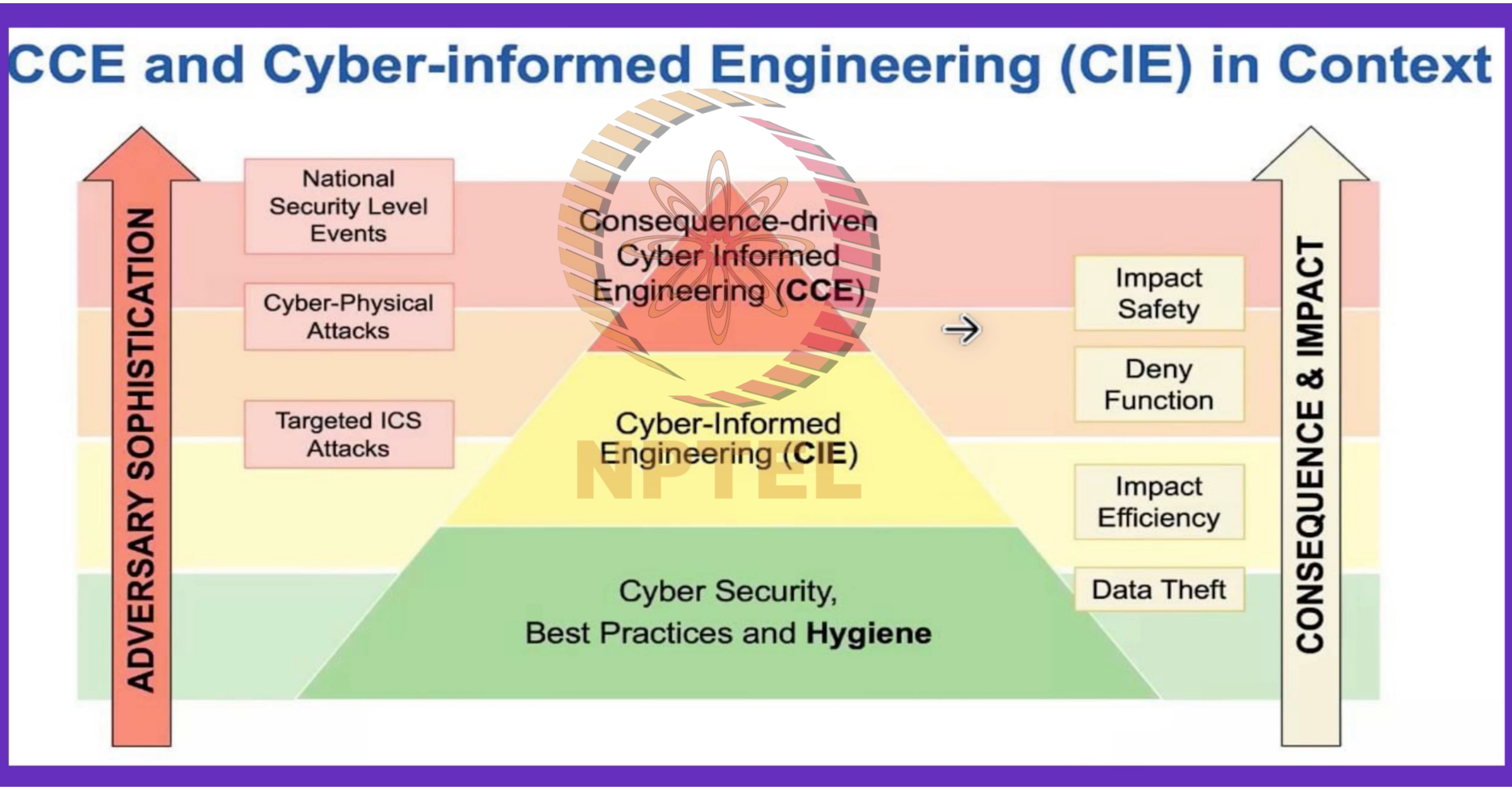
## Why Cyber Informed Engineering?

- Traditional engineering methods do not account for cyber risks.
- Engineering curriculum does not include cyber risk mitigation.
- Bolt on IT security solution put (fireWall,virus scanning etc..detection system)- does not work on digital industrial control systems.
- Engineers weed out risk,Thats their job .
- Through known risk models-common platform.



## Better Understanding-Cyber Informed Engineering

- Defi-Awareness of security challenges in operating digital /non digital indutsrial systems.Teach to ask right questions.
- What is it? -Not a check list..Philosphy to characterize cyber risks of digital control systems...Abstract...
- Objective-Promulgation of a strategy to learn to view cyber like other modes of failure.


CCE and Cyber-informed Engineering (CIE) in Context
ADVERSARY SOPHISTICATION
National Security Level Events
Cyber-Physical Attacks
Targeted ICS Attacks
Consequence-driven Cyber Informed Engineering (CCE)
Cyber-Informed Engineering (CIE)
Cyber Security, Best Practices and Hygiene
Impact Safety
Deny Function
Impact Efficiency
Data Theft
CONSEQUENCE & IMPACT
NPTEL

# CONCLUSION

- Cyber attack Vulnerability -All organization depending on digital technologies and internet -vulnerable to devastating cyberattack.
- Cyber Adversaries-Highly skilled, well-resourced criminal and terrorist groups,nation states.
- Strategy-Technological step backward vs smart engineering step forward.
- Continuity /Survivability-Goal to reduce, if not eliminate, the dependency of critical functions on digital technologies and their connections to the internet.
- FRA/FRM- higher cost vs potentially devastating price of business as usual.