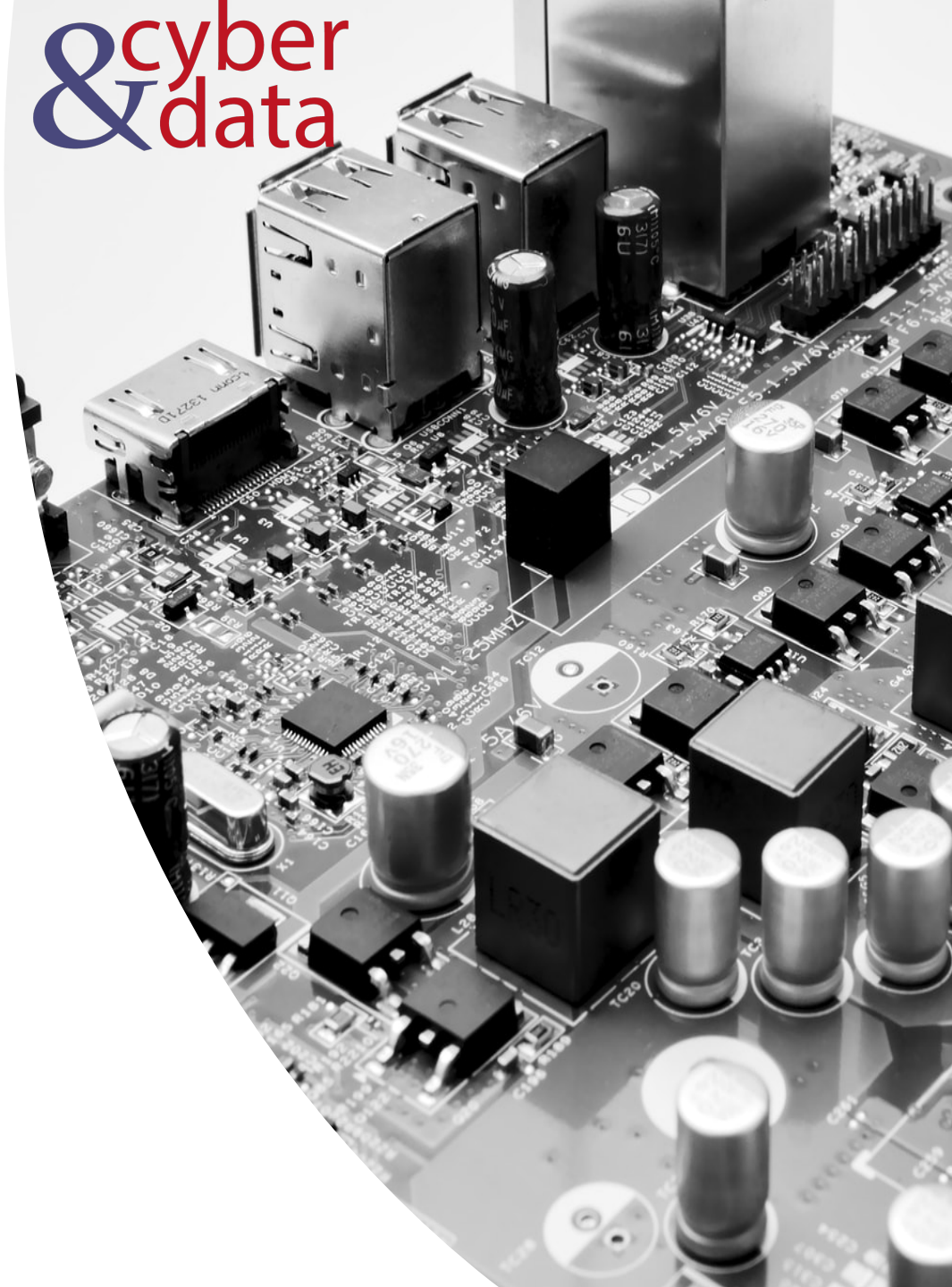
cyber & data

"From bits to information"

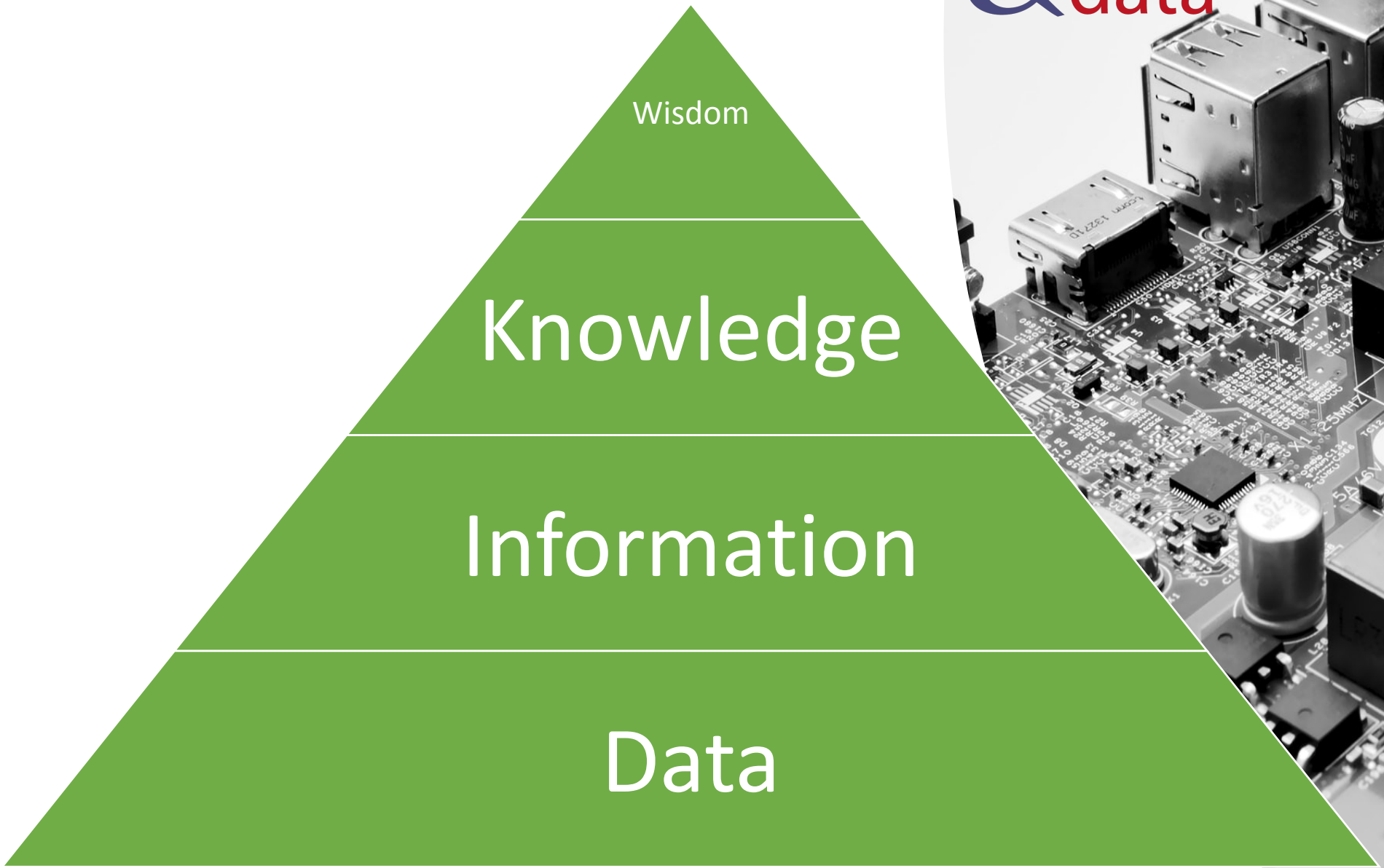
Defence Systems, Policies and Risks

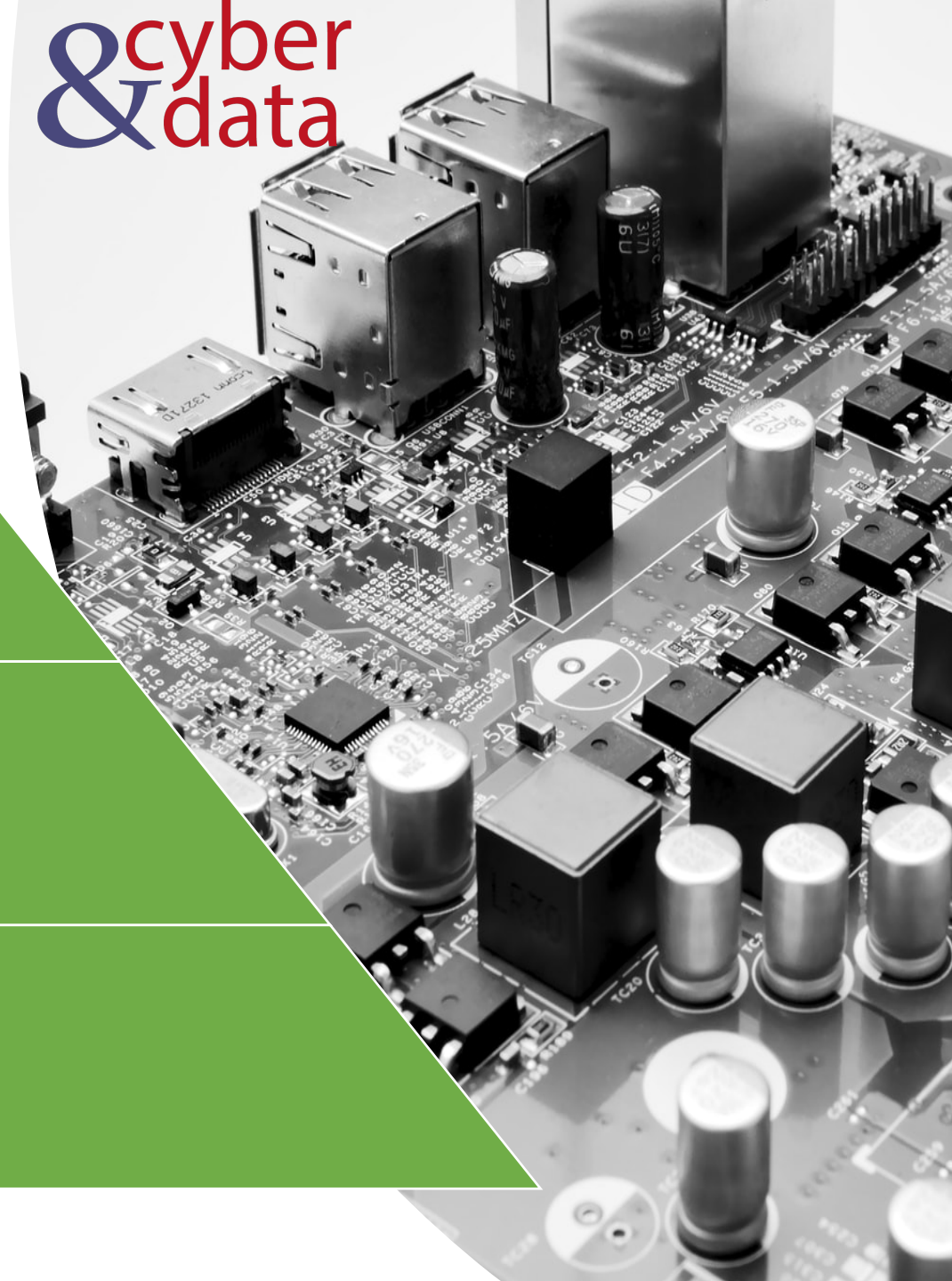
Outline

- Data, Information, Knowledge and Wisdom.
- Information Security and Forensic Computing.
- Impact and Harm.
- Risks, Costs and Benefits.
- Kill Chain Models.
- Defence Mechanisms.
- Defence-in-Depth.



