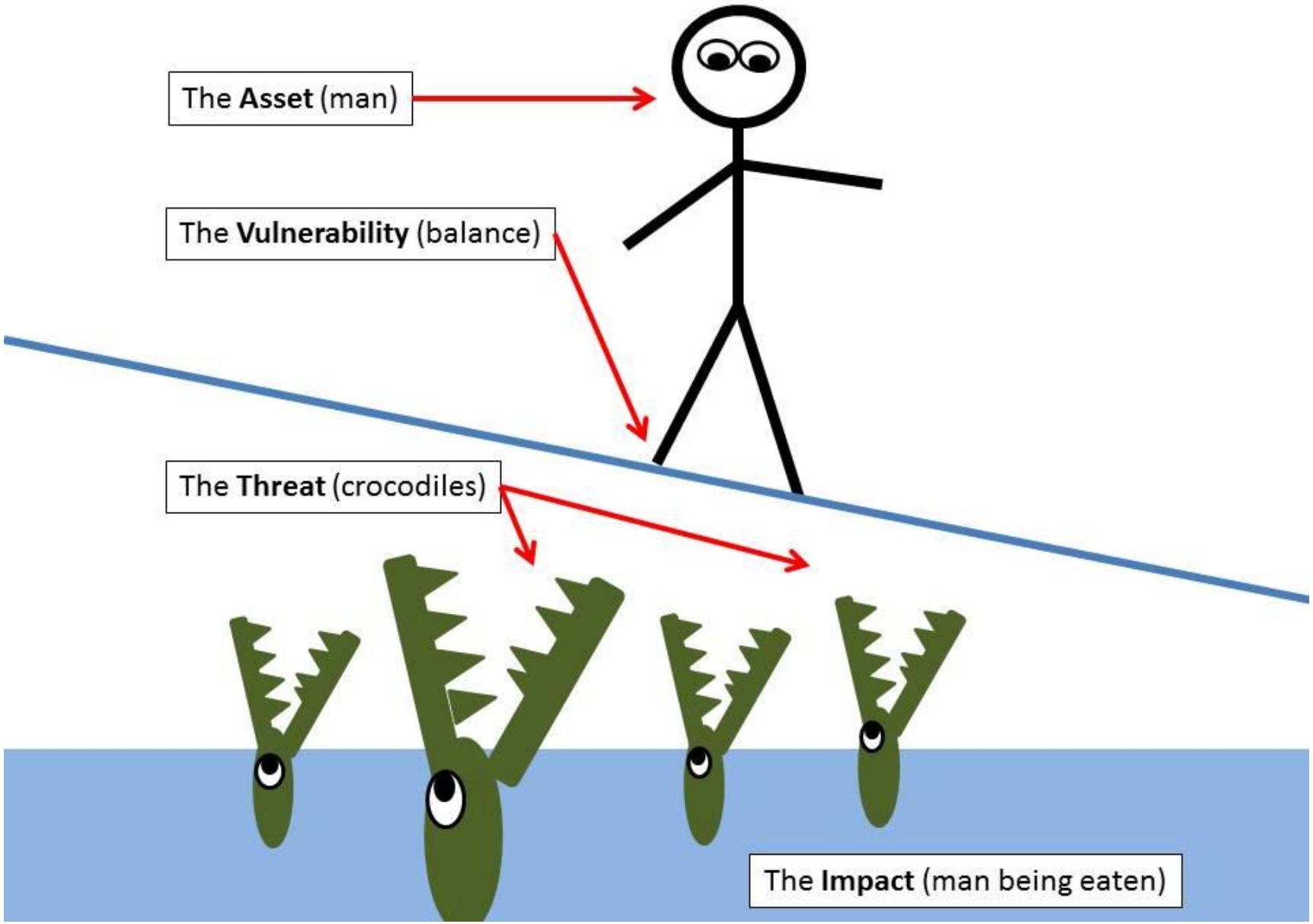

bmc
Threat
A new incident that has potential to harm a system
Vulnerability
A known weakness of an asset that hackers could exploit
Risk
The potential for loss or damage when a threat exploits a vulnerability

