Chapter 14 – Resilience Engineering

Topics covered

- ✧ Cybersecurity
- ✧ Sociotechnical resilience
- ✧ Resilient systems design

Resilience

- *The resilience of a system is a judgment of how well that system can maintain the continuity of its critical services in the presence of disruptive events, such as equipment failure and cyberattacks.*

- Cyberattacks by malicious outsiders are perhaps the most serious threat faced by networked systems but resilience is also intended to cope with system failures and other disruptive events.

Essential resilience ideas

- The idea that some of the services offered by a system are critical services whose failure could have serious human, social or economic effects.
- The idea that some events are disruptive and can affect the ability of a system to deliver its critical services.
- The idea that resilience is a judgment – there are no resilience metrics and resilience cannot be measured. The resilience of a system can only be assessed by experts, who can examine the system and its operational processes.

Resilience engineering assumptions

- Resilience engineering assumes that it is impossible to avoid system failures and so is concerned with limiting the costs of these failures and recovering from them.
- Resilience engineering assumes that good reliability engineering practices have been used to minimize the number of technical faults in a system.
- It therefore places more emphasis on limiting the number of system failures that arise from external events such as operator errors or cyberattacks.

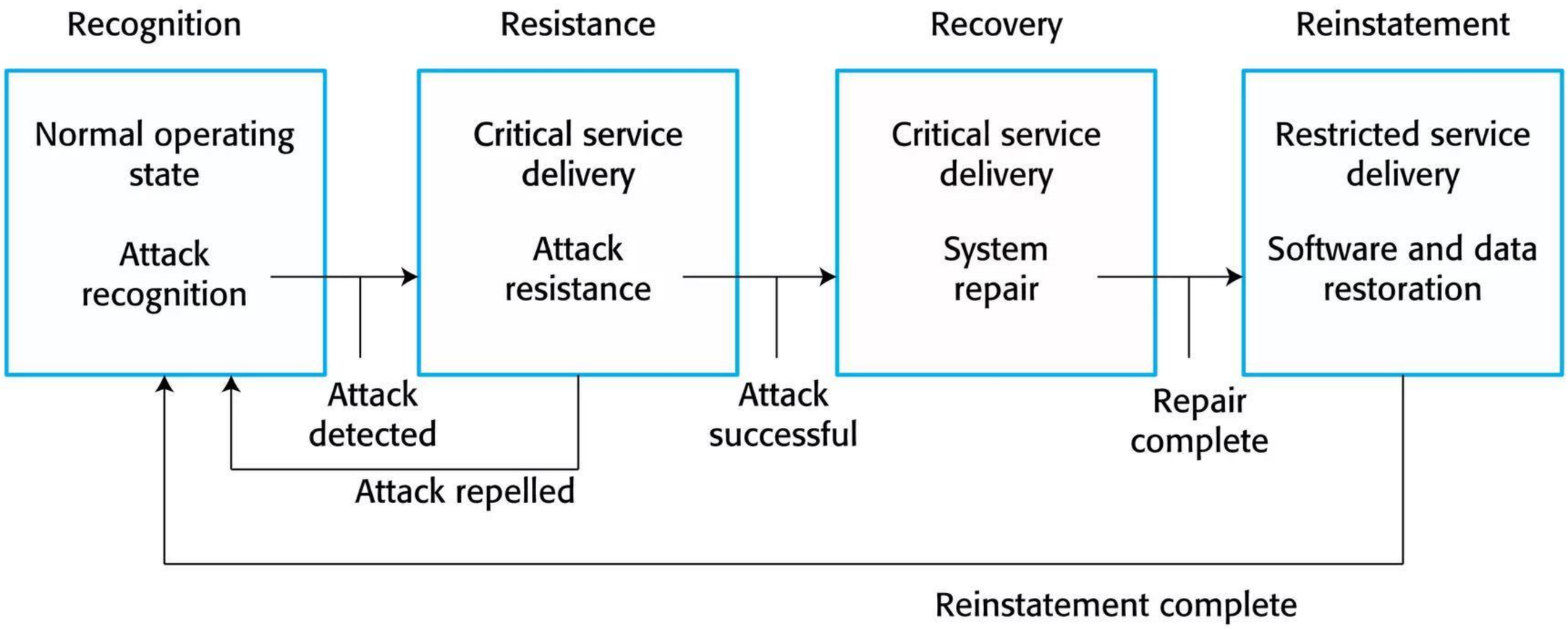
Resilience activities

- *Recognition* The system or its operators should recognise early indications of system failure.
- *Resistance* If the symptoms of a problem or cyberattack are detected early, then resistance strategies may be used to reduce the probability that the system will fail.
- *Recovery* If a failure occurs, the recovery activity ensures that critical system services are restored quickly so that system users are not badly affected by failure.
- *Reinstatement* In this final activity, all of the system services are restored and normal system operation can continue.

Resistance

- ✧ Resistance strategies may focus on isolating critical parts of the system so that they are unaffected by problems elsewhere.
- ✧ Resistance includes proactive resistance where defences are included in a system to trap problems and reactive resistance where actions are taken when a problem is discovered.

Resilience activities



Cybersecurity

Cybersecurity

- ✧ Cybercrime is the illegal use of networked systems and is one of the most serious problems facing our society.
- ✧ Cybersecurity is a broader topic than system security engineering
  - Cybersecurity is a sociotchnical issue covering all aspects of ensuring the protection of citizens, businesses and critical infrastructures from threats that arise from their use of computers and the Internet.
- ✧ Cybersecurity is concerned with all of an organization's IT assets from networks through to application systems.

Factors contributing to cybersecurity failure

- ✧ organizational ignorance of the seriousness of the problem,
- ✧ poor design and lax application of security procedures,
- ✧ human carelessness,
- ✧ inappropriate trade-offs between usability and security.

Cybersecurity threats

- *Threats to the confidentiality of assets* Data is not damaged but it is made available to people who should not have access to it.
- *Threats to the integrity of assets* These are threats where systems or data are damaged in some way by a cyberattack.
- *Threats to the availability of assets* These are threats that aim to deny use of assets by authorized users.