Data to Wisdom

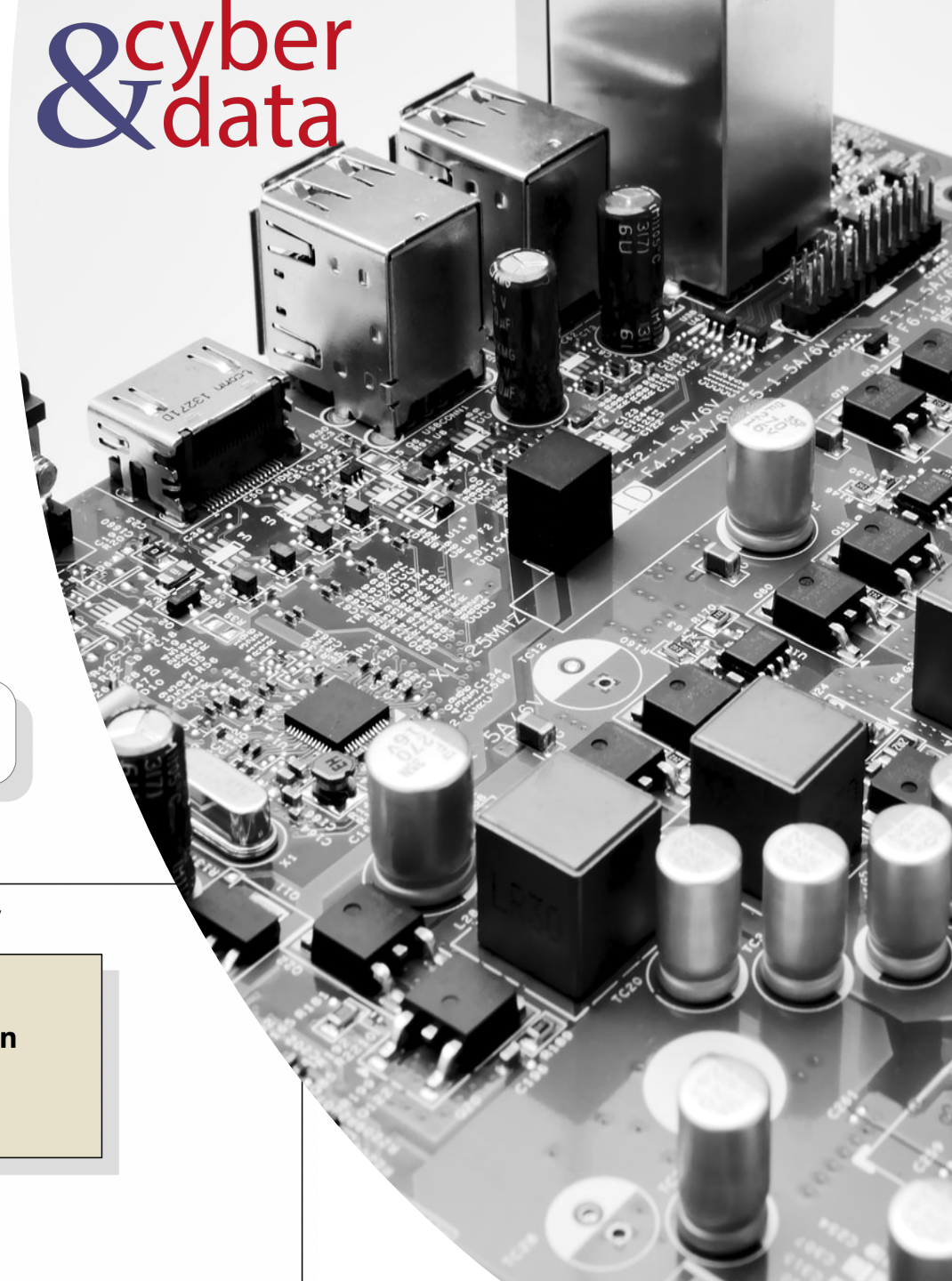


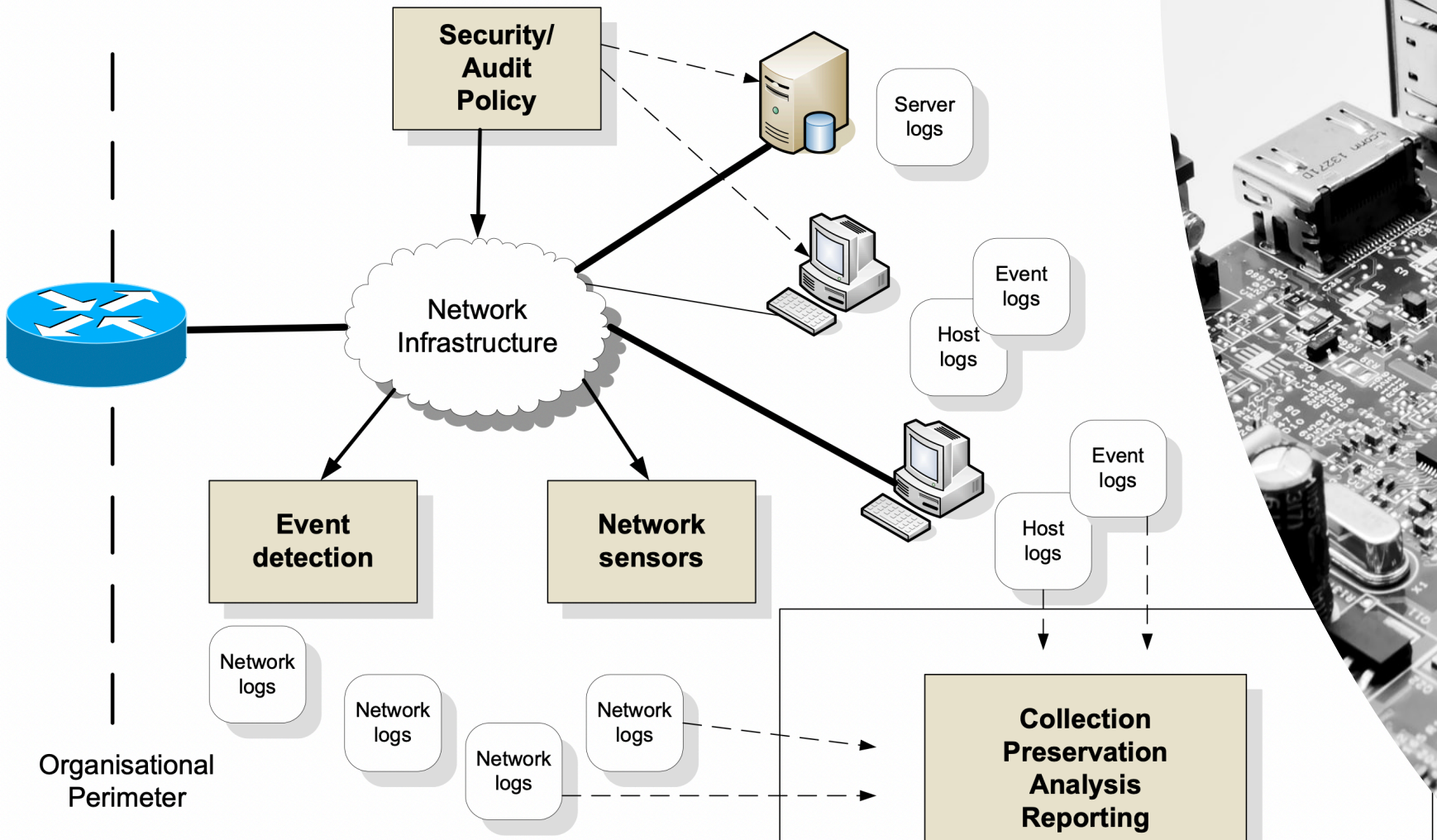


"From bits to information"

Security, Incident Response and Forensic Computing

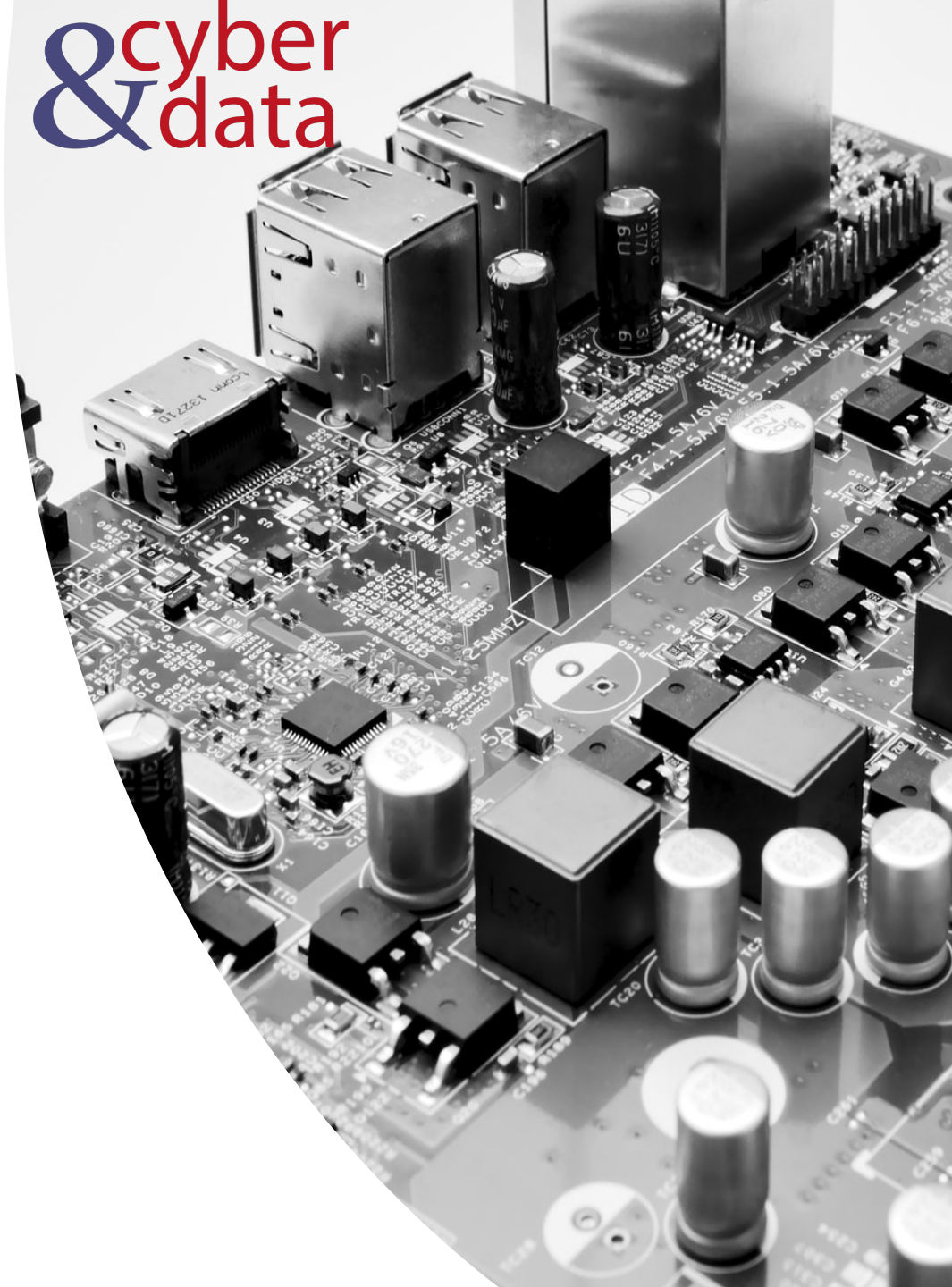
Information Security





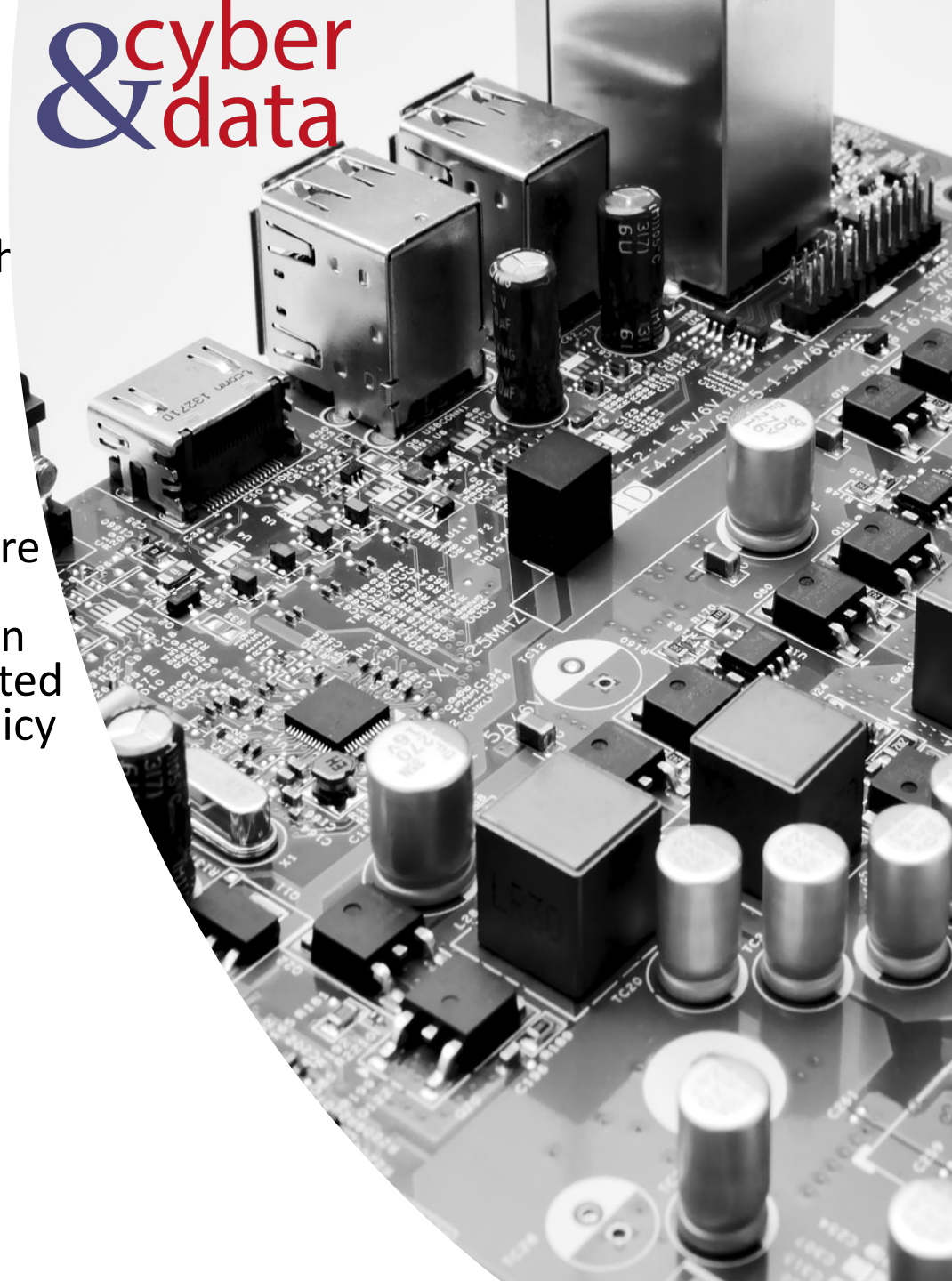
Investigation

- Investigating an intrusion on a system (incident response). This might lead to a criminal prosecution, but most of the time the intrusion is investigated in order to be able to detect it in the future, and to thwart the activities at an early stage.
- Investigation of a criminal activity (forensic computing). This might lead to a criminal prosecution, or to thwart the activities in the future.
- Investigation of a breach of security policy. This might lead to a disciplinary procedure within an organisation.



Due Care and Due Diligence

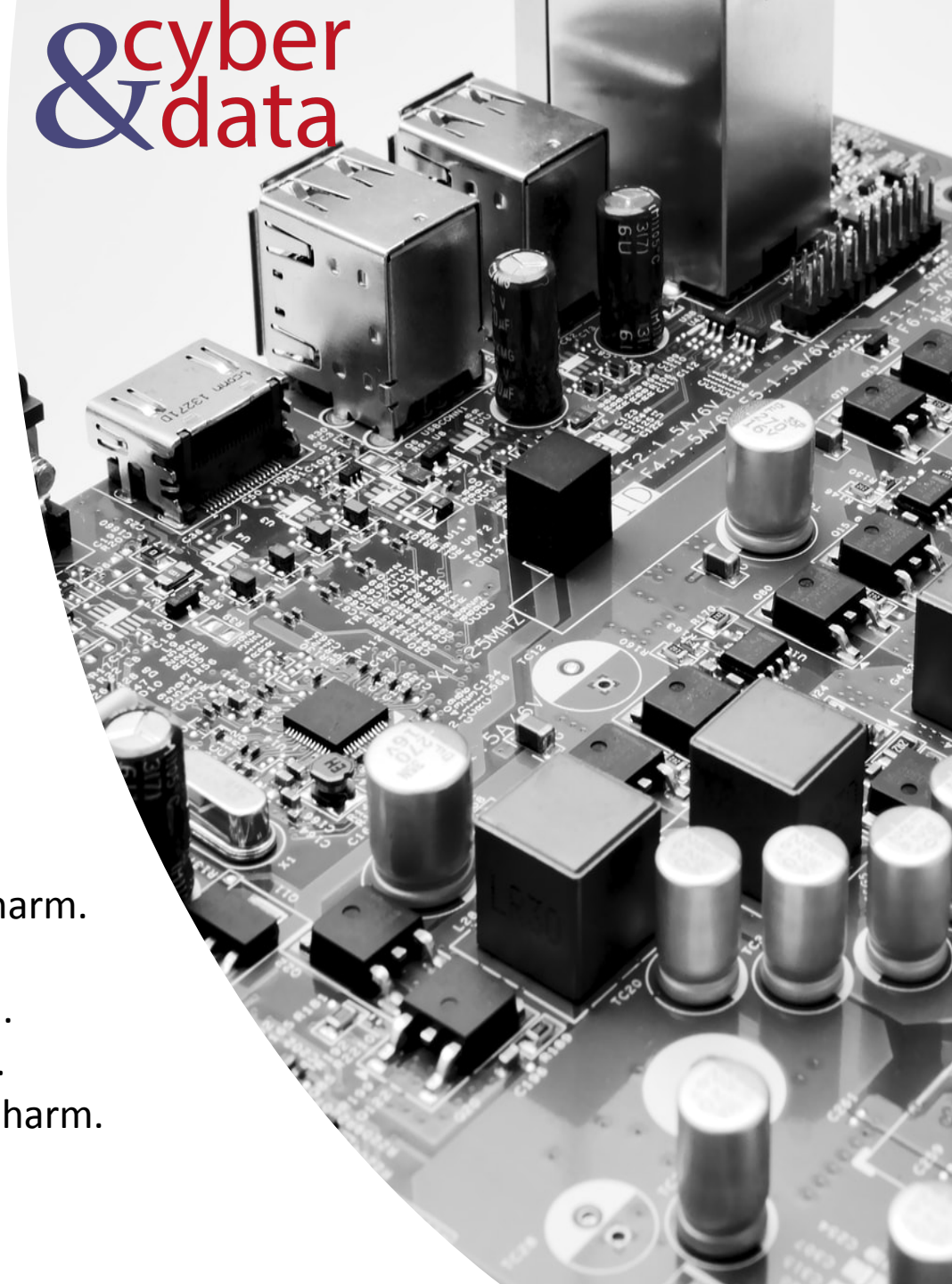
- With due care, the organisation must make sure that it h taken the correct steps in the creation and implementation of its security policy and in its risk analysis.
- Then due diligence relates to the actual operation and maintenance of its security system, especially around vulnerability testing. Thus a company might take due care in analysing and designing their security policy, but not take due diligence in actually proving that it works. It can work the other way, in that a policy might be implemented with due diligence, but the originally creation of the policy has not been properly analysed/designed. It is thus important, in terms of any future liability, that security systems are designed, analysed, implemented and maintained with both due care and due diligence.



