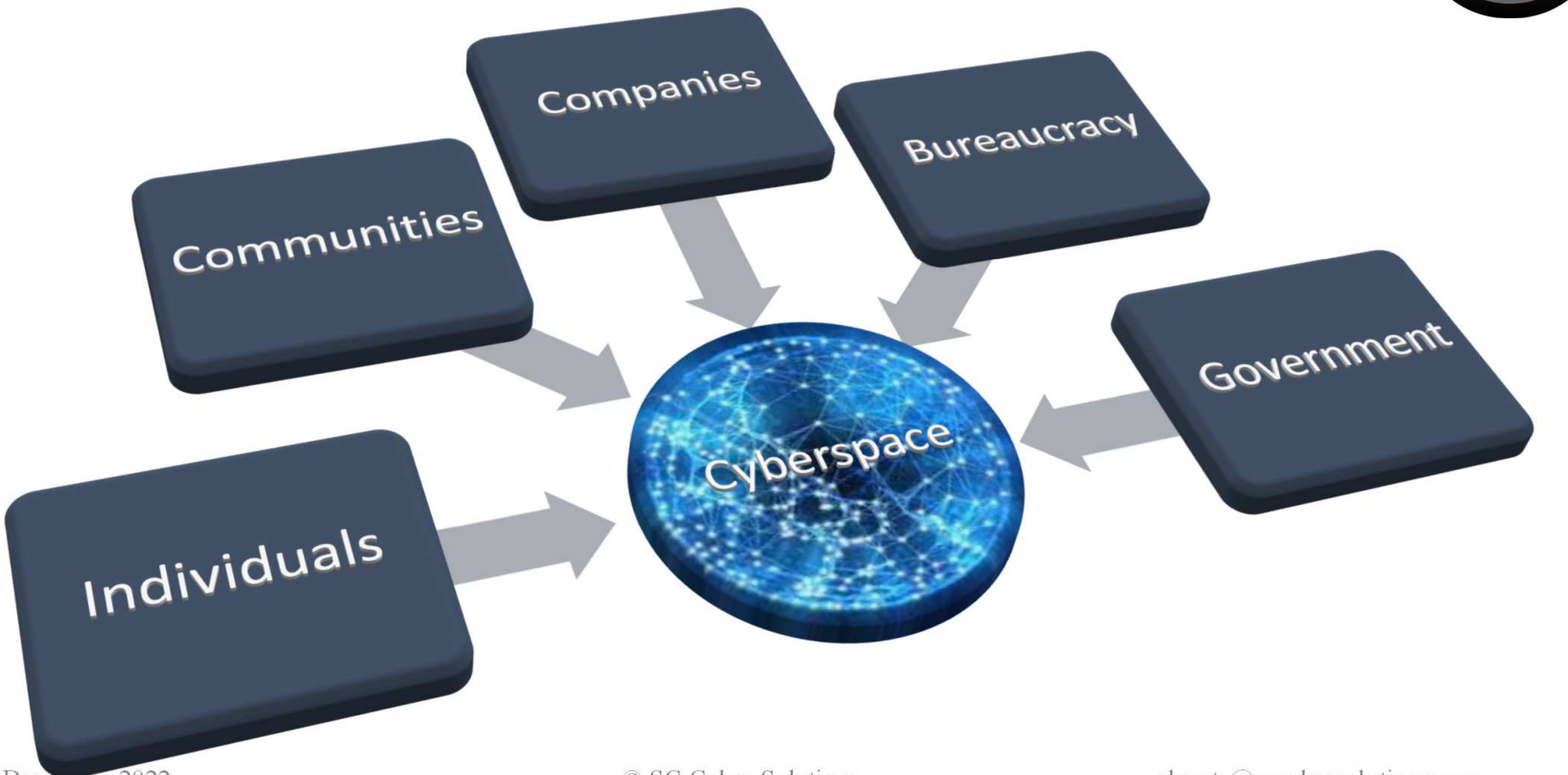
Compliance

Shweta A. Chawla
Founder & Investigator
SC Cyber Solutions

Stakeholders in Cyberspace



Communities

Companies

Bureaucracy

Government

Individuals

Cyberspace

Cyber Threats

Cyber Crimes

- Malware
- Financial
- Unauthorised access
- Espionage

Natural Disasters

- Earthquakes
- Floods

Cyber Attacks

- Malware
- DoS
- Misinformation
- Critical Infrastructure Attacks
    - Banking
    - Power
    - Water
    - GPS
    - Internet

Protection against Cyber Threats

Technological

- Proactive
  - AV
  - IDS
  - IPS
  - SIEM
  - Pentesting
  - Secure coding
  - Monitoring