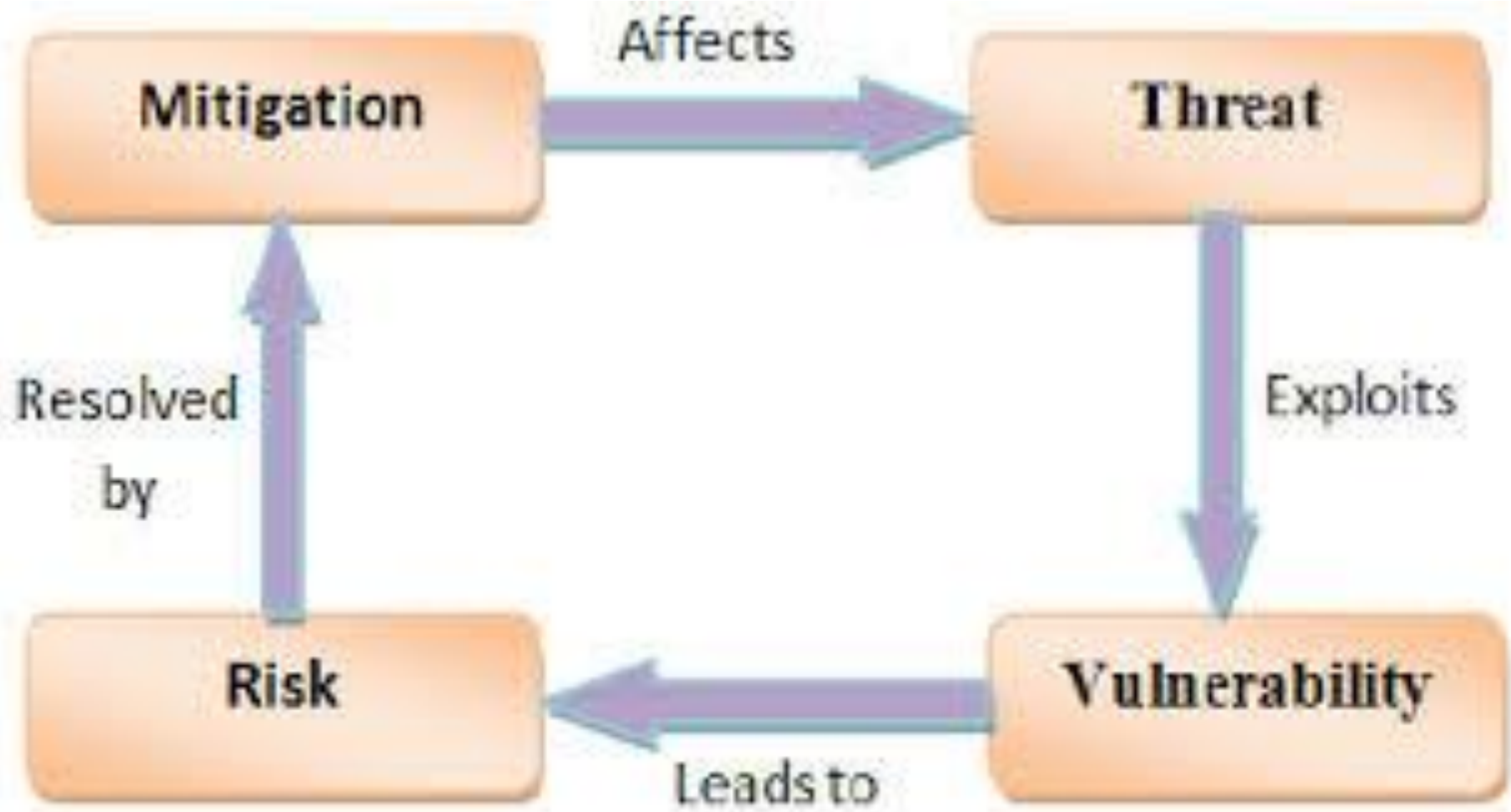

The **Asset** (man)
The **Vulnerability** (balance)
The **Threat** (crocodiles)
The **Impact** (man being eaten)

Silly Example

- Increase the size or weight of the pen, so that cat cannot move it
  - Close the vulnerability directly
- Secure the pen where the cat cannot reach it
  - Close the vulnerability by preventing its exploitation
- Prevent the cat from taking the pen
  - Mitigate the threat of the cat directly
  - Impractical in most information systems applications