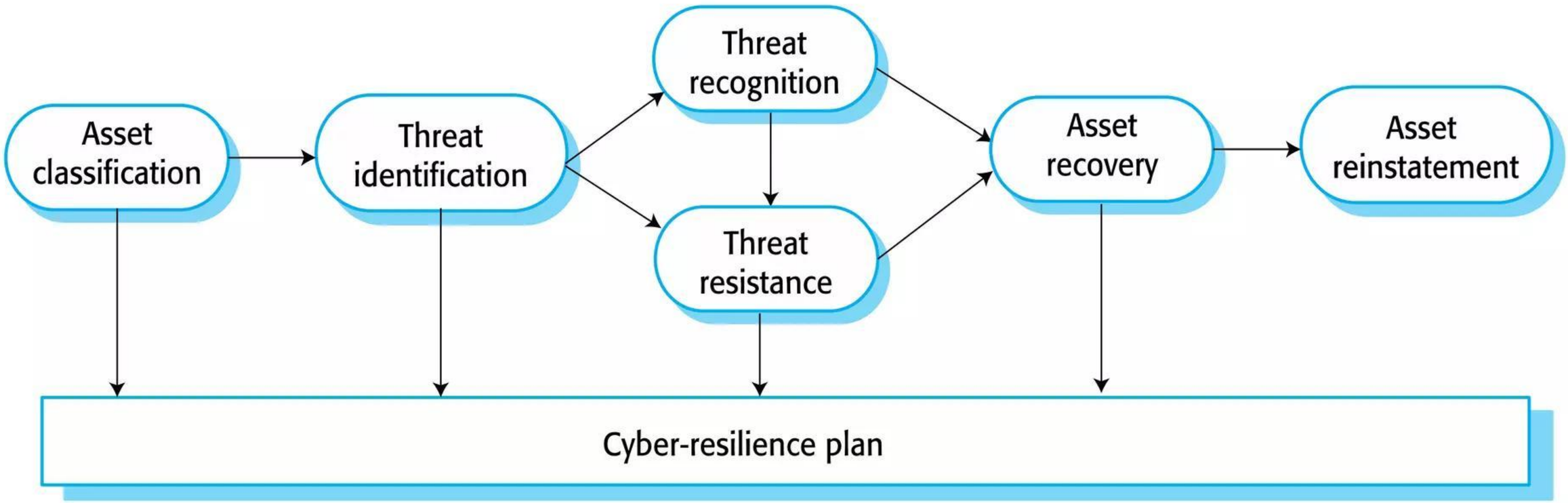
Examples of controls

- ✧ Authentication, where users of a system have to show that they are authorized to access the system
- ✧ Encryption, where data is algorithmically scrambled so that an unauthorized reader cannot access the information.
- ✧ Firewalls, where incoming network packets are examined then accepted or rejected according to a set of organizational rules.
  - Firewalls can be used to ensure that only traffic from trusted sources is passed from the external Internet into the local organizational network.

Redundancy and diversity

- ✧ Copies of data and software should be maintained on separate computer systems.
  - This supports recovery after a successful cyberattack. (recovery and reinstatement)
- ✧ Multi-stage diverse authentication can protect against password attacks.
  - This is a resistance measure
- ✧ Critical servers may be over-provisioned i.e. they may be more powerful than is required to handle their expected load. Attacks can be resisted without serious service degradation.

Cyber-resilience planning



Cyber resilience planning

- ✧ *Asset classification*
  - The organization's hardware, software and human assets are examined and classified depending on how essential they are to normal operations.
- ✧ *Threat identification*
  - For each of the assets (or, at least the critical and important assets), you should identify and classify threats to that asset.
- ✧ *Threat recognition*
  - For each threat or, sometimes asset/threat pair, you should identify how an attack based on that threat might be recognised.

Cyber resilience planning

✧ *Threat resistance*

- For each threat or asset/threat pair, you should identify possible resistance strategies. These may be either embedded in the system (technical strategies) or may rely on operational procedures.

✧ *Asset recovery*

- For each critical asset or asset/threat pair, you should work out how that asset could be recovered in the event of a successful cyberattack.

✧ *Asset reinstatement*

- This is a more general process of asset recovery where you define procedures to bring the system back into normal operation.