- Reactive
  - Investigation
  - Risk mitigation
  - Evolution

SC
Cyber Solutions

Protection against Cyber Threats

Human

- Proactive
  - Awareness
  - Training
  - Vigilance
  - Governance
  - Policy
  - Legislation

- Reactive
  - Insurance
  - Litigation

Policy

- A course or principle of action adopted or proposed by the governing body of a government, business, or individual
- It is a deliberate set of guidelines to achieve outcomes
- A statement of intent
- A policy can help with subjective and objective decision making

WHY SOMETHING IS DONE

Standard

- Stipulates uniform (hence standard) use of something
- Applies to technology, settings, configuration
- Could be internal or by a third party
- Often helps an user/organization comply with a policy

WHAT IS DONE

Procedure

- Mandatory steps to be followed to achieve a desired outcome, usually a task or a policy outcome
- Often takes the form of a checklist
- Informs users on how to implement a policy
- Mandatory in nature

HOW SOMETHING IS DONE

SC
Cyber Solutions

Guideline

- Provides information, advice and guidance
- General in nature
- Usually aligned towards a policy
- Guidelines offer suggestions
- Following guidelines is a voluntary activity
- Provide flexibility for unexpected situations / circumstances

SC
Cyber Solutions

What is Compliance?

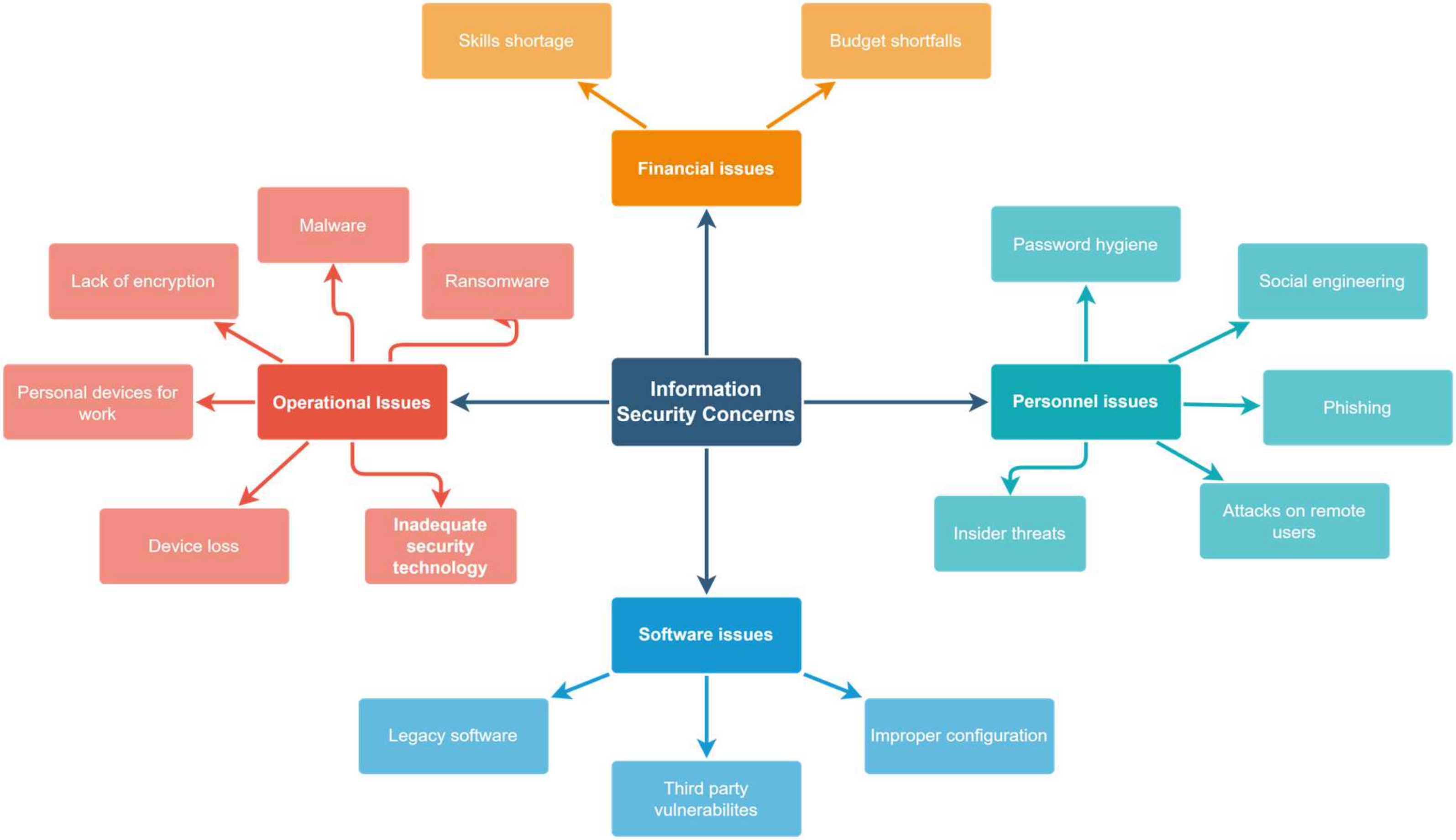
- The act of obeying an order, rule or request
- Conformity in fulfilling official requirements
- Conforming to a specification, standard or law that has been clearly defined
- The state of being in accordance with established guidelines or specifications, or the process of becoming so.