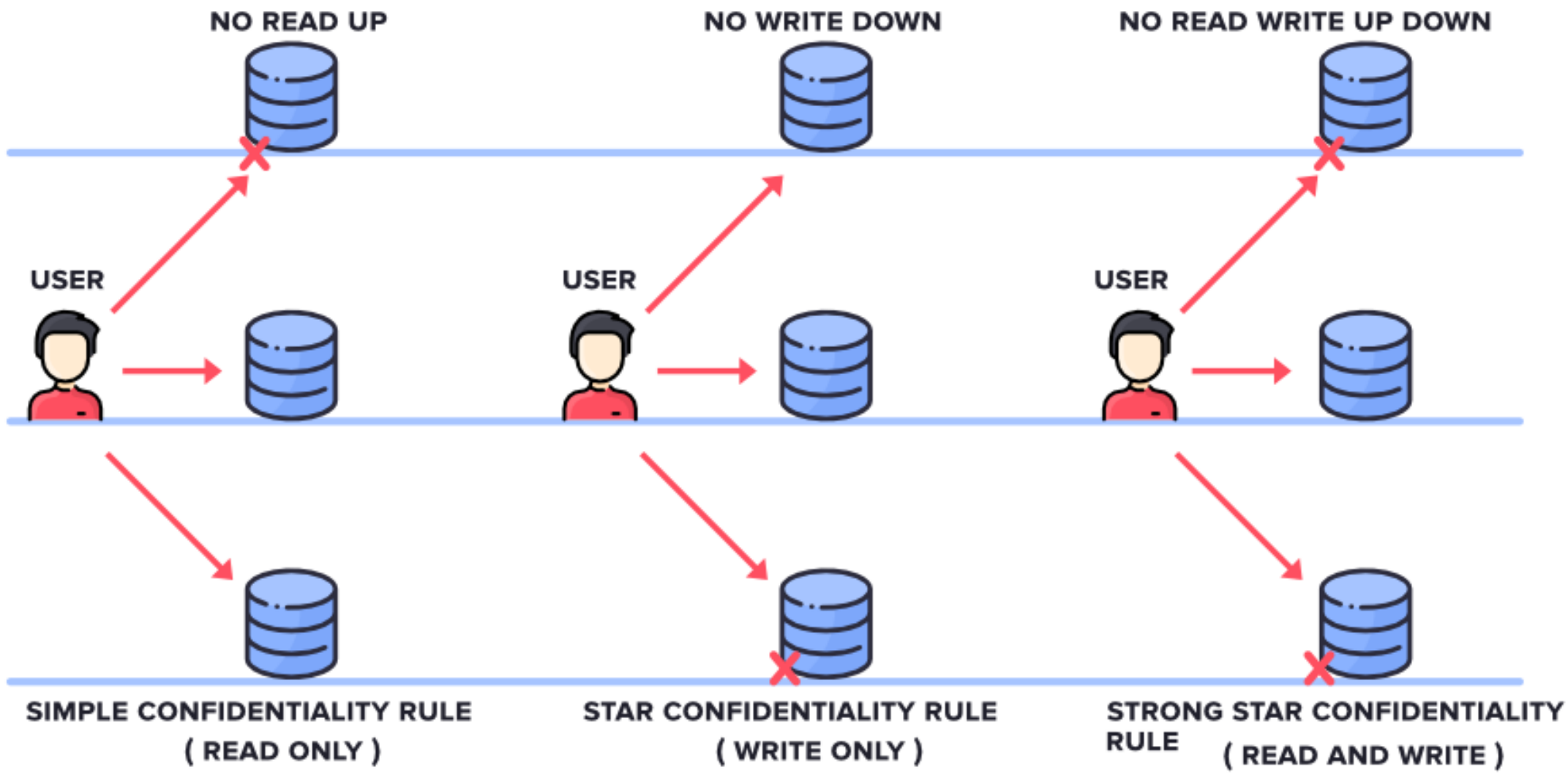
	Vulnerability	Threat	Risk
Example 1	Terminated employee ID's are not removed from the system	Dialing into the company's network and accessing proprietary info	Unauthorized disclosure of sensitive business information
Example 2	Improper maintenance of fire fighting equipment	Fire	Loss of life, data and infrastructure