Sociotechnical resilience

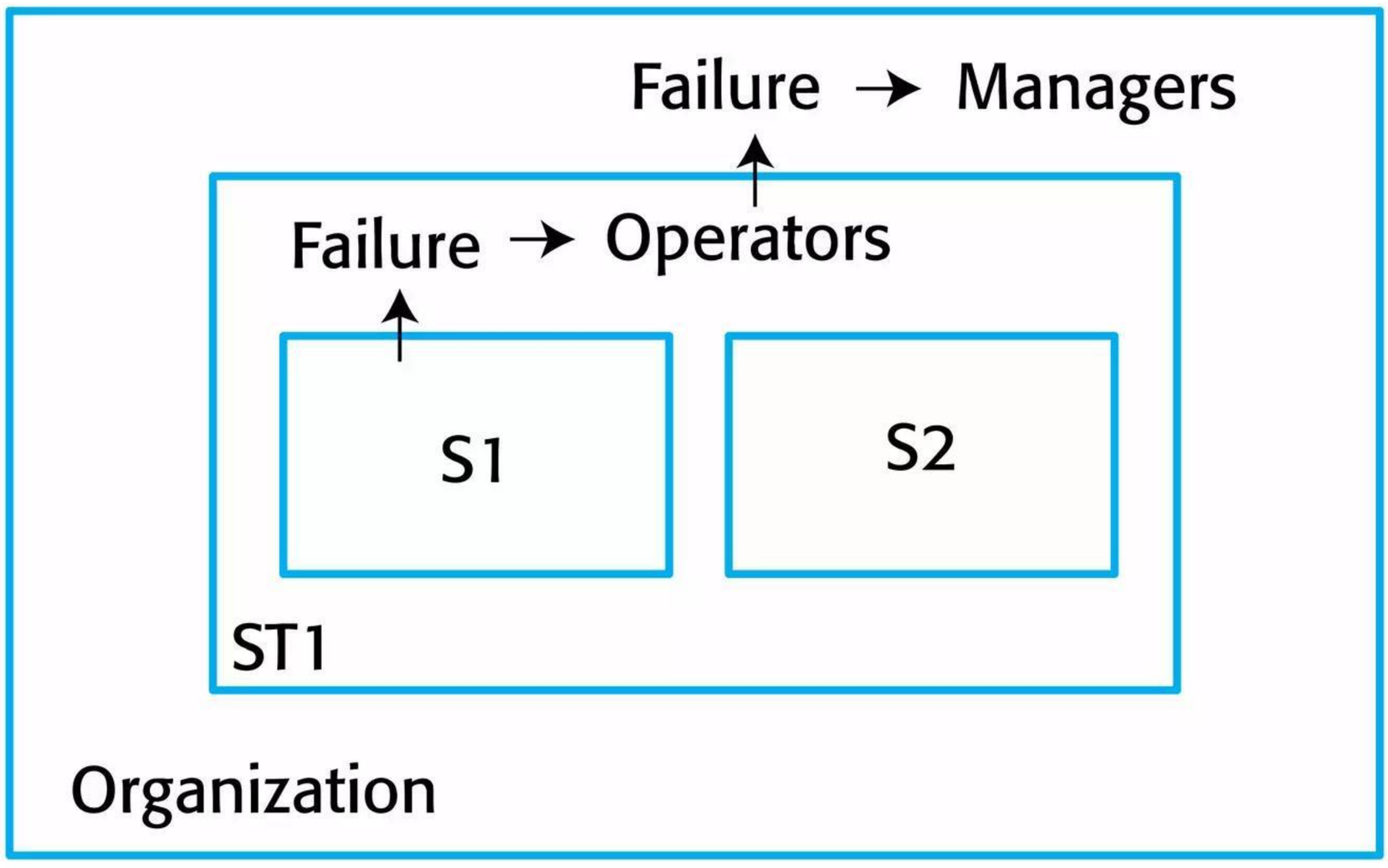
Sociotechnical resilience

- ✧ Resilience engineering is concerned with adverse external events that can lead to system failure.
- ✧ To design a resilient system, you have to think about sociotechnical systems design and not exclusively focus on software.
- ✧ Dealing with these events is often easier and more effective in the broader sociotechnical system.

Mentcare example

- ✧ Cyberattack may aim to steal data, gaining access using a legitimate user's credentials
- ✧ Technical solution may be to use more complex authentication procedures.
- ✧ These irritate users and may reduce security as users leave systems unattended without logging out.
- ✧ A better strategy may be to introduce organizational policies and procedures that emphasise the importance of not sharing login credentials and that tell users about easy ways to create and maintain strong passwords.

Nested technical and sociotechnical systems



Failure hierarchy

- ✧ A failure in system S1 may be trapped in the broader sociotechnical system ST1 through operator actions
- ✧ Organizational damage is therefore limited
- ✧ If the failure in S1 leads to a failure in ST1, then it is up to managers in the broader organization to deal with that failure.

Characteristics of resilient organizations

Organizational resilience

- There are four characteristics that reflect the resilience of an organization
  - Responsiveness, monitoring, anticipation, learning
- *The ability to respond*
  - Organizations have to be able to adapt their processes and procedures in response to risks. These risks may be anticipated risks or may be detected threats to the organization and its systems.
- *The ability to monitor*
  - Organizations should monitor both their internal operations and their external environment for threats before they arise.

Organizational resilience

- ✧ *The ability to anticipate*
  - A resilient organization should not simply focus on its current operations but should anticipate possible future events and changes that may affect its operations and resilience.
- ✧ *The ability to learn*
  - Organizational resilience can be improved by learning from experience. It is particularly important to learn from successful responses to adverse events such as the effective resistance of a cyberattack. Learning from success allows