"From bits to information"

Impact and Harm

Impact and Harm



Physical or Digital harm.
Economic harm.
Psychological harm.
Reputational harm.
Social and Societal harm.

cyber & data

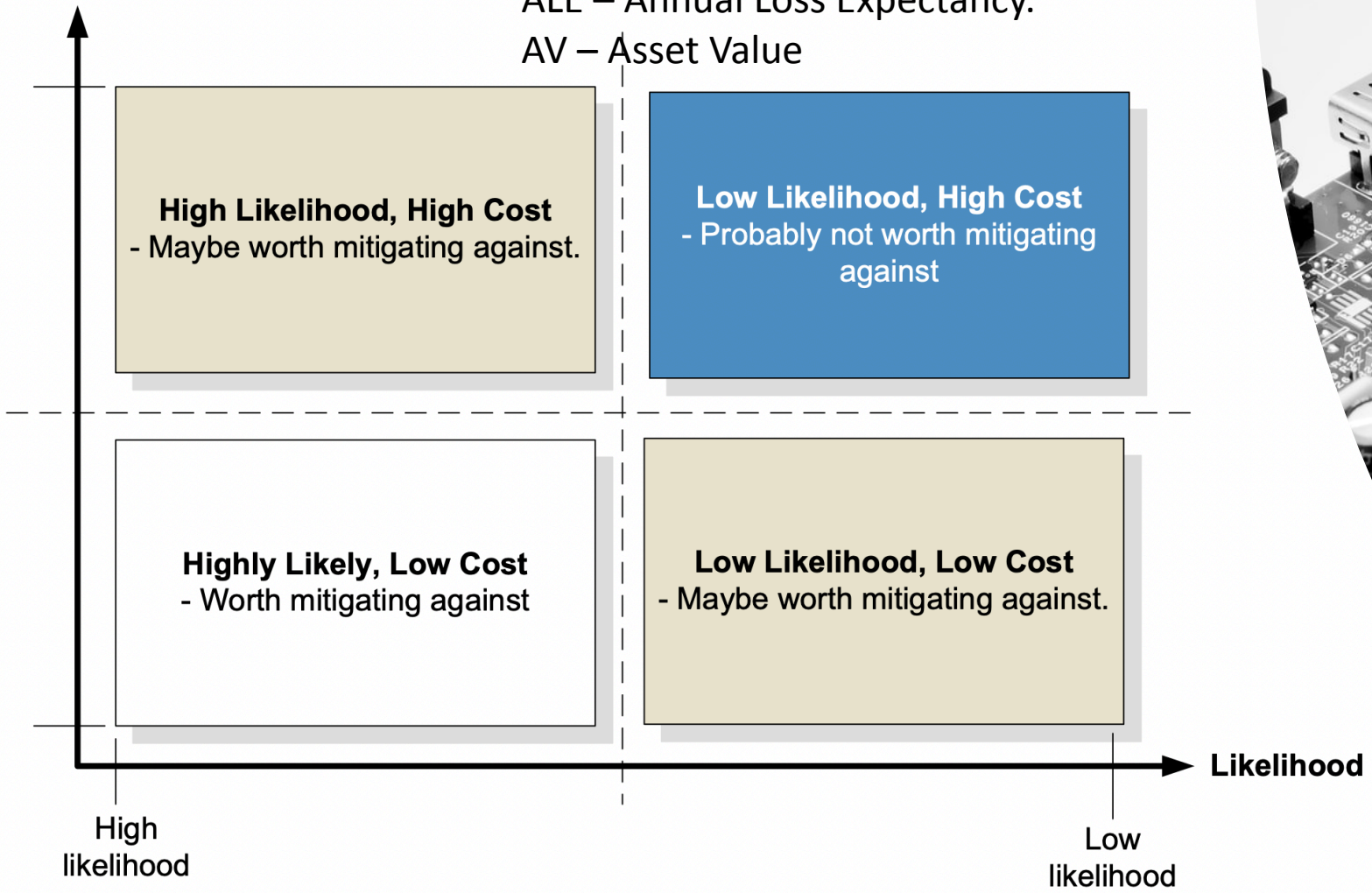
"From bits to information"

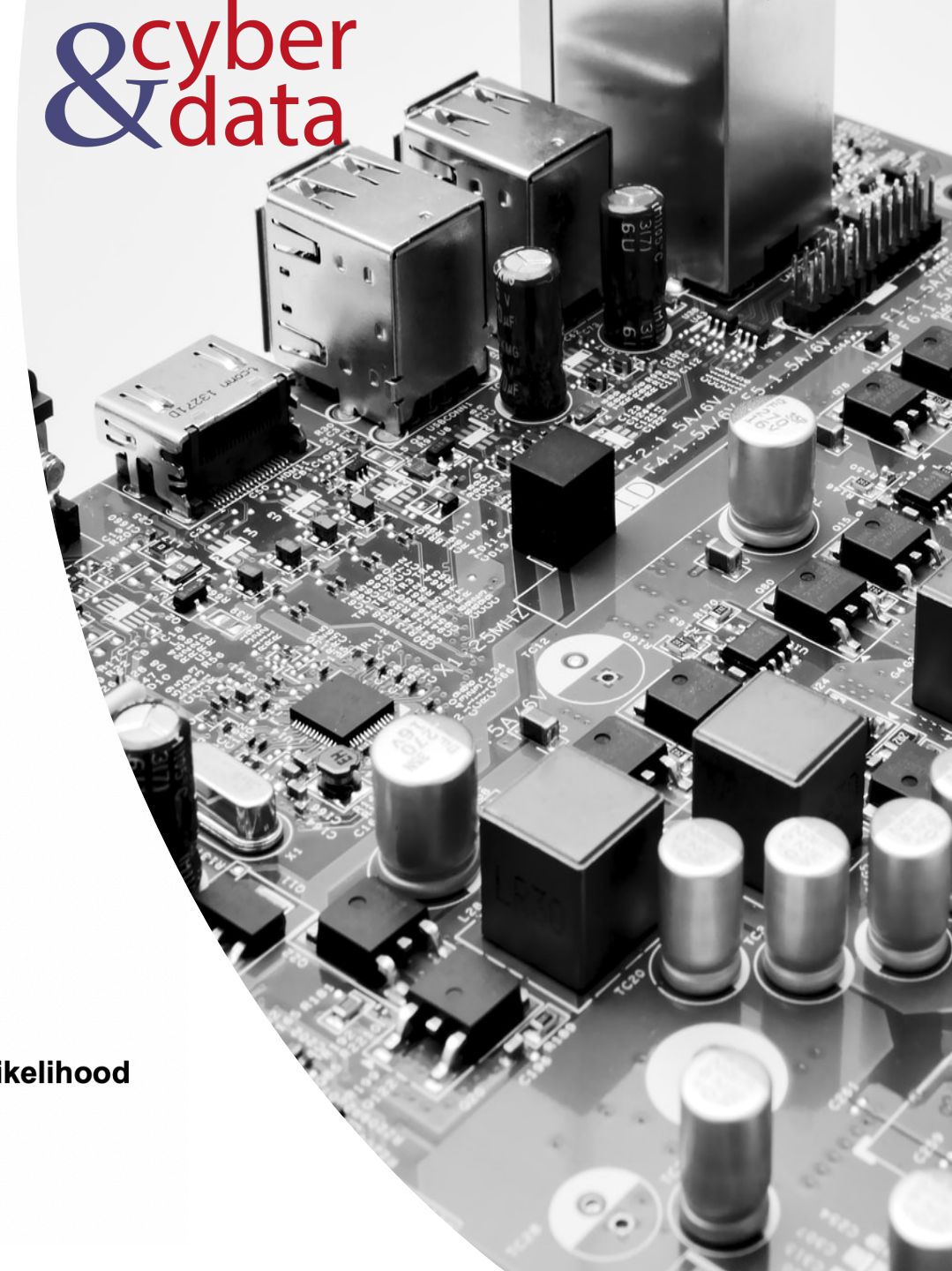
Risks, Costs and Benefits

Risks, Costs and Benefits

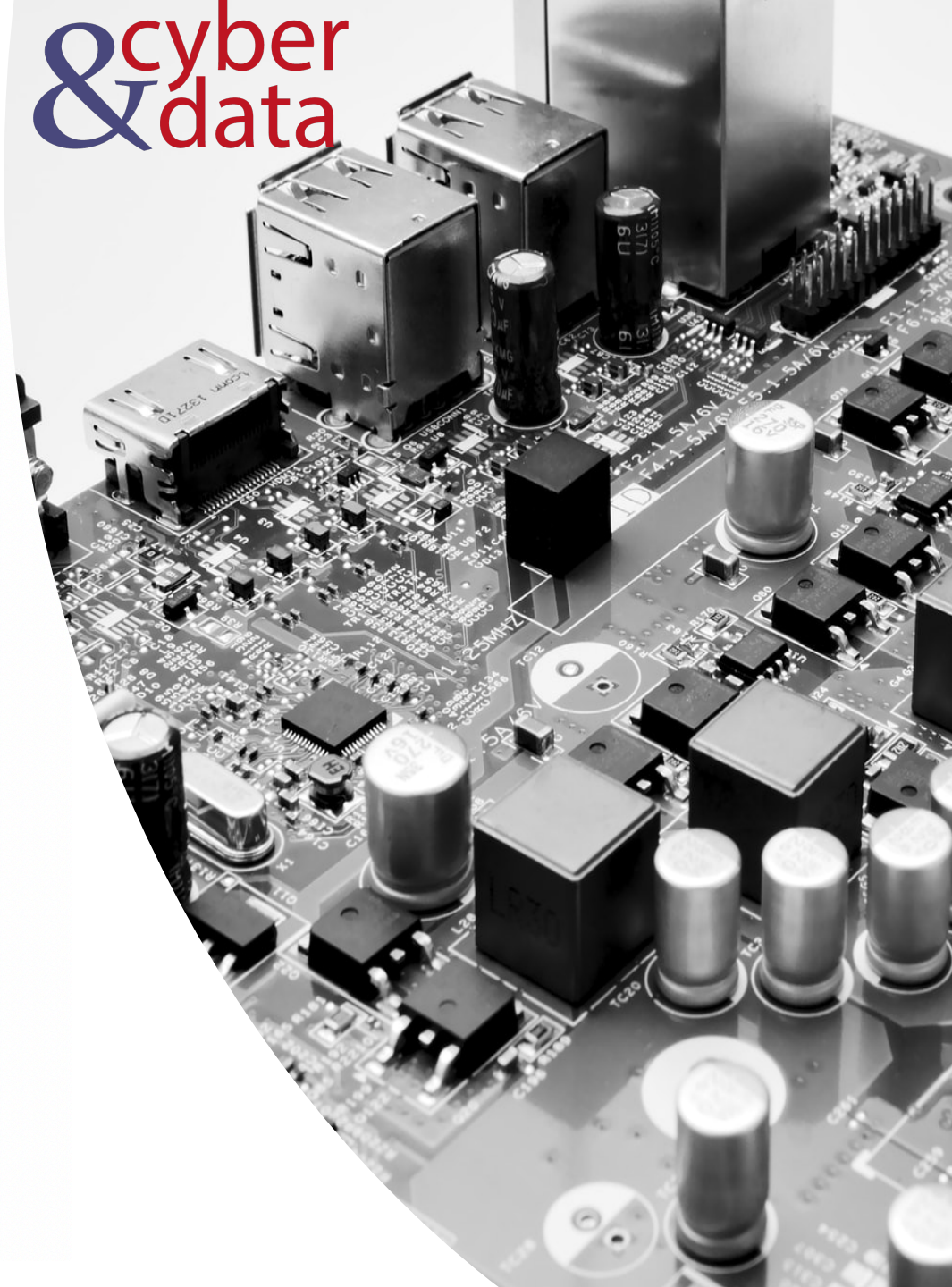
ALE = AV x ARO

ALE – Annual Loss Expectancy.
AV – Asset Value





Risks, Costs and Benefits



Error Operating (10-200)
Input (10-50,000) Programming (1-200)

Static discharge
General 300-3000)

Hardware
General (10-200)