THREAT
VERSUS
VULNERABILITY

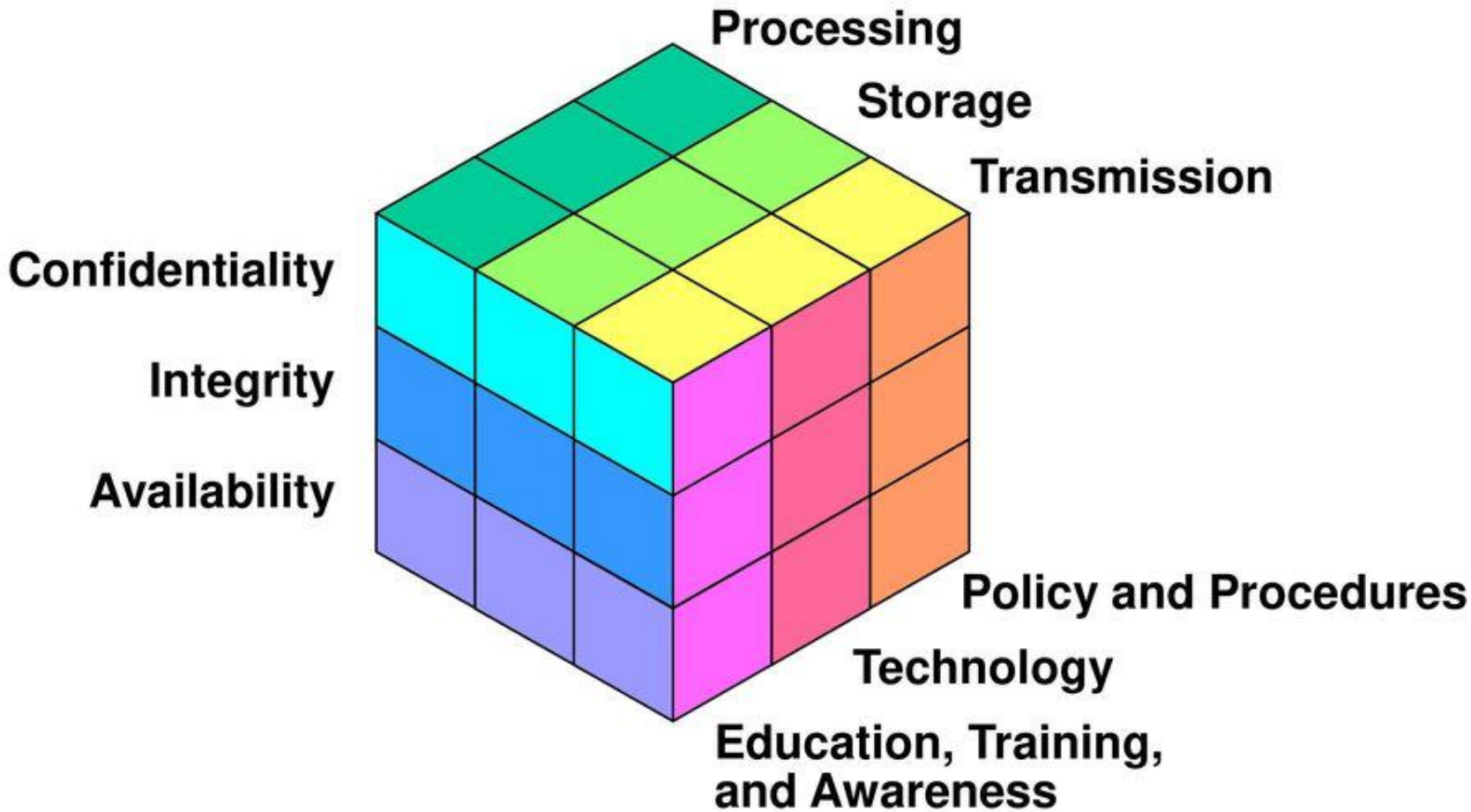

Mitigation
Affects
Threat
Resolved by
Exploits
Risk
Vulnerability
Leads to

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Control Recommendations
System failure — Overheating in server room High	Air-conditioning systems is ten years old. High	Servers Critical	All services (website, email, etc.) will be unavailable for at least 3 hours. Critical	High Current temperature in server room is 40C	High Potential loss of $50,000 per occurrence	Buy a new air conditioner, $3,000 cost.
Malicious human (interference) — DDOS attack. High	Firewall is configured properly and has good DDOS mitigation. Low	Website Critical	Website resources will be unavailable. Critical	Medium DDOS was discovered once in 2 years.	Medium Potential loss of $10,000 per hour of downtime	Monitor the firewall.
Natural disasters — Flooding High	Server room is on the 3rd floor. Low	Servers. Critical	All services will be unavailable. Critical	Low Last flood in the area happened 10 years ago.	Low	No action needed.
Accidental human interference — Accidental file deletions High	Permissions are configured properly; IT auditing software is in place; backups are taken regularly. Low	Files on a file share Medium	Critical data could be lost but almost certainly could be restored from backup. Low	Medium	Low	Continue monitoring permissions changes, privileged users and backups.