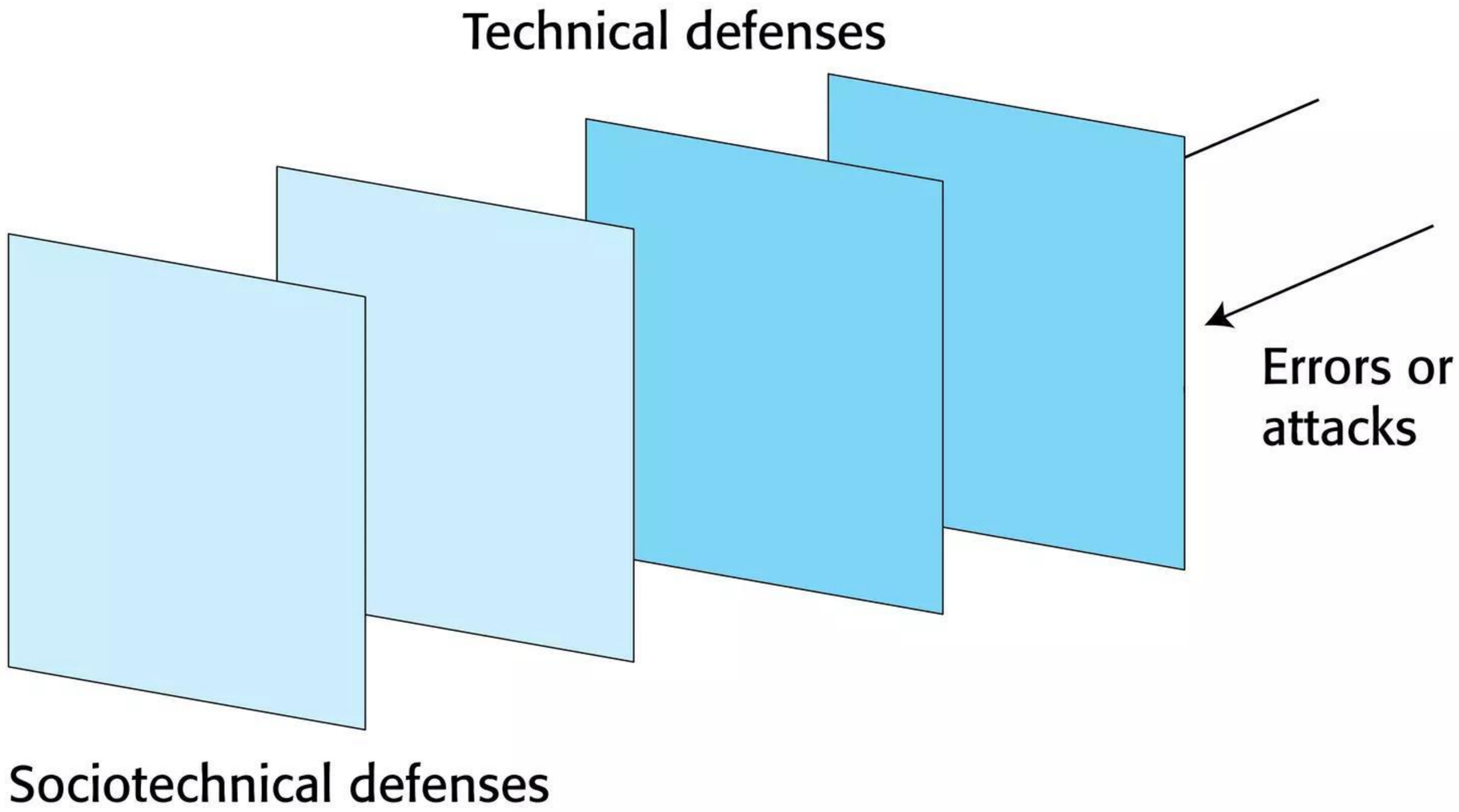
Human error

- ✧ People inevitably make mistakes (human errors) that sometimes lead to serious system failures.
- ✧ There are two ways to consider human error
  - *The person approach*. Errors are considered to be the responsibility of the individual and 'unsafe acts' (such as an operator failing to engage a safety barrier) are a consequence of individual carelessness or reckless behaviour.
  - *The systems approach*. The basic assumption is that people are fallible and will make mistakes. People make mistakes because they are under pressure from high workloads, poor training or because of inappropriate system design.

Systems approach

- ✧ Systems engineers should assume that human errors will occur during system operation.
- ✧ To improve the resilience of a system, designers have to think about the defences and barriers to human error that could be part of a system.
- ✧ Can these barriers should be built into the technical components of the system (technical barriers)? If not, they could be part of the processes, procedures and guidelines for using the system (sociotechnical barriers).

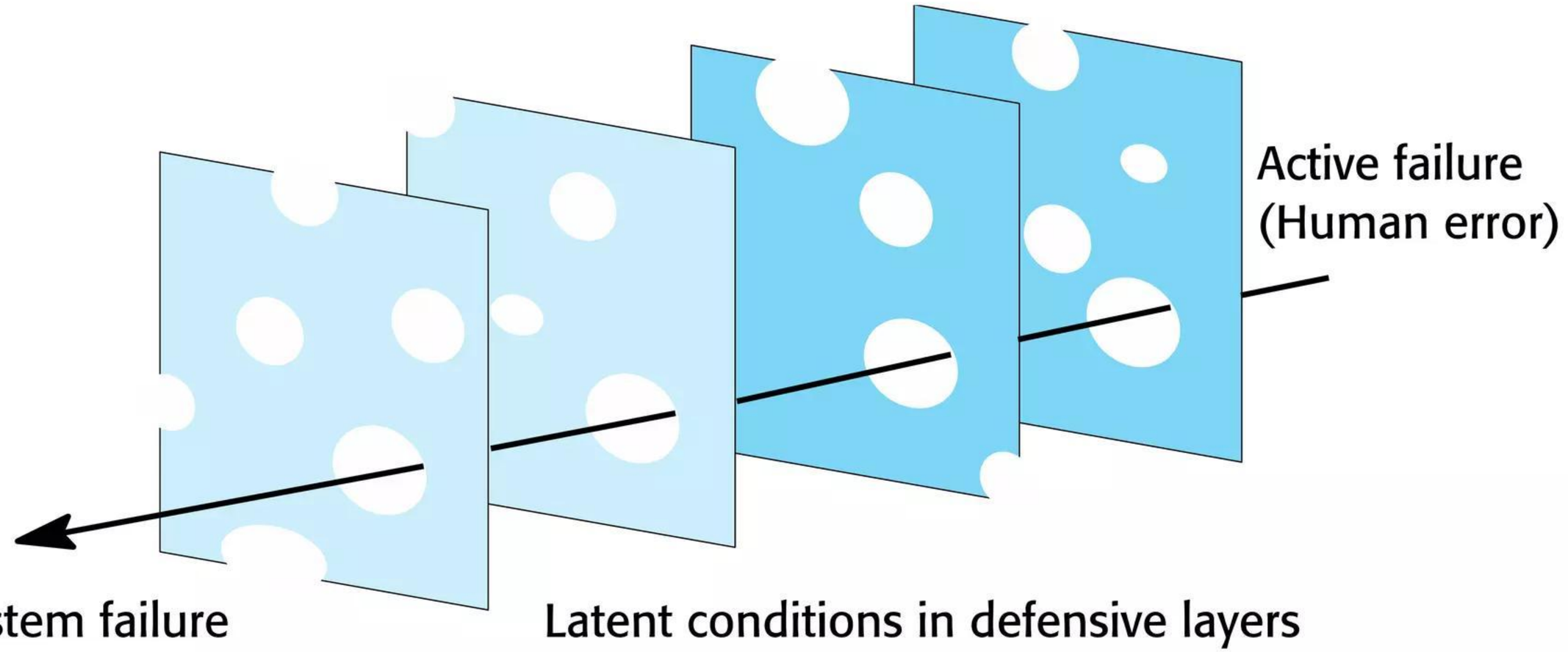
Defensive layers



Defensive layers

- ✧ You should use redundancy and diversity to create a set of defensive layers, where each layer uses a different approach to deter attackers or trap technical/human failures.
- ✧ ATC system examples
  - Conflict alert system
  - Formalized recording procedures
  - Collaborative checking

Reason's Swiss Cheese Model



Swiss Cheese model

- ✧ Defensive layers have vulnerabilities
  - They are like slices of Swiss cheese with holes in the layer corresponding to these vulnerabilities.
- ✧ Vulnerabilities are dynamic
  - The ‘holes’ are not always in the same place and the size of the holes may vary depending on the operating conditions.
- ✧ System failures occur when the holes line up and all of the defenses fail.

Increasing system resilience

- ✧ Reduce the probability of the occurrence of an external event that might trigger system failures.
- ✧ Increase the number of defensive layers.
  - The more layers that you have in a system, the less likely it is that the holes will line up and a system failure occur.
- ✧ Design a system so that diverse types of barriers are included.
  - The 'holes' will probably be in different places and so there is less chance of the holes lining up and failing to trap an error.
- ✧ Minimize the number of latent conditions in a system.
  - This means reducing the number and size of system 'holes'.