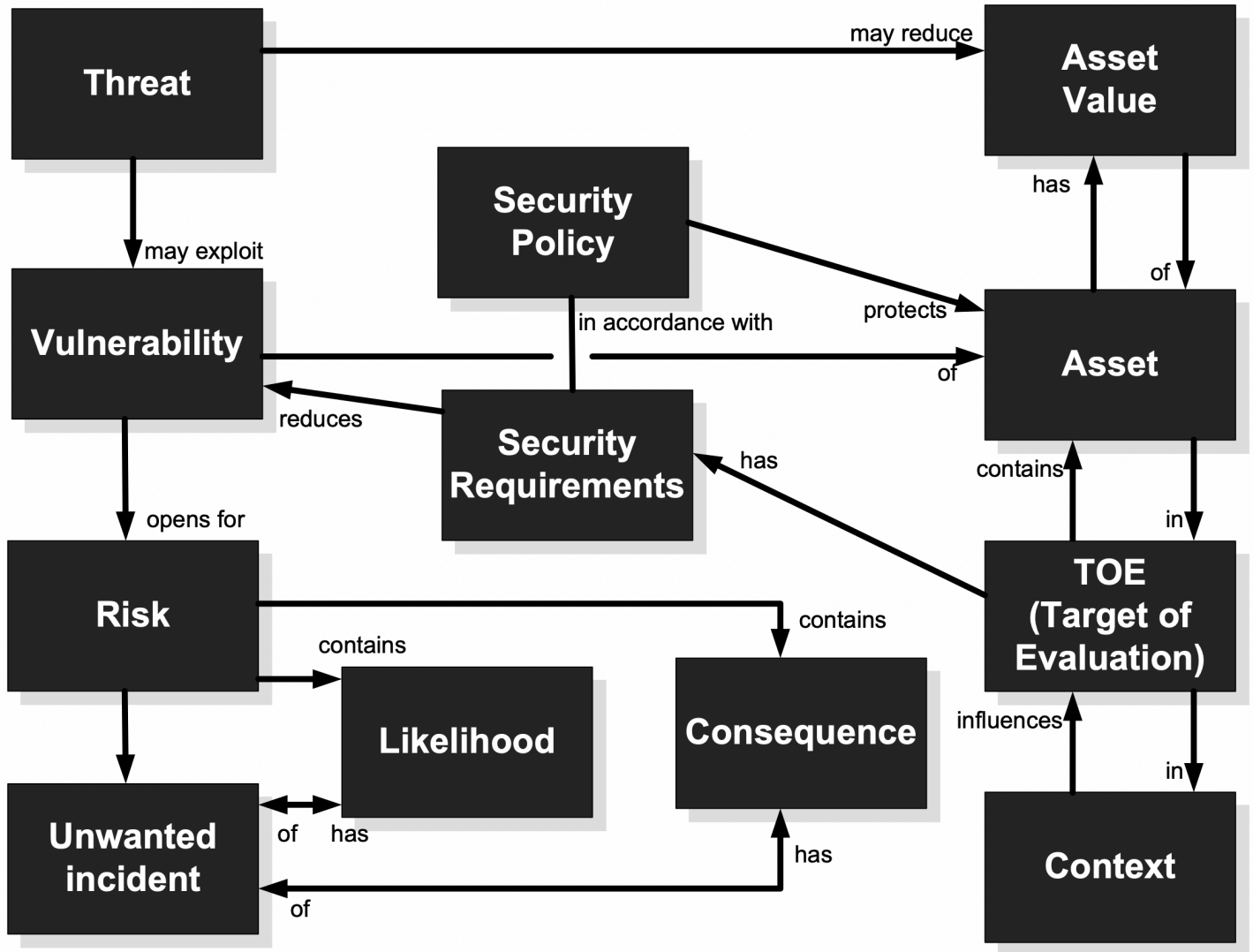
Improper release (0.2-5) Ex-employee access (0.1-1)
Compromise
Loose Documents (0-5) Improper marking (0.1-100)

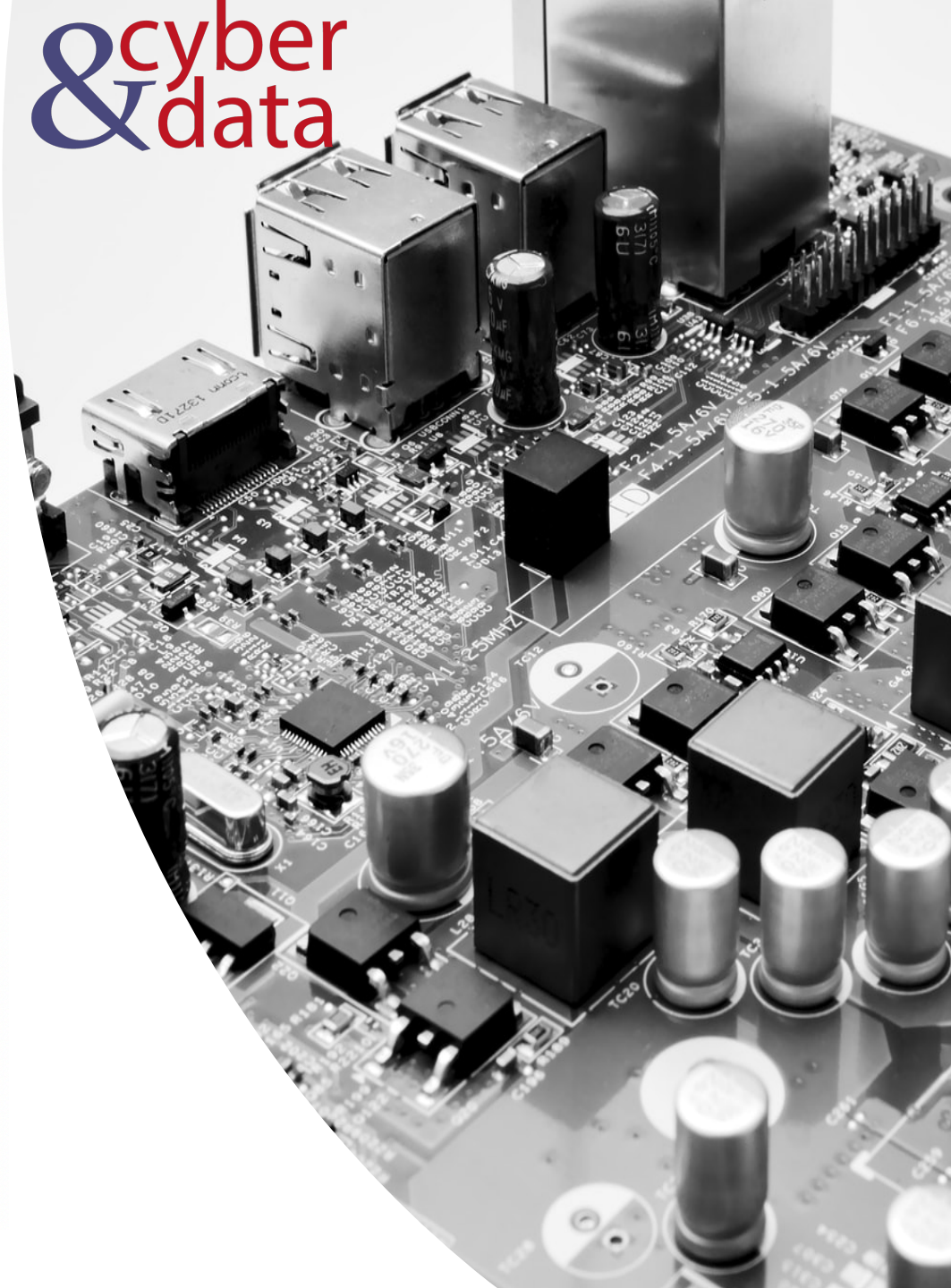
Password compromise
System entry (1-5) Uncleared visit (0.1-1000)

Major (0.01-0.09) Explosion (0.0001-0.01)
Fire
Minor (0.1-0.9) Catastrophic (0.001-0.009)

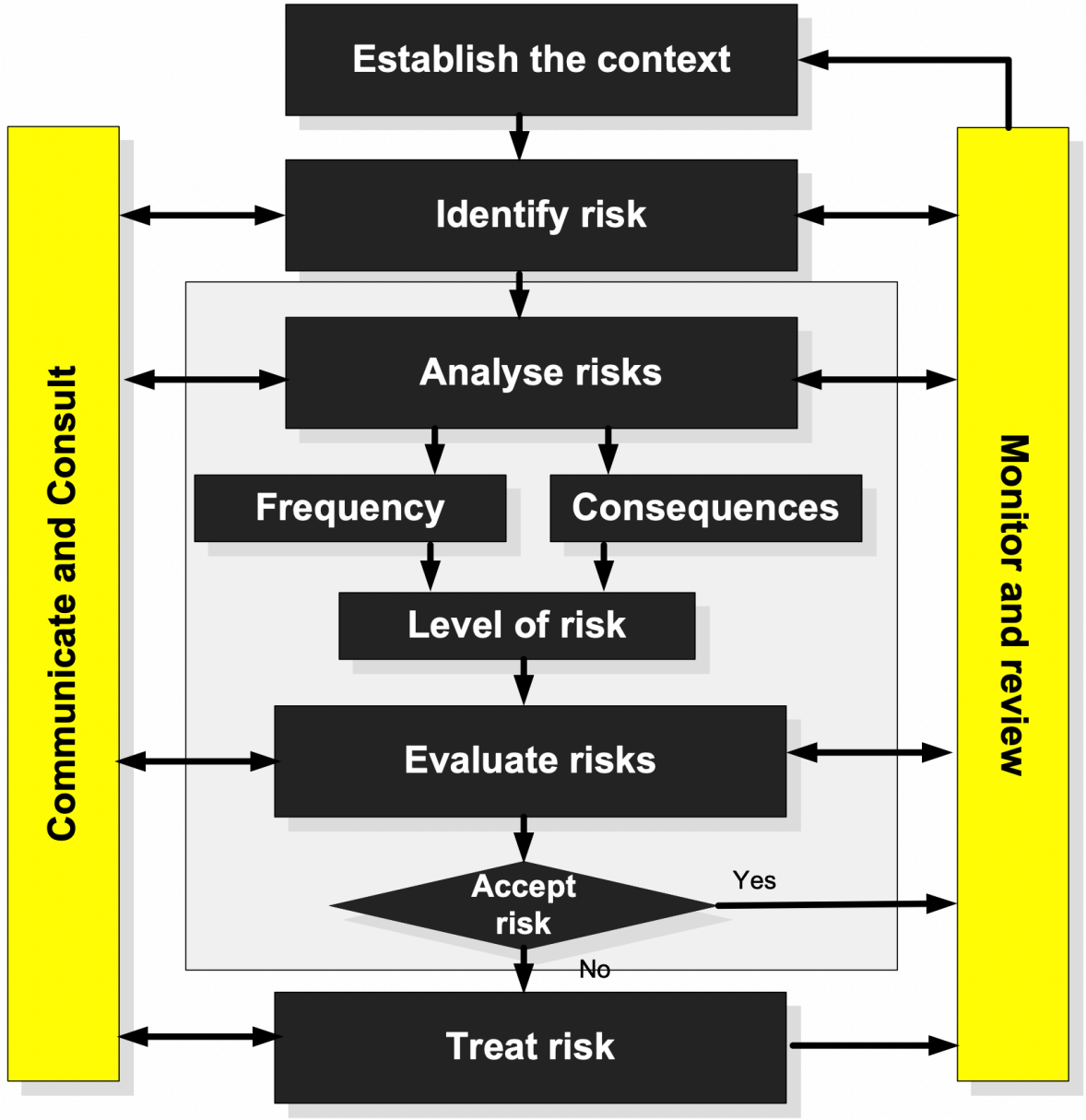
Disgruntled employee (0.1-5) Terrorism (0.002-0.006)
Forced entry
Burglary (?) Vandalism (0.008-1)