BELL - LAPADULA MODEL

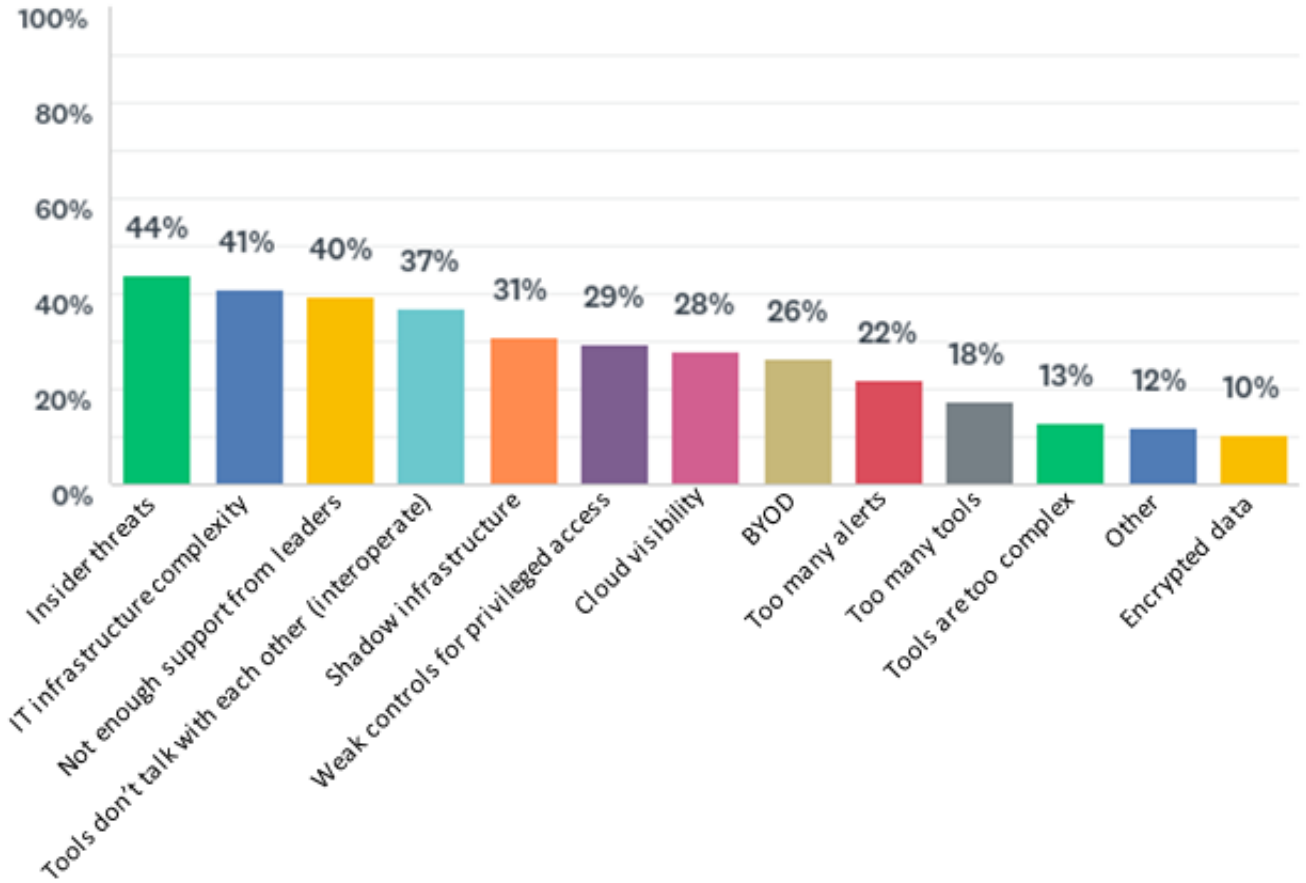


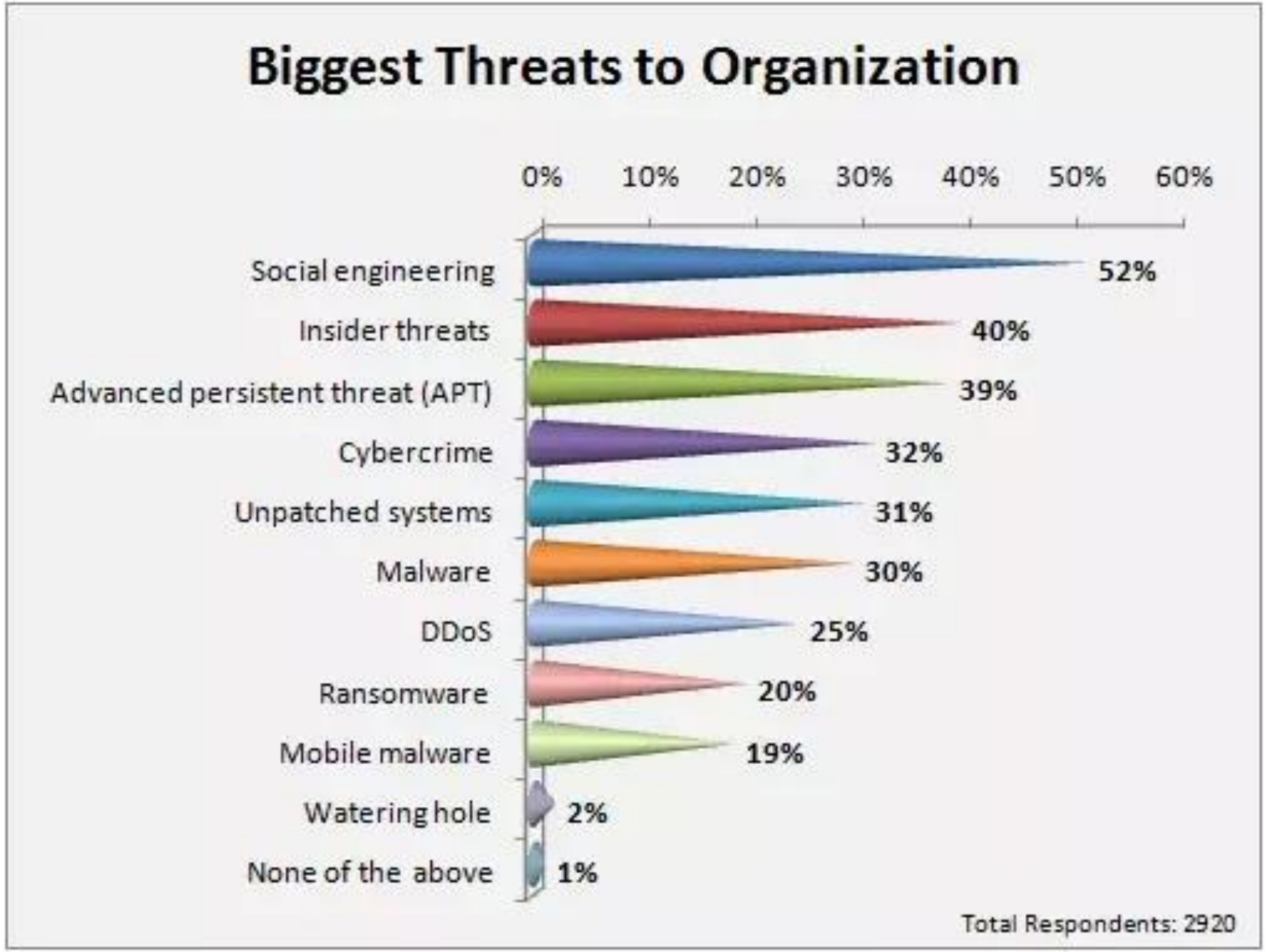