Operational and management processes

- ✧ All software systems have associated operational processes that reflect the assumptions of the designers about how these systems will be used.
- ✧ For example, in an imaging system in a hospital, the operator may have the responsibility of checking the quality of the images immediately after these have been processed.
- ✧ This allows the imaging procedure to be repeated if there is a problem.

Operational processes

- ✧ Operational processes are the processes that are involved in using the system for its defined purpose.
- ✧ For new systems, these operational processes have to be defined and documented during the system development process.
- ✧ Operators may have to be trained and other work processes adapted to make effective use of the new system.

Personal and Enterprise IT processes

- For personal systems, the designers may describe the expected use of the system but have no control over how users will actually behave.
- For enterprise IT systems, however, there may be training for users to teach them how to use the system.
- Although user behaviour cannot be controlled, it is reasonable to expect that they will normally follow the defined process.

Process design

- ✧ Operational and management processes are an important defense mechanism and, in designing a process, you need to find a balance between efficient operation and problem management.
- ✧ Process improvement focuses on identifying and codifying good practice and developing software to support this.
- ✧ If process improvement focuses on efficiency, then this can make it more difficult to deal with problems when these arise.

Efficiency and resilience

Efficient process operation	Problem management
Process optimization and control	Process flexibility and adaptability
Information hiding and security	Information sharing and visibility
Automation to reduce operator workload with fewer operators and managers	Manual processes and spare operator/manager capacity to deal with problems
Role specialization	Role sharing

Coping with failures

- What seems to be ‘inefficient’ practice often arises because people maintain redundant information or share information because they know this makes it easier to deal with problems when things go wrong.
- When things go wrong, operators and system managers can often recover the situation although this may sometimes mean that they have to break rules and ‘work around’ the defined process.
- You should therefore design operational processes to be flexible and adaptable.

Information provision and management

- To make a process more efficient, it may make sense to present operators with the information that they need, when they need it.
- If operators are only presented with information that the process designer thinks that they 'need to know' then they may be unable to detect problems that do not directly affect their immediate tasks.
- When things go wrong, the system operators do not have a broad picture of what is happening in the system, so it is more difficult for them to formulate strategies for dealing with problems.

Process automation

- ✧ Process automation can have both positive and negative effects on system resilience.
- ✧ If the automated system works properly, it can detect problems, invoke cyberattack resistance if necessary and start automated recovery procedures.
- ✧ However, if the problem can’t be handled by the automated system, there are fewer people available to tackle the problem and the system may have been damaged by the process automation doing the wrong thing.

Disadvantages of process automation

- ✧ Automated management systems may go wrong and take incorrect actions. As problems develop, the system may take unexpected actions that make the situation worse and which cannot be understood by the system managers.
- ✧ Problem solving is a collaborative process. If fewer managers are available, it is likely to take longer to work out a strategy to recover from a problem or cyberattack.

Resilient systems design

Resilient systems design

- ✧ *Identifying critical services and assets*
  - Critical services and assets are those elements of the system that allow a system to fulfill its primary purpose.
  - For example, the critical services in a system that handles ambulance dispatch are those concerned with taking calls and dispatching ambulances.
- ✧ *Designing system components that support problem recognition, resistance, recovery and reinstatement*
  - For example, in an ambulance dispatch system, a watchdog timer may be included to detect if the system is not responding to events.

Survivable systems analysis

✧ *System understanding*

- For an existing or proposed system, review the goals of the system (sometimes called the mission objectives), the system requirements and the system architecture.

✧ *Critical service identification*

- The services that must always be maintained and the components that are required to maintain these services are identified.