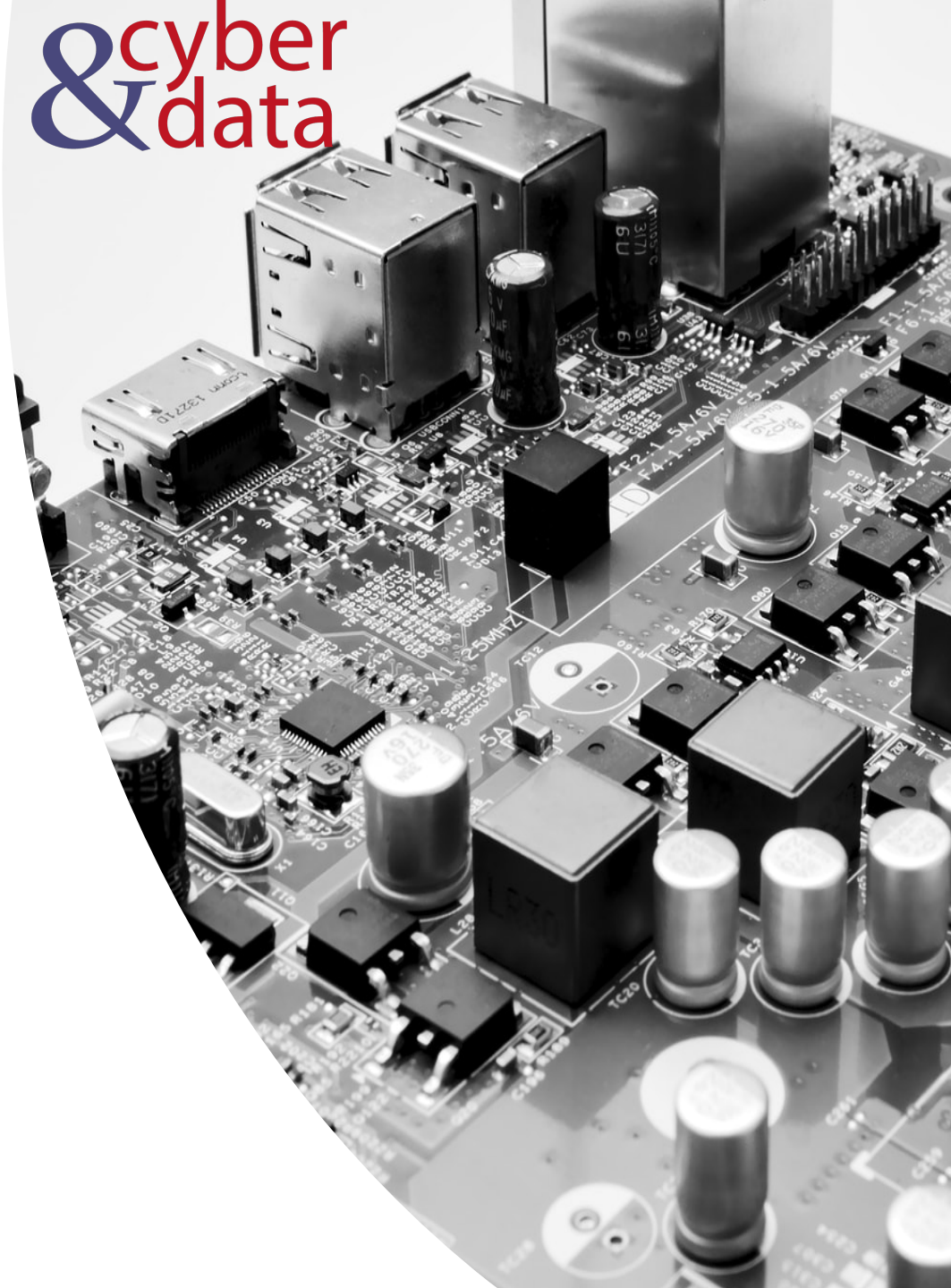
CORAS Ontology





CORAS Risk Management



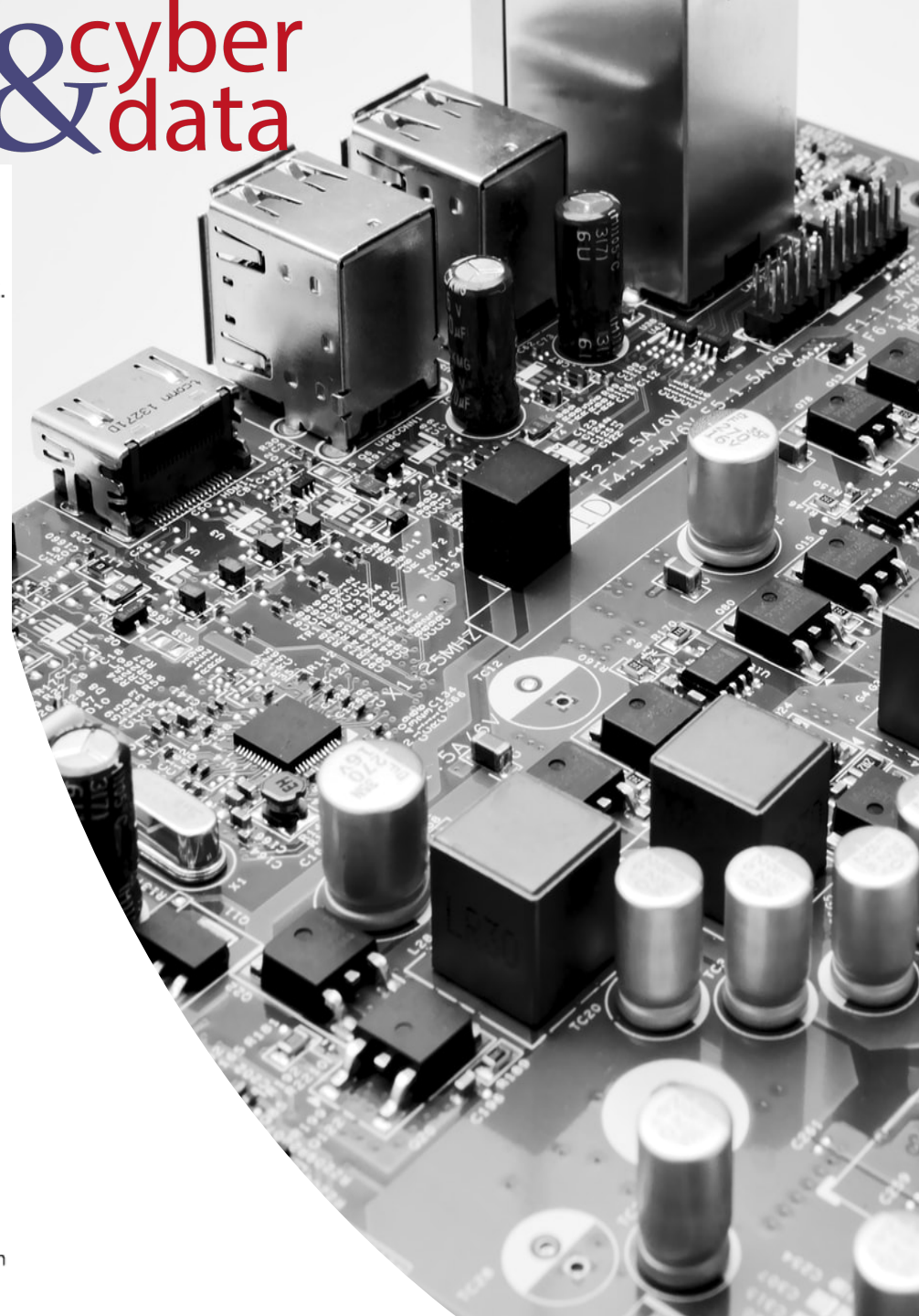


cyber & data

"From bits to information"

Kill Chain Model

Incident Taxonomy



A Threat:
- Hacker.
- Spies
- Terrorists.
- Corporate Raiders.
- Professional Criminals.
- Vandals.
- Military Forces.

is achieved with Attack Tools:
- User command.
- Script or program.
- Autonomous Agent.
- Toolkit
- Distributed Tool.
- Data Tap.

for Vulnerabilities:
- Implementation vulnerability.
- Design vulnerability.
- Configuration vulnerability.

A **Threat** (eg Spies) **Is achieved with** **Attack Tools** (eg Toolkit) **for** **Vulnerabilities** (eg design vulnerability) **with** **Access** (eg Unauthorized Access for Processes) **which** **Results** (eg Theft of Service) **in, for** **Objectives** (eg Financial Gain)

for Objectives:
- Challenge/Status.
- Political Gain.
- Financial Gain.
- Damage.
- Destruction of an Enemy.

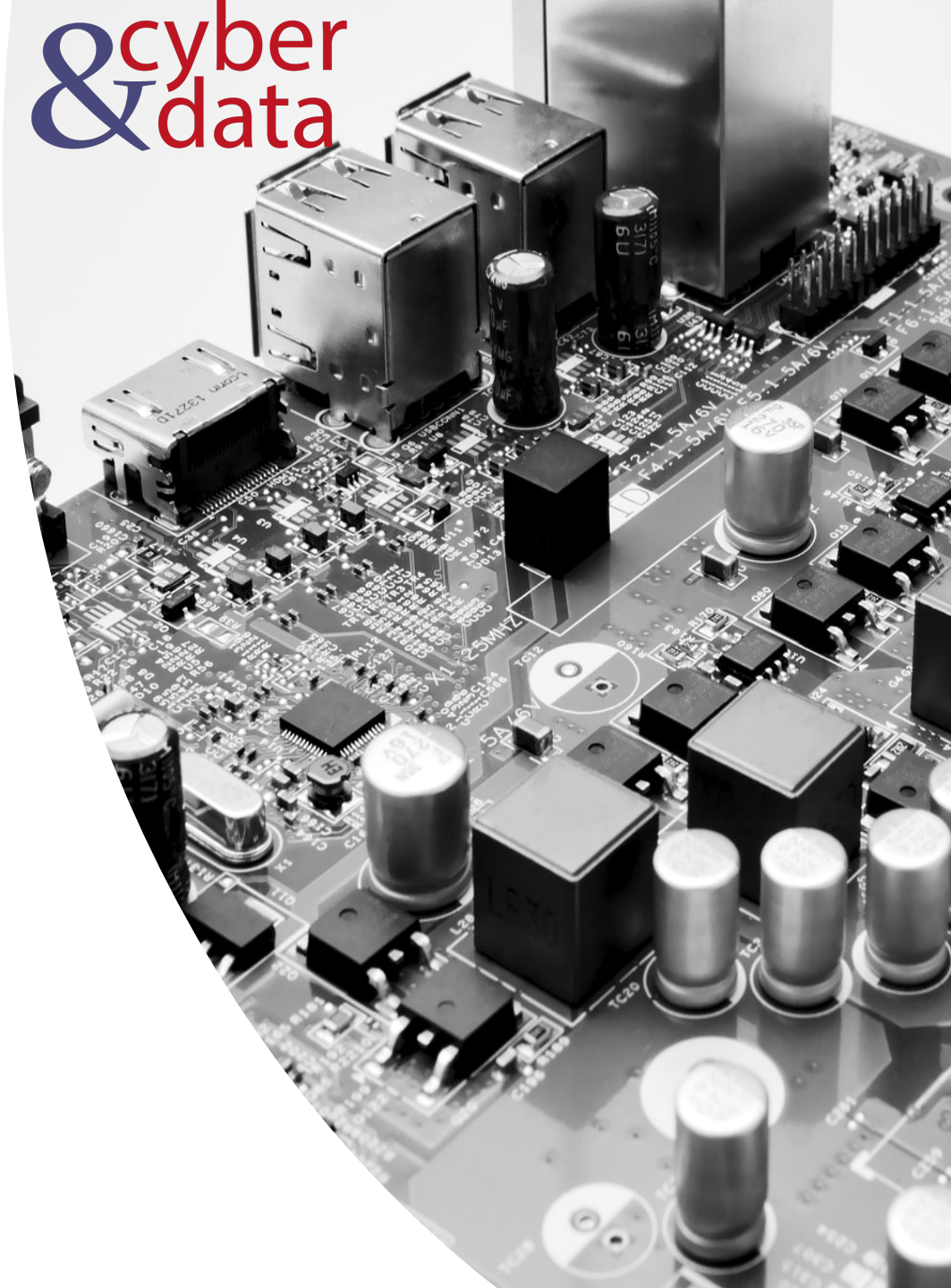
which Results in:
- Corruption of Information.
- Disclosure of Information.
- Theft of Service.
- Denial-of-Service.

with Access for:
- Files.
- Data in transit.
- Objects in Transit.
- Invocations in Transit.

Author: Prof Bill Buchanan

Kill Chain Model

Reconnaissance	Identification, Selection and Profiling of Target
Weaponize	Coupling of Remote Access Trojan with an Exploit into a deliverable payload called as Cyber Weapon
Delivery	Transmission of the cyber weapon to the targeted environment
Exploitation	Triggering the attacker's payload on target system
Installation	Installation of backdoor and maintaining persistence
Command and Control	Outbound internet controller servers to communicate with compromised host
Act on Objective	Data Exfiltration, Network Spreading, System Disruption



Unified Kill Chain Phases

Initial Foothold: Compromised System

- Reconnaissance
- Weaponization
- Delivery
- Social Engineering
- Exploitation
- Persistence
- Defense Evasion
- Command & Control

Pivoting

Network Propagation: Internal Network

- Discovery
- Privilege Escalation
- Execution
- Credential Access
- Lateral Movement

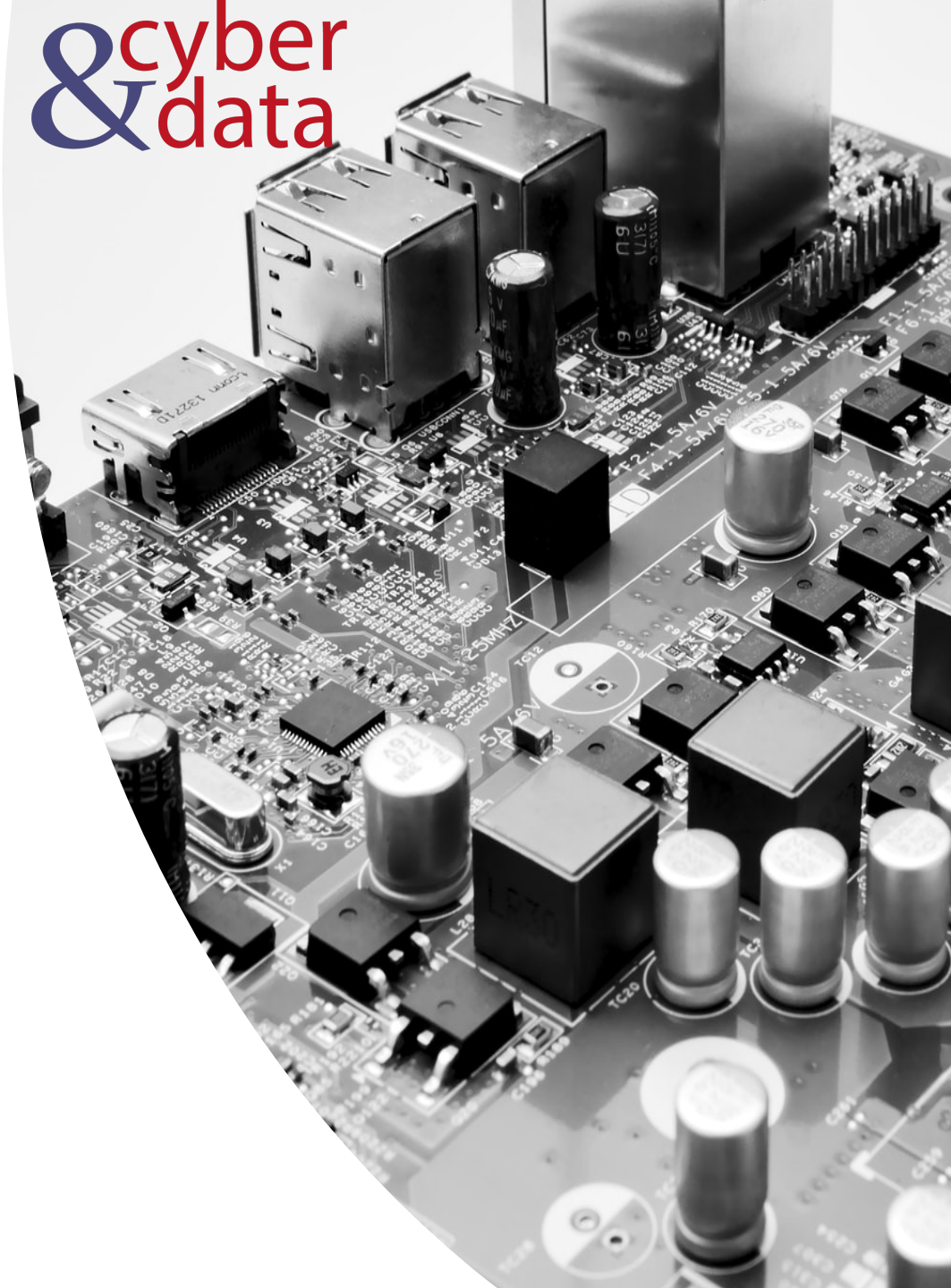
Access

Action on Objectives: Critical Asset Access

- Collection
- Exfiltration
- Target Manipulation
- Objectives

Unified Kill Chain Model

#	Unified Kill Chain	Cyber Kill Chain® (CKC)	Laliberte	Nachreiner	Bryant	Malone	MITRE ATT&CK™	UKC after literature study	UKC after Red Team C1	UKC after Red Team C2	UKC after Red Team C3	UKC after Red Team KC	UKC after APT28 C4 & KC
1	Reconnaissance	1	1	1	1	1		1	1	1	1	1	1
2	Weaponization	2	3	3	3	2		2	2	2	2	2	2
3	Delivery	3	5	5	6	3		7	7	3	3	3	3
4	Social Engineering	5	6	6	11	5		3	3	4	4	4	4
5	Exploitation	6	8	8	14	6		5	4	5	5	5	5
6	Persistence	8	14	9	18	8	6	6	5	6	6	6	6
7	Defense Evasion	18	18	14	16	10	11	8	6	7	7	7	7
8	Command & Control			18		5	7	9	8	8	8	8	8
9	Pivoting					11	13	11	9	9	9	9	9
10	Discovery					14	10	10	11	11	11	10	10
11	Privilege Escalation					17	14	14	10	10	10	11	11
12	Execution					18	12	12	14	14	14	12	12
13	Credential Access						15	13	12	12	12	13	13
14	Lateral Movement						16	17	13	13	13	14	14
15	Collection						8	15	17	17	17	17	15
16	Exfiltration							16	15	15	15	15	16
17	Target Manipulation								16	16	16	16	17
18	Objectives												18