- Audit: an official examination of the present state of something
- IT audit: Auditing of information technology, computer systems, networks, etc.

- Compliance means conforming to
  - Laws
  - Regulations
  - Policies
  - Procedures
  - Obligations

SC
Cyber Solutions

InfoSec Concerns



Security Audit

- A security audit
  - Many ways organisations test and assess their overall security posture incl cyber security
  - A comprehensive assessment of the organization's information system
  - Typically, this assessment measures information system's security against an audit checklist of industry best practices, externally established standards, or federal regulations

- Security audits will help
  - protect critical data
  - identify security loopholes
  - create new security policies
  - track the effectiveness of security strategies

- Regular audits can help ensure employees stick to security practices and can catch new vulnerabilities.

SC
Cyber Solutions

Benefits of Security Audit

- Test adequacy of current security strategy
- Test security training efforts
- Uncover extraneous hardware and software
- Reduce costs by removing unnecessary resources
- Identify flaws in new technology or processes
- Verify compliance with regulations

Types of Security Audits

- Risk assessment
- Vulnerability assessment
- Penetration testing
- Compliance audit

Types of Security Audits

- Internal audits
- External audits
- Ideally all stakeholders must be involved in the process

Internal Audit Team

- Why does an Internal Audit Team exist?
  - Assurance that internal controls exist and are functioning
  - Improve the state of these internal controls
  - Reporting security issues
  - Monitoring mitigation

- Qualities of an auditor
  - Objective
  - Unbiased

Qualities of an Auditor

- Ability and willingness to dig into details without getting lost in them
- Analytical skills
- Written and oral communication skills
- Ability to learn new technology / areas
- Ability to look for areas of weakness and risk quickly
- Relationship building

Phases of a Security Audit

- **Pre-audit agreement**
  - Scope and objectives
  - Level of support provided
  - Locations, duration
  - Financial considerations
  - Audit protocols
  - NDAs etc
- **Initiation and planning**
  - Risk assessment
  - Research
  - Preliminary review
  - Audit objective
  - Formal agreement
  - Entrance conference
- **Fieldwork**
  - Interview
  - Inspection
  - Observation
  - Re-performance
  - Testing
- **Analysis**
  - Confirmation
  - Verification
  - Reconciliation
  - Exit conference
- **Reporting**
  - Findings
  - Recommendations
  - Client responses
  - Draft reports
  - Final report
  - Schedule client corrective action report
  - Plan for follow-up engagement
- **Follow-up**
  - Confirm corrective action
  - Address challenges
  - Repeat phases (As necessary)

Audit Workflow

- Define assessment criteria
  - Clearly define goals at onset
  - Determine overall objectives and then break them down into departmental priorities
  - Agree on how the audit is performed and tracked
  - Maintain a record of out-of-scope items and things being exempted
  - Take into account
    - Industry and geographic standards
    - Create and maintain a threat catalog of all discovered threat vectors
    - Decide on stakeholder involvement and their ability/permission to participate
    - Use outside resources if and when possible
- Prepare the security audit
  - Prioritise success criteria and business objectives
  - Select the tools and methodologies to meet the goals
  - Find or create methods to gather the correct data

- Conduct the security audit
  - Avoid shortcuts
  - Provide appropriate documentation
  - Perform due diligence
  - Monitor audit progress and data points for accuracy
  - Use previous audits and new info to deep dive into findings
  - Prioritise deep dives as required
- Complete and share the results
  - A security audit is focused on uncovering risk; stay focused on it
  - Share results with all previously determined parties
  - Create a list of action items based on audit findings
  - Prioritise fixes to remediate security items discovered

  - Source: https://www.varonis.com/blog/security-audit

Assessment Types

- One time: For special events eg introduction of new software
- Tollgate: yes or no response to using a new process
- Portfolio: Regularly scheduled audits to verify and assess procedures

- Source: https://www.varonis.com/blog/security-audit

Stitching Auditing through the Work Processes

- Consult on improving internal controls all through the work process
- Discuss them with company teams
- Get involved early in the development/design stage
- Conduct informal audits
- Share learnings

Thank You!

Contact details:
Mob: +91 98230 80864
shweta@sccybersolutions.com
www.sccybersolutions.com
@sccs1300