Survivable systems analysis

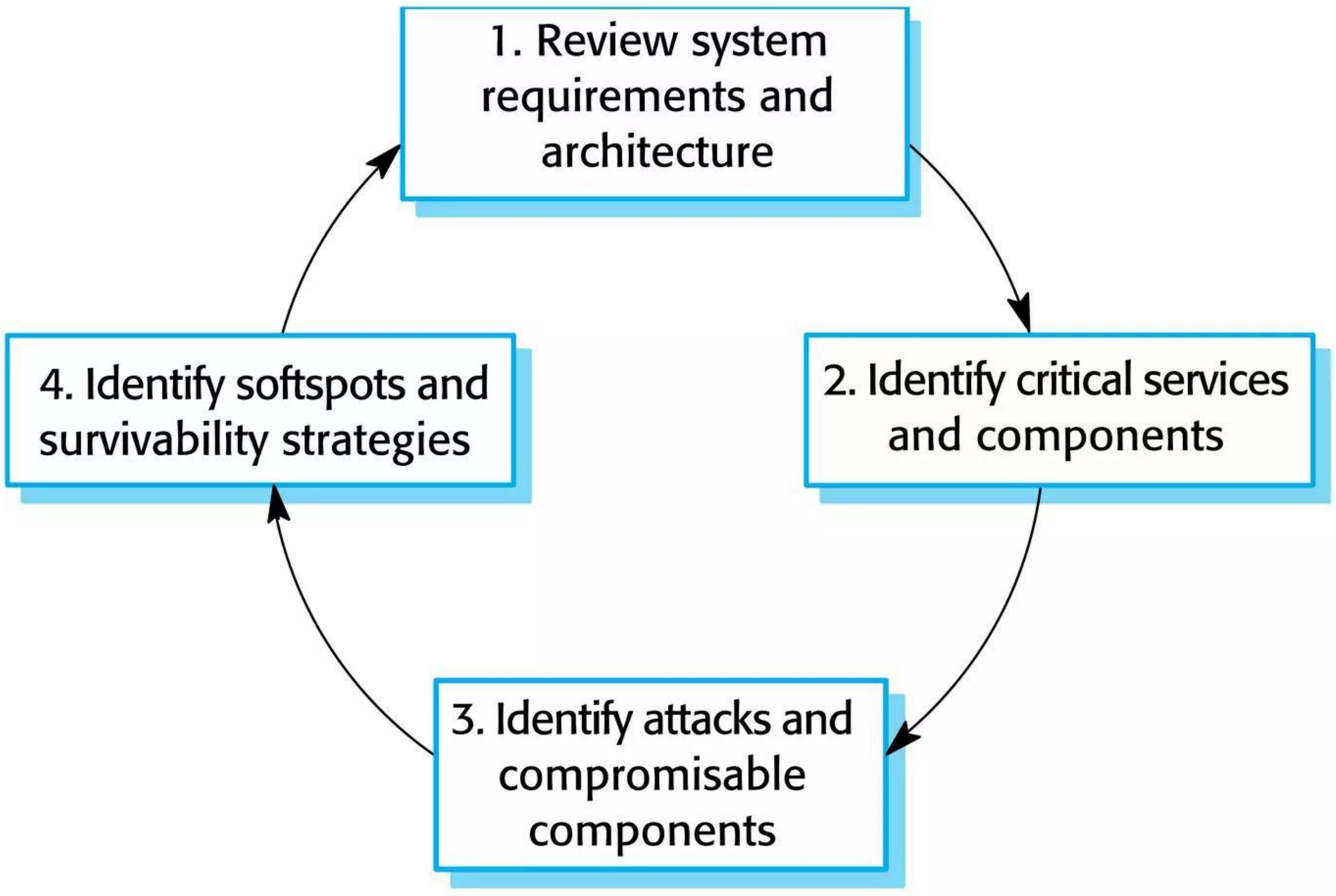
✧ *Attack simulation*

- Scenarios or use cases for possible attacks are identified along with the system components that would be affected by these attacks.

✧ *Survivability analysis*

- Components that are both essential and compromisable by an attack are identified and survivability strategies based on resistance, recognition and recovery are identified.

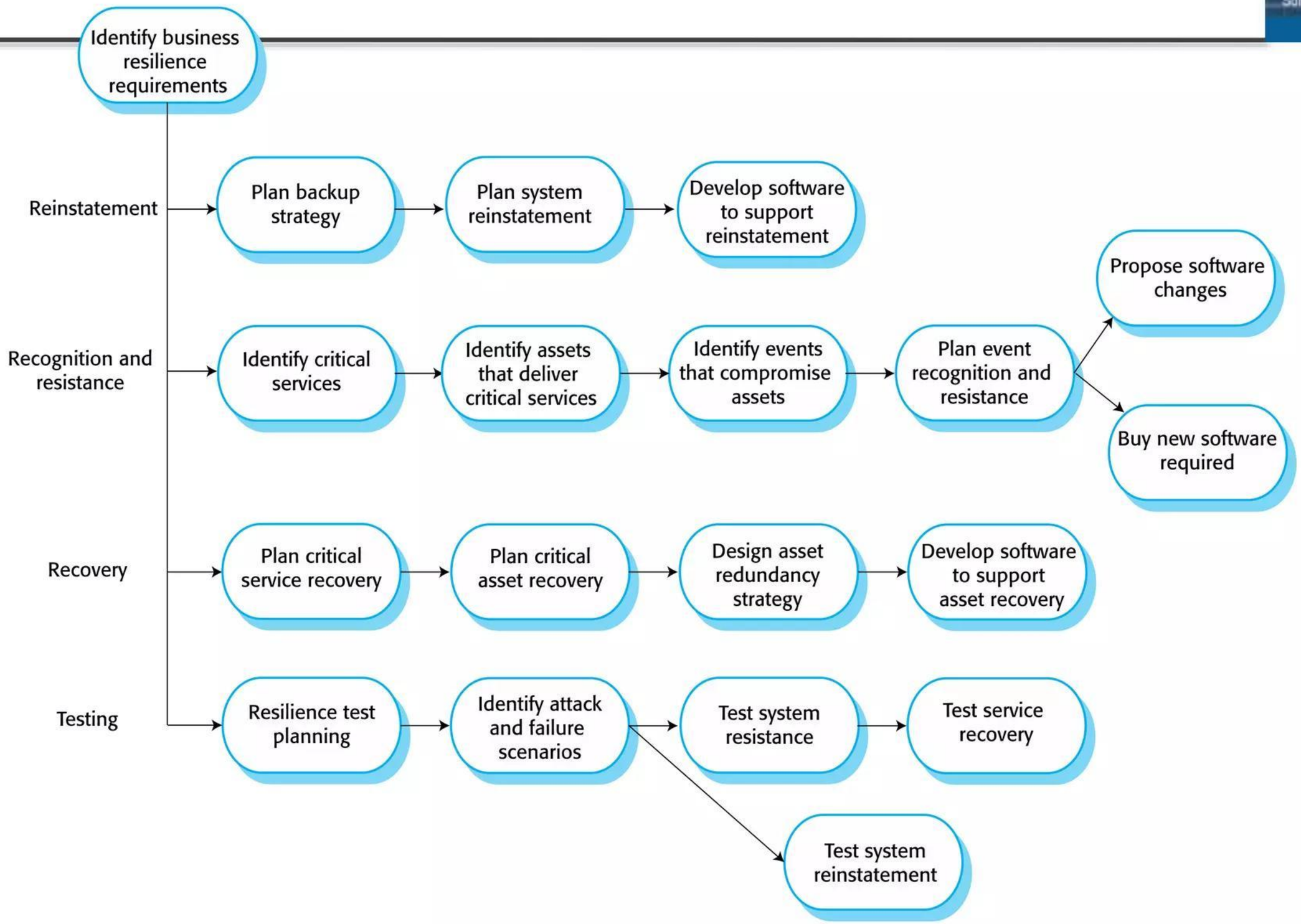
Stages in survivability analysis



Problems for business systems

- The fundamental problem with this approach to survivability analysis is that its starting point is the requirements and architecture documentation for a system.
- However for business systems:
  - It is not explicitly related to the business requirements for resilience. I believe that these are a more appropriate starting point than technical system requirements.
  - It assumes that there is a detailed requirements statement for a system. In fact, resilience may have to be ‘retrofitted’ to a system where there is no complete or up-to-date requirements document.

Resilience engineering



Streams of work in resilience engineering

- ✧ Identify business resilience requirements
- ✧ Plan how to reinstate systems to their normal operating state
- ✧ Identify system failures and cyberattacks that can compromise a system
- ✧ Plan how to recover critical services quickly after damage or a cyberattack
- ✧ Test all aspects of resilience planning

Maintaining critical service availability

✧ To maintain availability, you need to know:

- the system services that are the most critical for a business,
- the minimal quality of service that must be maintained,
- how these services might be compromised,
- how these services can be protected,
- how you can recover quickly if the services become unavailable.