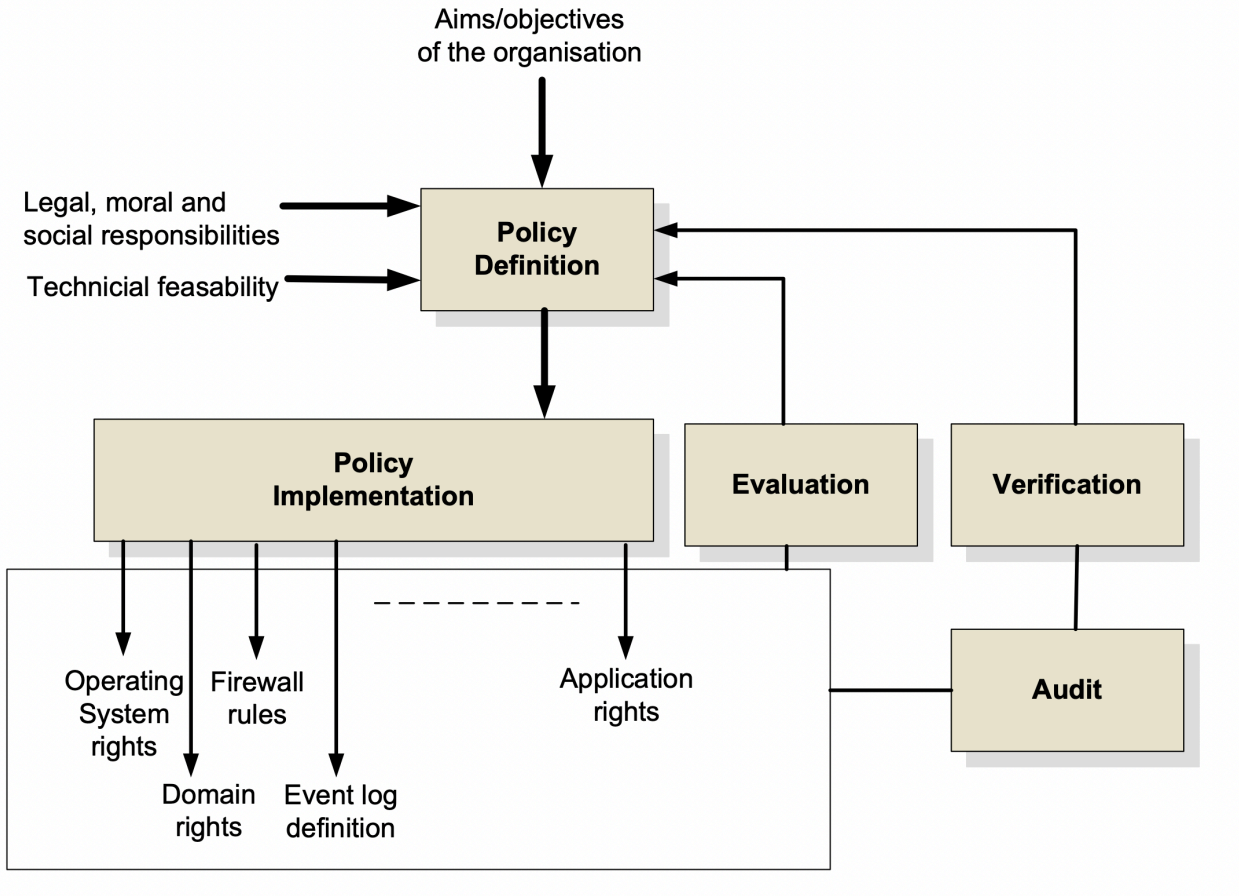
cyber & data

"From bits to information"

Defence Mechanisms

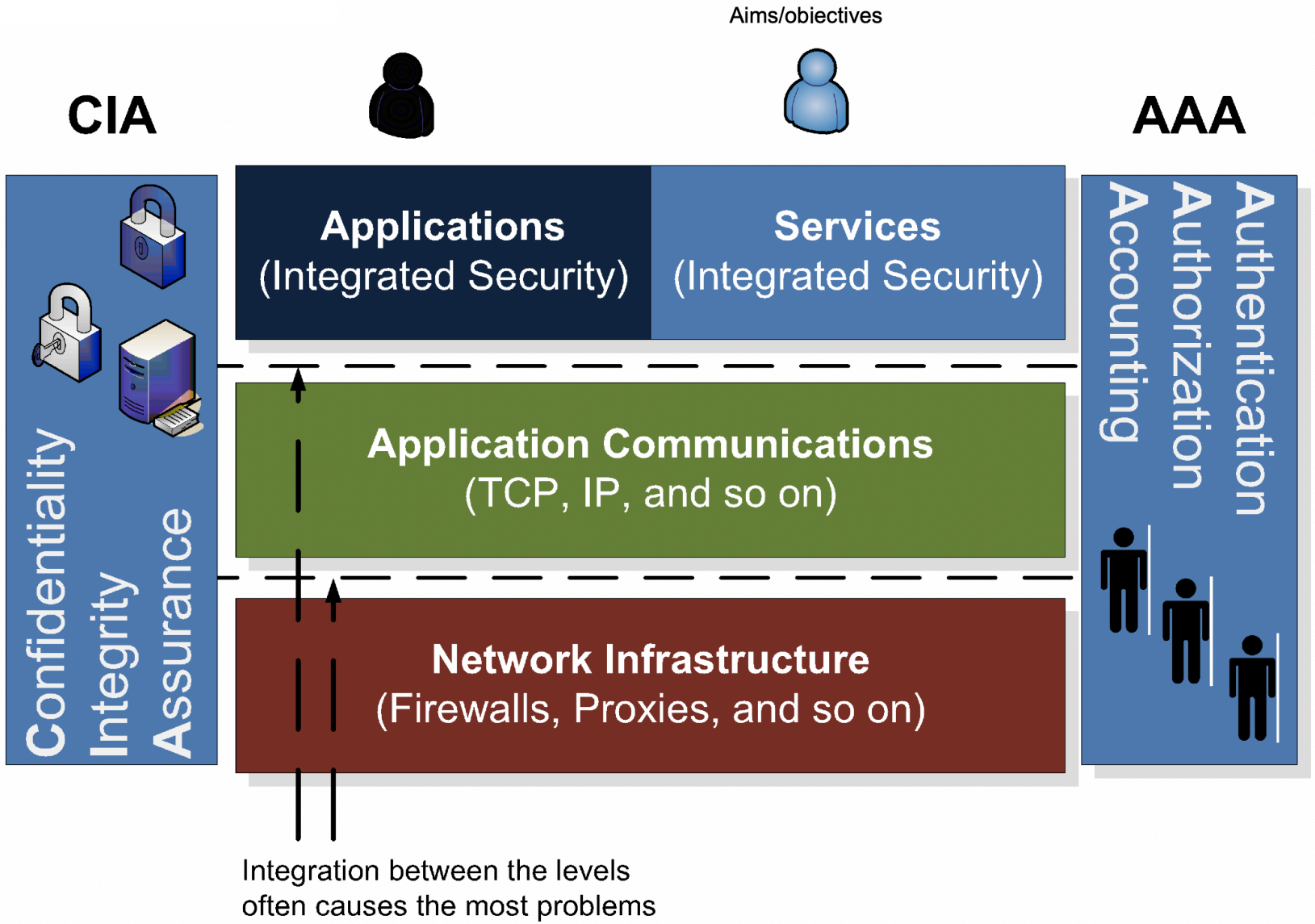
Types of intelligence

- **Deter**. This is where the system is designed and implemented in order to initially deter intruders from attacking the system in the first place.
- **Log**. This is a key element in modern systems which requires some form of logging system. It is important that the data that is logged does not breach any civil liberties, and is in a form which can be used to enhance the future security of the system.
- **Detect**. This is where detection agents are placed within the network to detect intrusions, and has methods of tracing the events that occurred in an intrusion, so that it can be used either in a forensic computing investigation, and/or to overcome a future intrusion. Organisations often have many reasons for detecting network traffic.
- **Protect**. This is where policies are created which protect systems, users and data against attack, and in reducing this potential damage. A key element of this is to protect them against accidental damage, as accidental damage is often more prevalent than non-accidental damage.
- **React**. This is where a policy is defined which reacts to intrusions, and defines ways to overcome them in the future. Often organisations do not have formal policies for this type of activity, and often rely on ad-hoc arrangements, where the method of reacting to a security breach is created after the event.
- **Recover**. This is where policies are defined to overcome any system damage, whether it is actual physical damage, the abuse of users; or the damage to data.
- **Audit/verify**. It is important that the security policy allows for auditing and for the verification that it achieves its requirements.



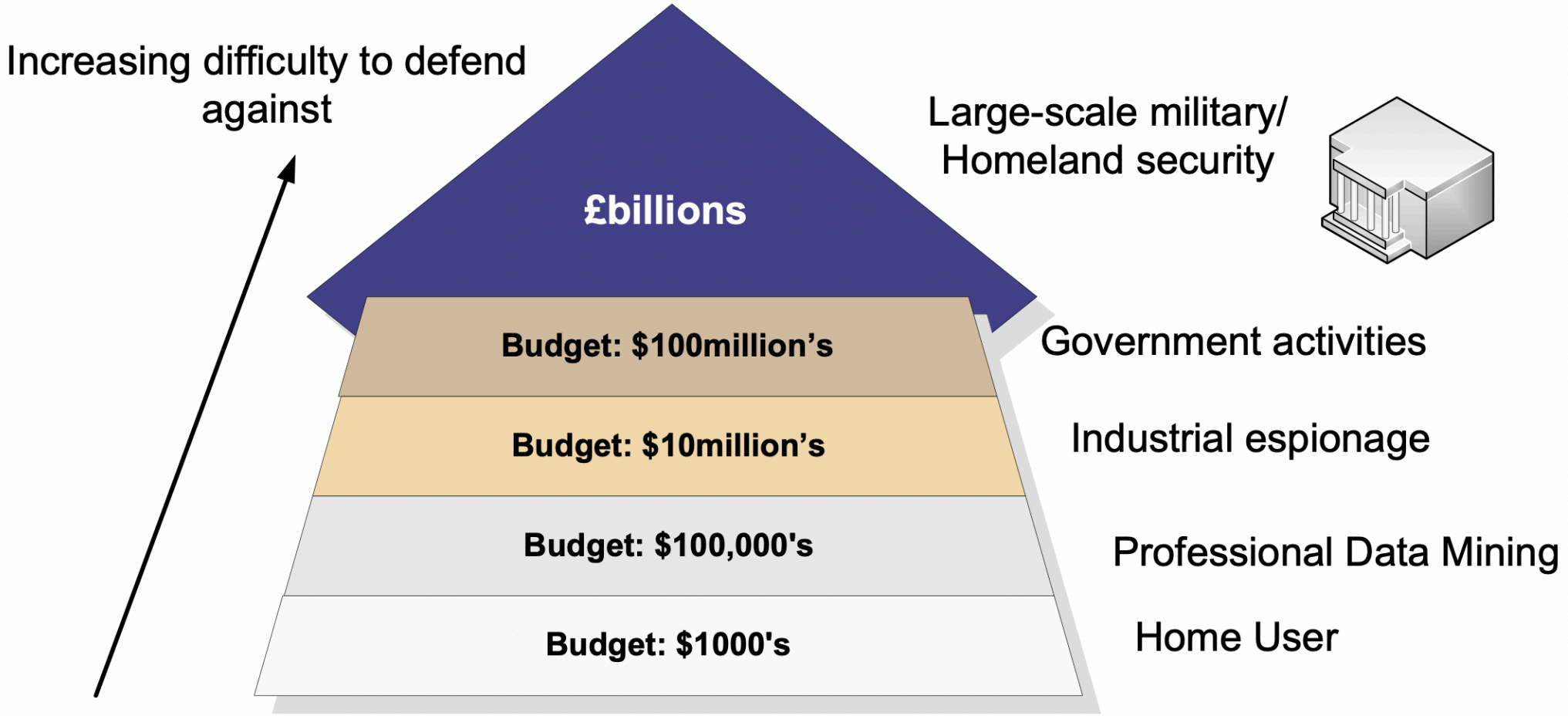
Types of intelligence

- **Deter**. This is where the system is d order to initially deter intruders fro first place.
- **Log**. This is a key element in moder some form of logging system. It is ir logged does not breach any civil lib can be used to enhance the future
- **Detect**. This is where detection age network to detect intrusions, and h events that occurred in an intrusior in a forensic computing investigatio future intrusion. Organisations ofte detecting network traffic.
- **Protect**. This is where policies are c users and data against attack, and i damage. A key element of this is to accidental damage, as accidental da than non-accidental damage.
- **React**. This is where a policy is defir and defines ways to overcome then organisations do not have formal p and often rely on ad-hoc arrangem reacting to a security breach is crea
- **Recover**. This is where policies are system damage, whether it is actua of users; or the damage to data.
- **Audit/verify**. It is important that th auditing and for the verification tha



Types of intelligence

Aims/objectives



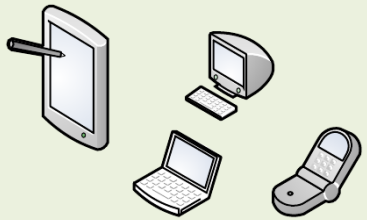
often causes the most problems

"From bits to information"

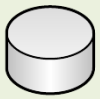
Defence in Depth

Defence in depth

Users

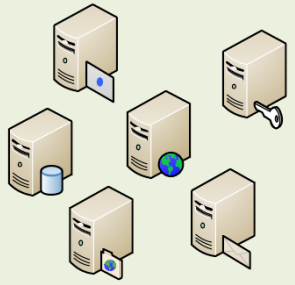


Assets

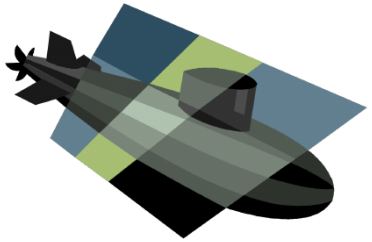


Hello. How are you? Is this okay?