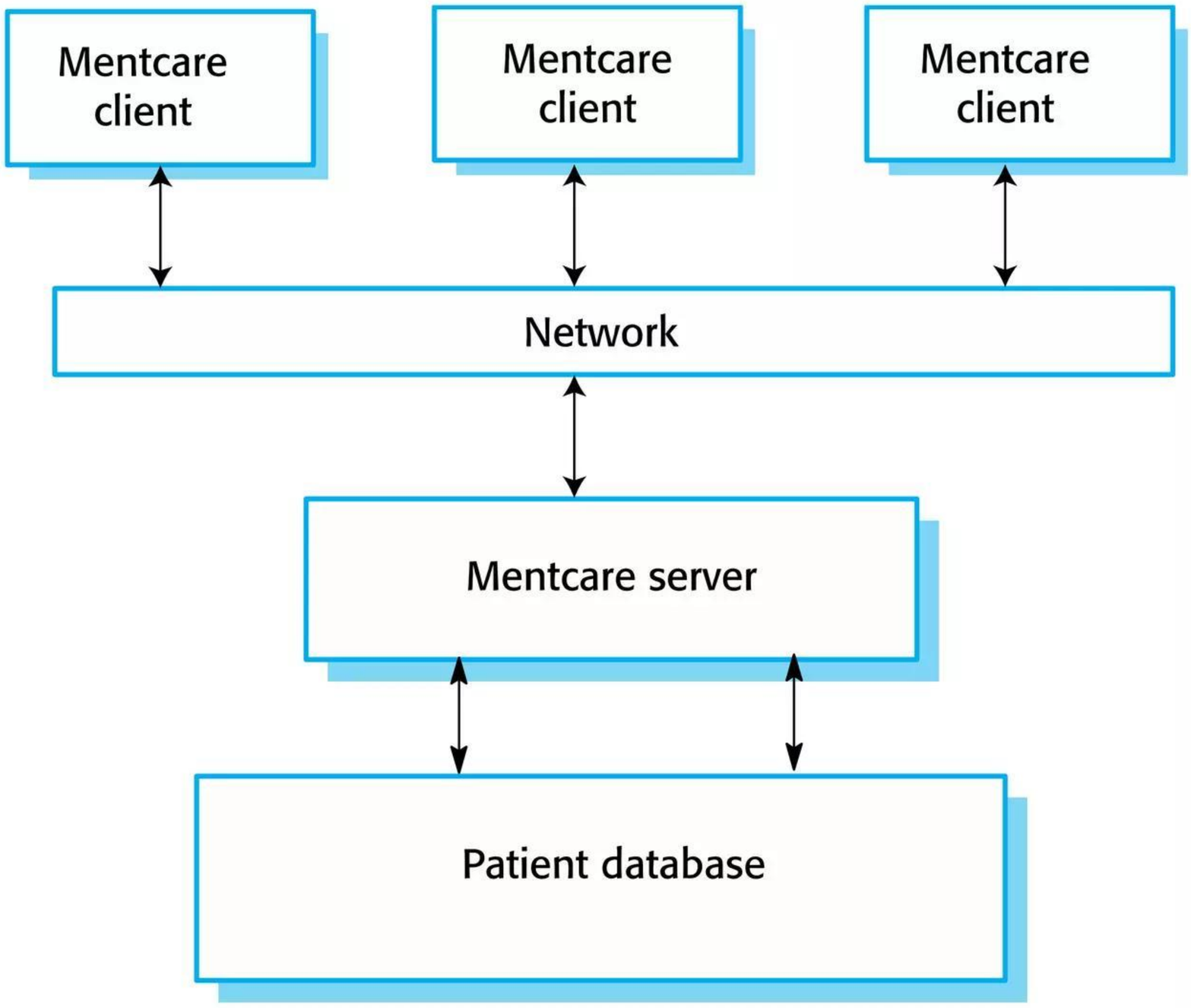
✧ Critical assets are identified during service analysis.

- Assets may be hardware, software, data or people.

Mentcare system resilience

- The Mentcare system is a system used to support clinicians treating patients that suffer from mental health problems.
- It provides patient information and records of consultations with doctors and nurses.
- It includes checks that can flag patients who may be dangerous or suicidal.
- Based on a client-server architecture.

Client-server architecture (Mentcare)



Critical Mentcare services

- ✧ An information service that provides information about a patient's current diagnosis and treatment plan.
- ✧ A warning service that highlights patients that could pose a danger to others or to themselves.
- ✧ Availability of the complete patient record is NOT a critical service as routine patient information is not normally required during consultations.

Assets required for normal service operation

- ✧ The patient record database that maintains all patient information.
- ✧ A database server that provides access to the database for local client computers.
- ✧ A network for client/server communication.
- ✧ Local laptop or desktop computers used by clinicians to access patient information.
- ✧ A set of rules to identify patients who are potentially dangerous and which can flag patient records. Client software that highlights dangerous patients to system users.