Data

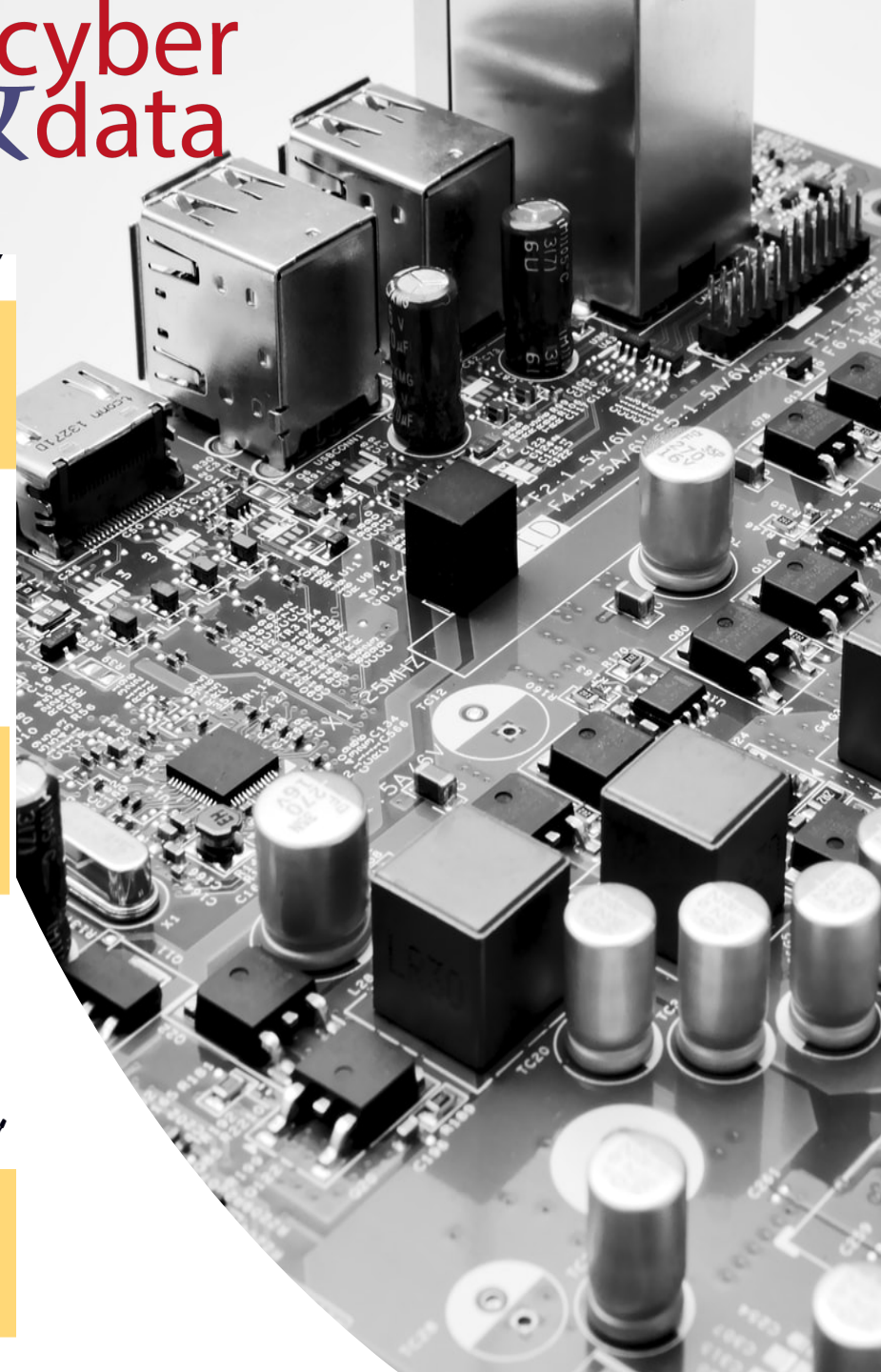


Systems



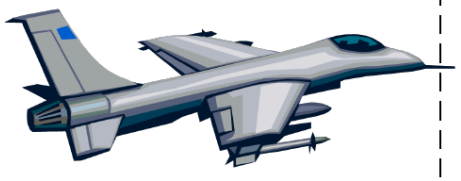
Even with the best defences, intruders can

& cyber data



Defence in depth

&cyber data

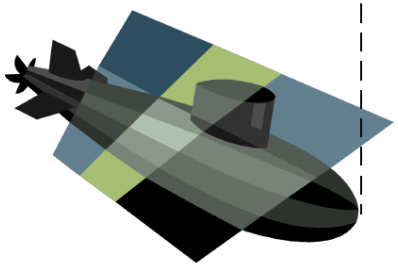


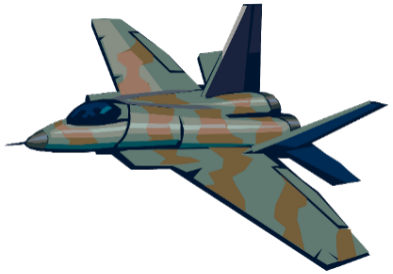
Defence

Defence

Defence

Defence



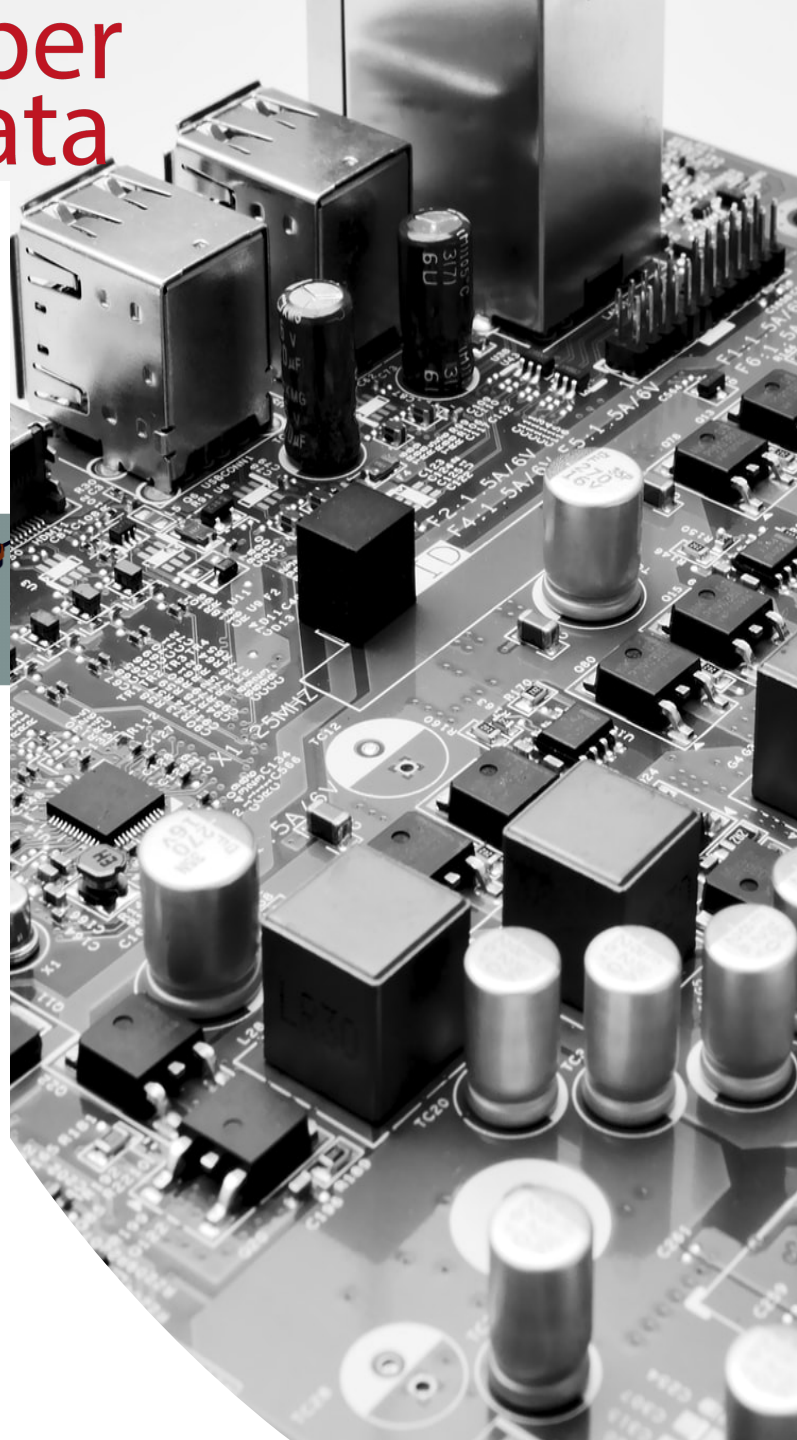


Forth-level defence

Third-level defence

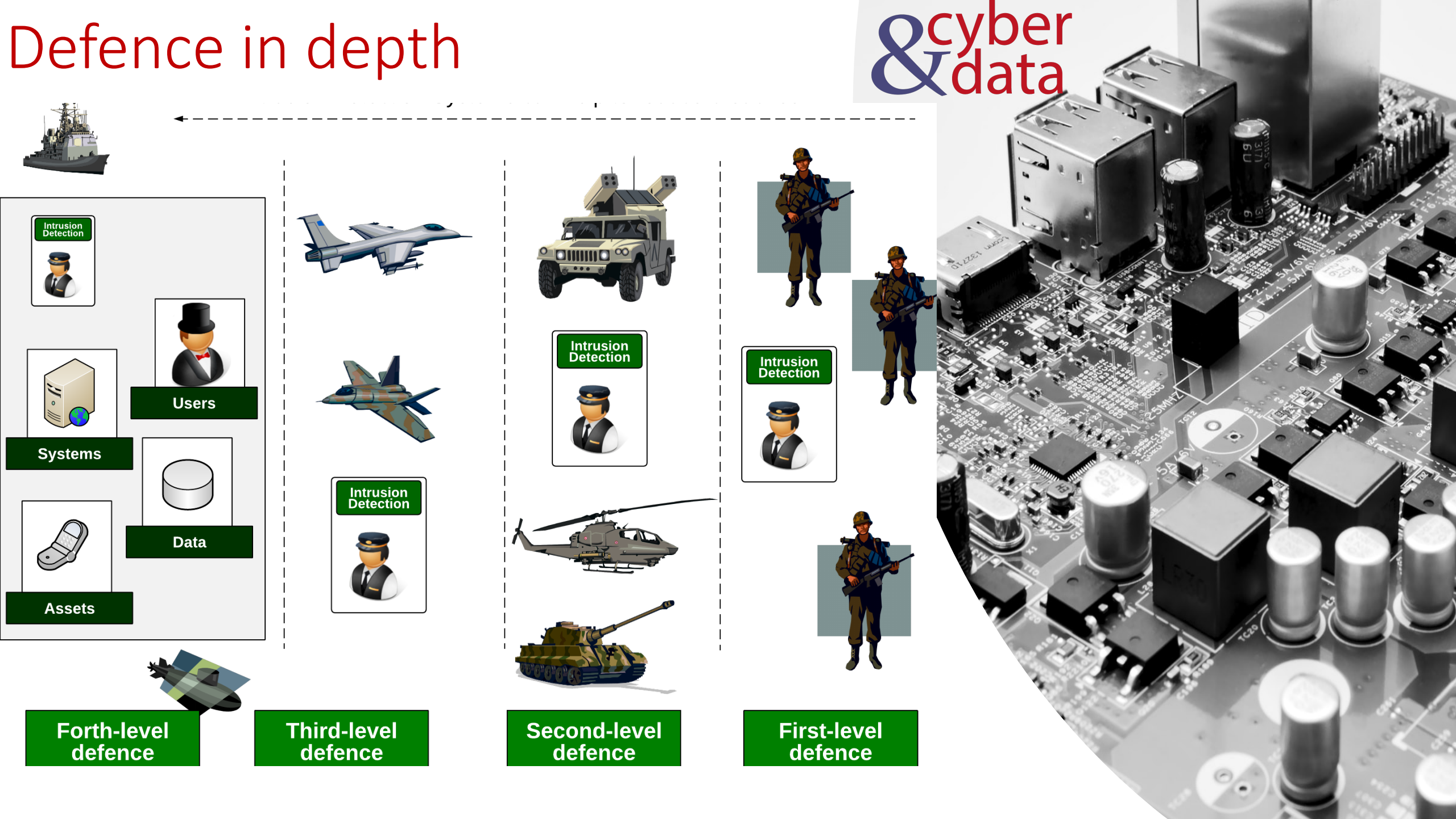
Second-level defence

First-level defence



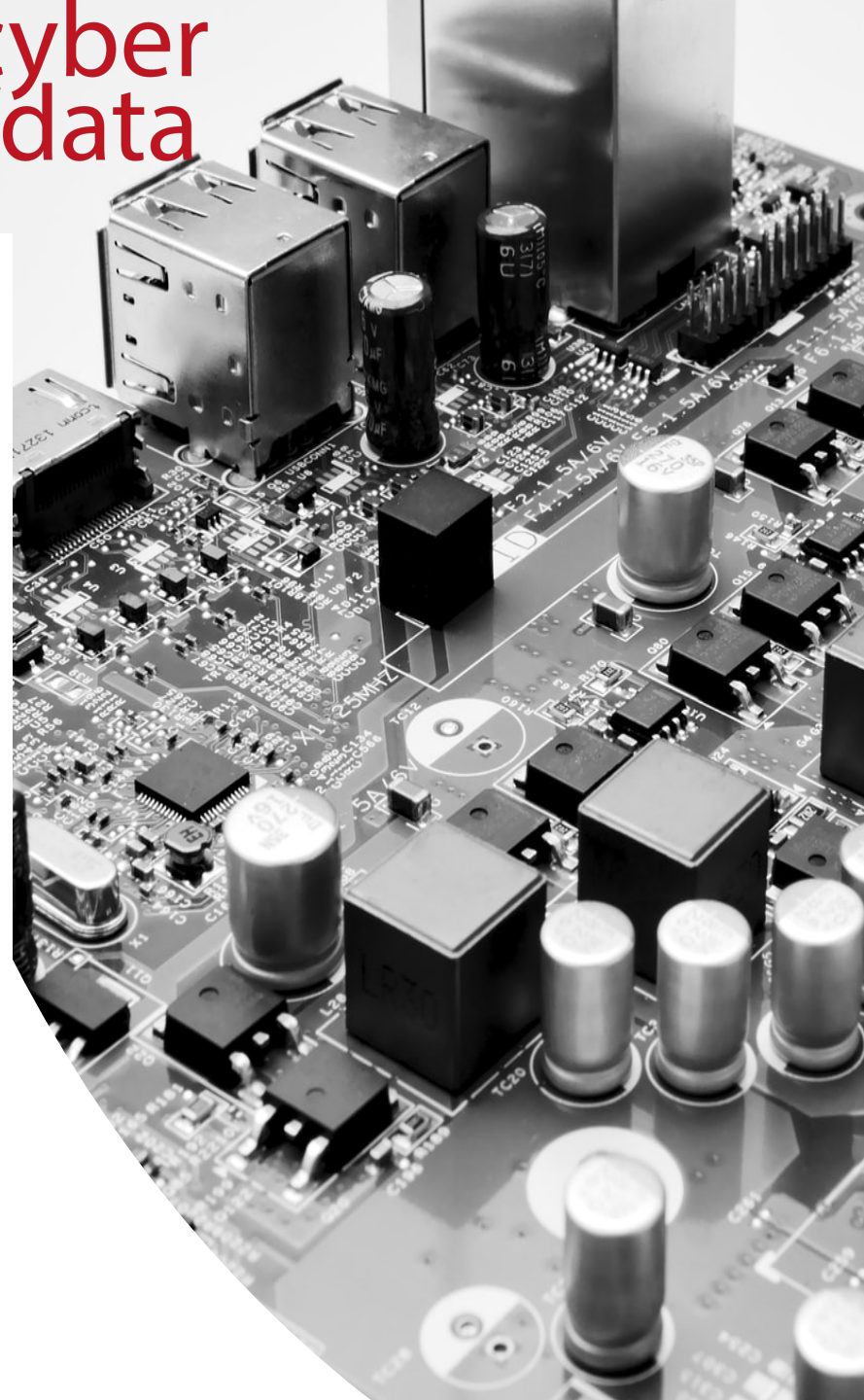
Defence in depth

&cyber data



Threats

&cyber data



Corporate access

Email access

Web access

Intrusion Detection

Users

Systems

Data

Assets

Network/Organisational perimeter

Firewall/ gateway

Data stealing

External hack

DoS (Denial-of-sevice)