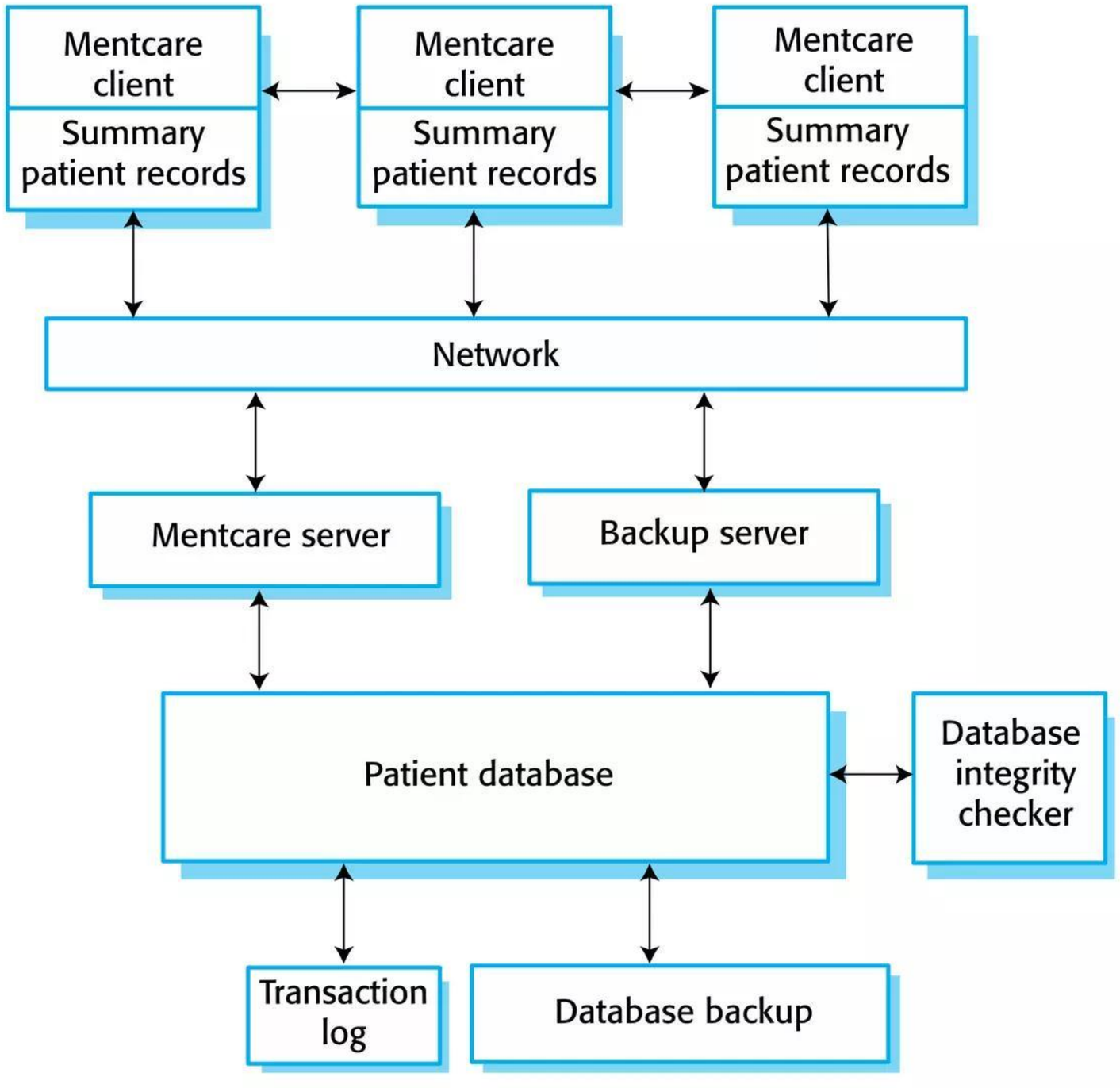
Adverse events

- ✧ Unavailability of the database server either through a system failure, a network failure or a denial of service cyberattack
- ✧ Deliberate or accidental corruption of the patient record database or the rules that define what is meant by a ‘dangerous patient’
- ✧ Infection of client computers with malware
- ✧ Access to client computers by unauthorized people who gain access to patient records

Recognition and resistance strategies

Event	Recognition	Resistance
Server unavailability	1. Watchdog timer on client that times out if no response to client access 2. Text messages from system managers to clinical users	1. Design system architecture to maintain local copies of critical information 2. Provide peer-to-peer search across clients for patient data 3. Provide staff with smart phones that can be used to access the network in the event of server failure 4. Provide backup server
Patient database corruption	1. Record level cryptographic checksums 2. Regular auto-checking of database integrity 3. Reporting system for incorrect information	1. Replayable transaction log to update database backup with recent transactions 2. Maintenance of local copies of patient information and software to restore database from local copies and backups
Malware infection of client computers	1. Reporting system so that computer users can report unusual behaviour. 2. Automated malware checks on startup.	1. Security awareness workshops for all system users 2. Disabling of USB ports on client computers 3. Automated system setup for new clients 4. Support access to system from mobile devices 5. Installation of security software
Unauthorized access to patient information	1. Warning text messages from users about possible intruders 2. Log analysis for unusual activity	1. Multi-level system authentication process 2. Disabling of USB ports on client computers 3. Access logging and real-time log analysis 4. Security awareness workshops for all system users

Mentcare system resilience



Architecture for resilience

- ✧ Summary patient records that are maintained on local client computers.
  - The local computers can communicate directly with each other and exchange information using either the system network or using an *ad hoc* network created using mobile phones. If the database is unavailable, doctors and nurses can still access essential patient information.
- ✧ A backup server to allow for main server failure.
  - This server is responsible for taking regular snapshots of the database as backups. In the event of the failure of the main server, it can also act as the main server for the whole system.

Architecture for resilience

✧ Database integrity checking and recovery software.

- Integrity checking runs as a background task checking for signs of database corruption. If corruption is discovered, it can automatically initiate the recovery of some or all of the data from backups. The transaction log allows these backups to be updated with details of recent changes

Critical service maintenance

- By downloading information to the client at the start of a clinic session, the consultation can continue without server access.
  - Only the information about the patients who are scheduled to attend consultations that day needs to be downloaded.
- The service that provides a warning to staff of patients that may be dangerous can be implemented using this approach.
  - The records of possibly patients who may harm themselves or others are identified before the download process. When clinical staff access these records, the software can highlight them to indicate that this is a patient that requires special care.

Risks to confidentiality

- To minimize risks to confidentiality that arise from multiple copies of information on laptops:
  - Only download the summary records of patients who are scheduled to attend a clinic. This limits the numbers of records that could be compromised.
  - Encrypt the disk on local client computers. An attacker who does not have the encryption key cannot read the disk if they gain access to the computer.
  - Securely delete the downloaded information at the end of a clinic session. This further reduces the chances of an attacker gaining access to confidential information.
  - Ensure that all network transactions are encrypted. If an attacker intercepts these transactions, they cannot get access to the information.

Key points

- ✧ Resilience is a judgment of how well a system can maintain the continuity of its critical services in the presence of disruptive events.
- ✧ Resilience should be based on the 4 R's model – recognition, resistance, recovery and reinstatement.
- ✧ Resilience planning should be based on the assumption of cyberattacks by malicious insiders and outsiders and that some of these attacks will be successful.
- ✧ Systems should be designed with defensive layers of different types. These layers trap human and technical failures and help resist cyberattacks.

Key points

- ✧ To allow system operators and managers to cope with problems, processes should be flexible and adaptable. Process automation can make it more difficult for people to cope with problems.
- ✧ Business resilience requirements should be the starting point for designing systems for resilience. To achieve system resilience, you have to focus on recognition and recovery from problems, recovery of critical services and assets and reinstatement of the system.
- ✧ An important part of design for resilience is identifying critical services. Systems should be designed so that these services are protected and, in the event of failure, recovered as quickly as possible.