Personal abuse

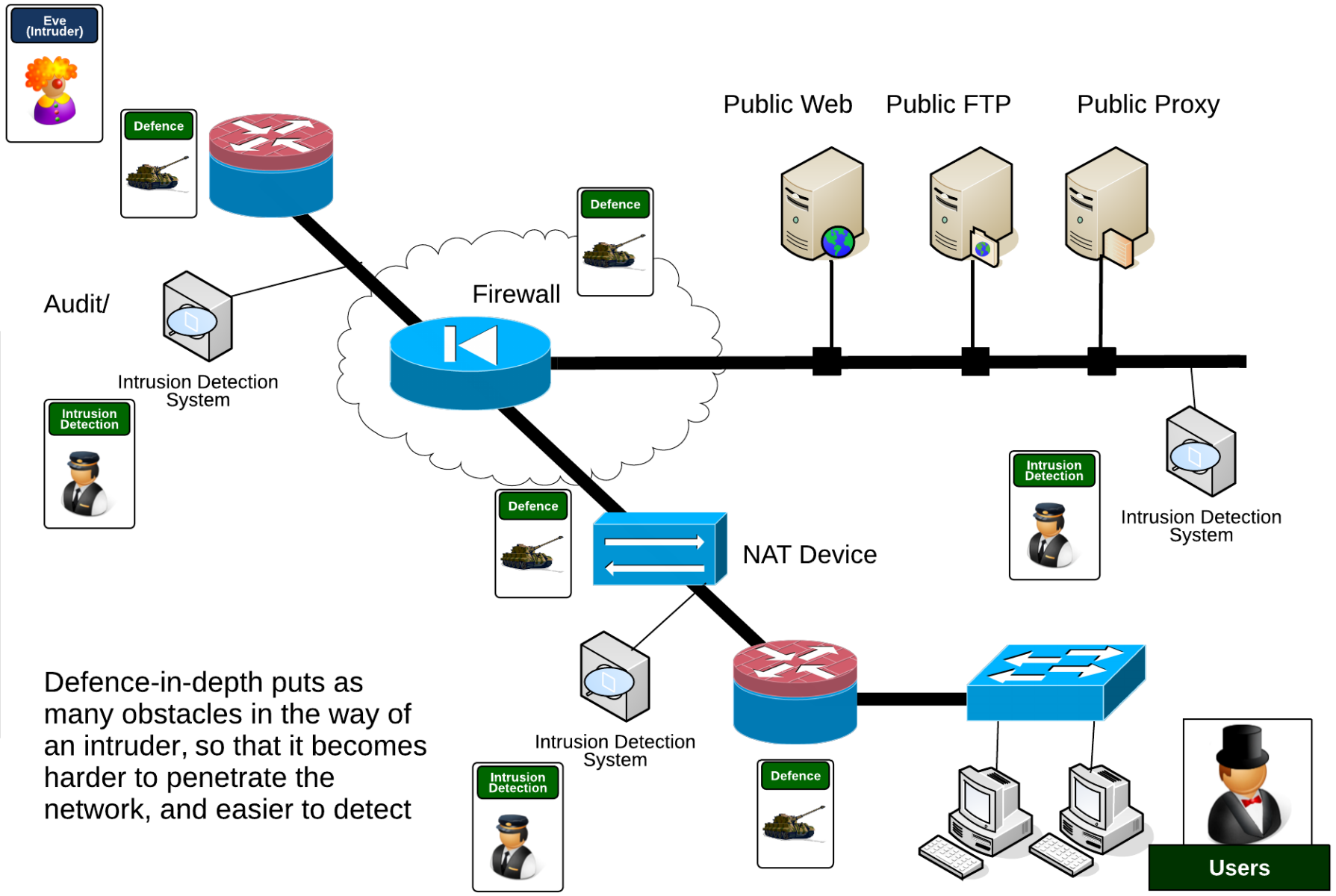
Worms/viruses

Terrorism/extortion

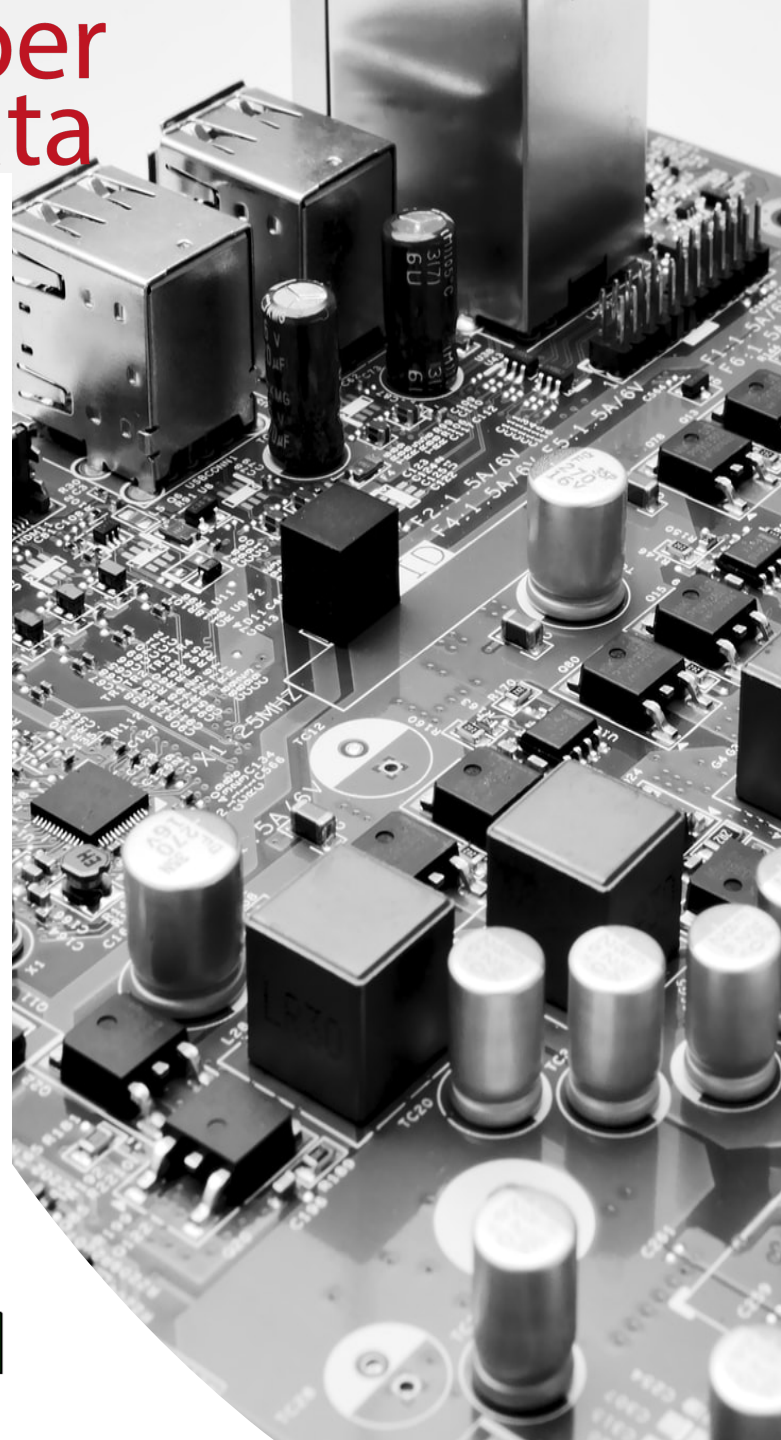
Fraud

Defence in depth

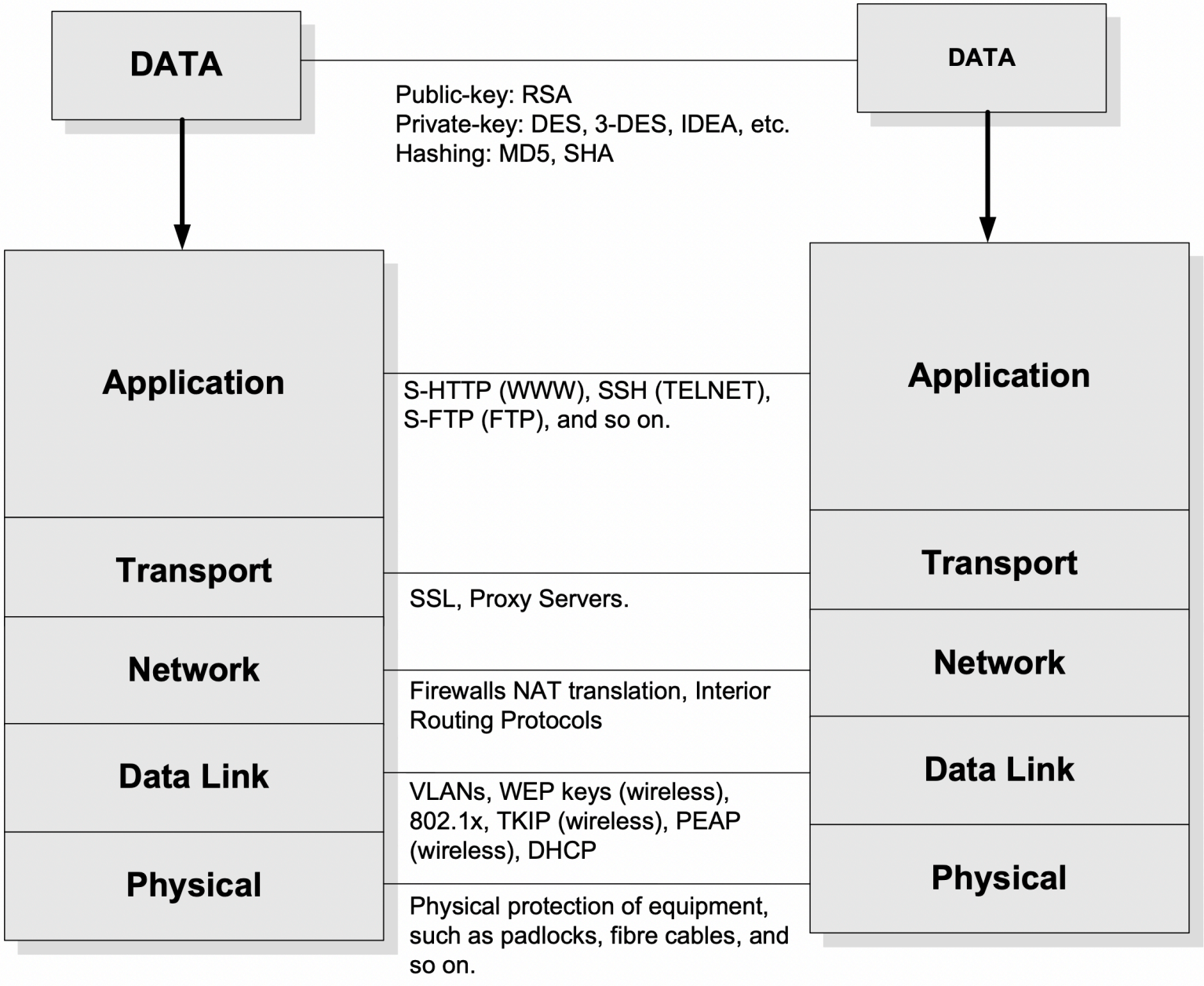
&cyber data

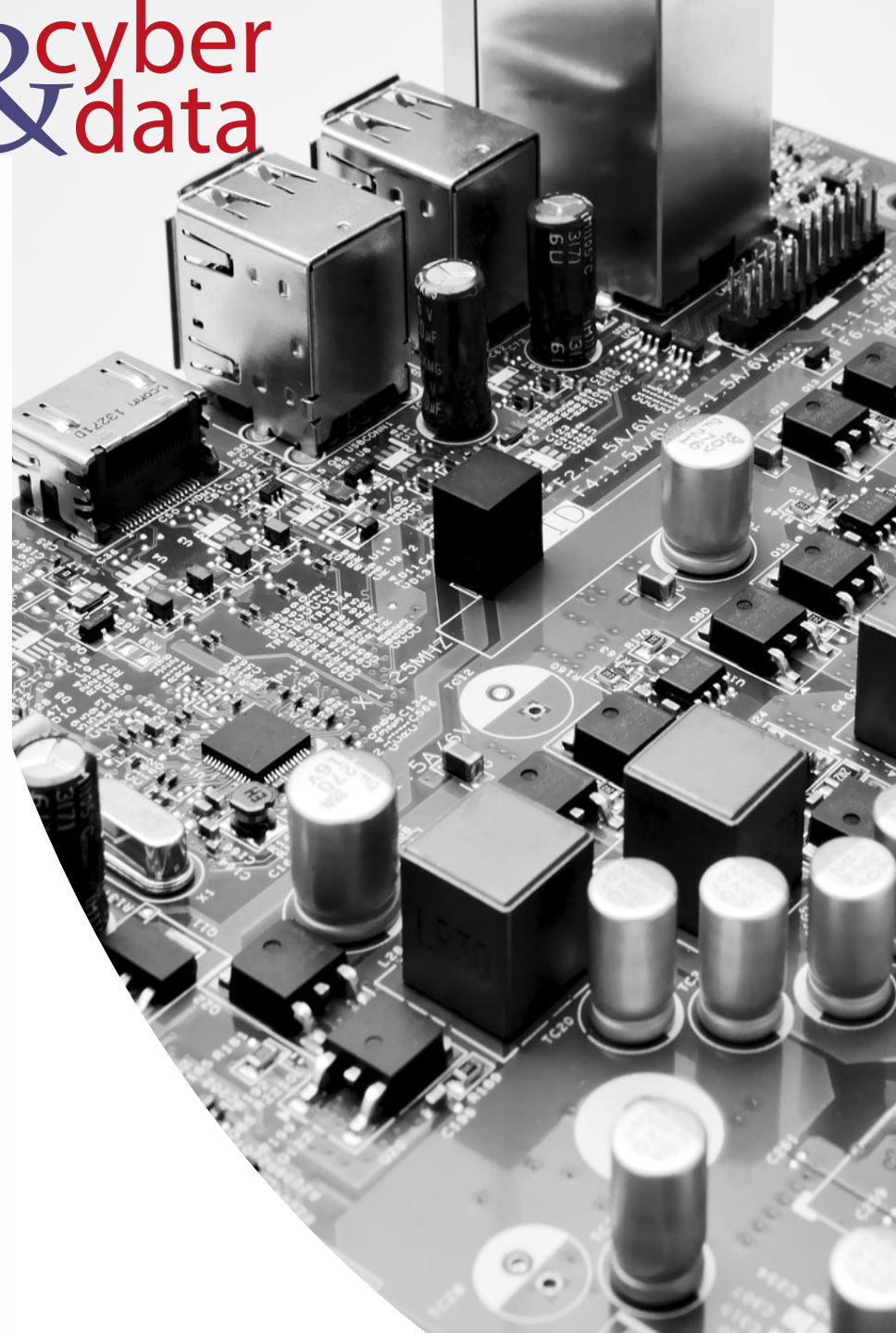


Defence-in-depth puts as many obstacles in the way of an intruder, so that it becomes harder to penetrate the network, and easier to detect



Layered Model





cyber & data

"From bits to information"

Defence Systems, Policies and Risks