Information Security Model

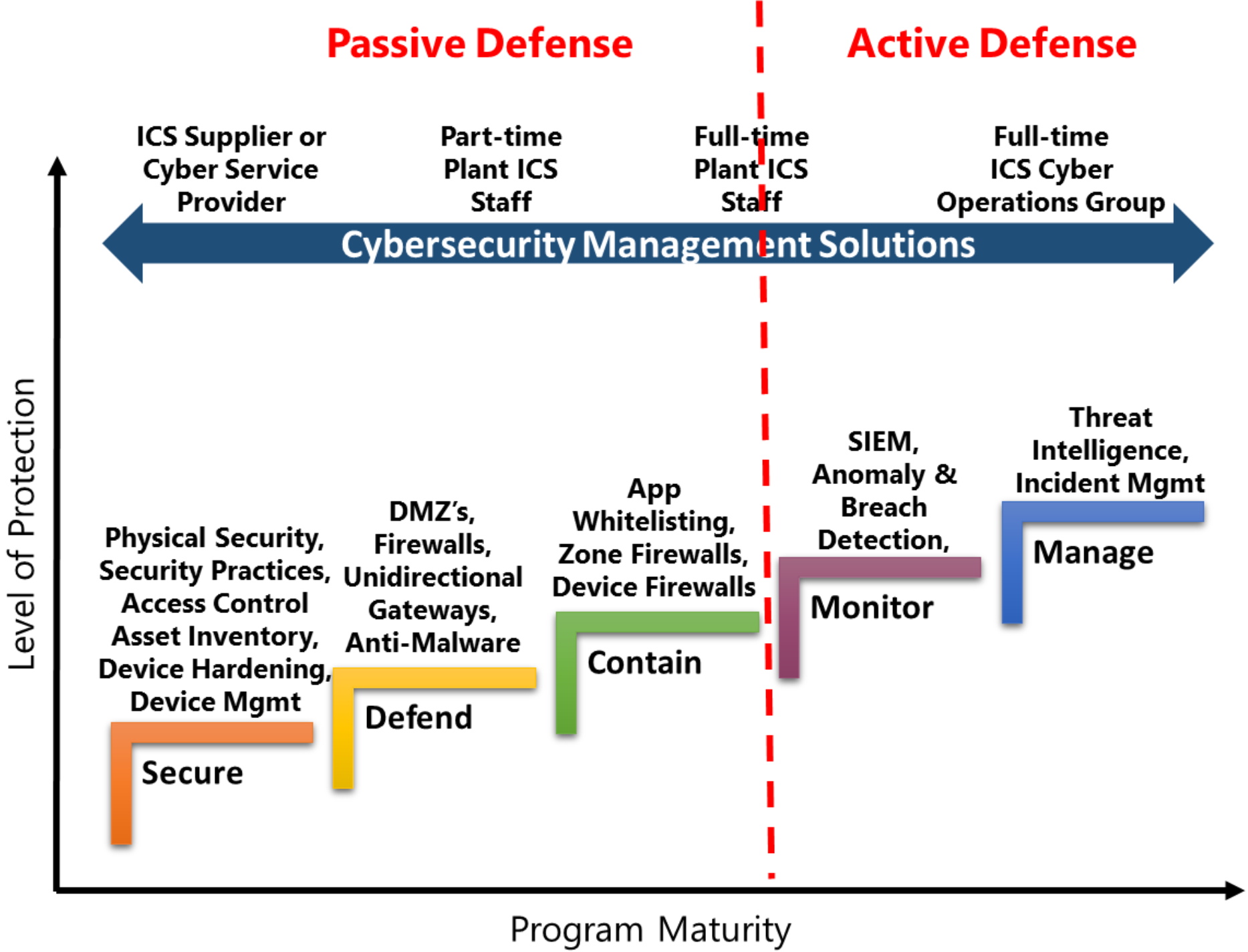


The attack life cycle of APTs

What are the top challenges in network security facing your organization?




Biggest Threats to Organization
0%
10%
20%
30%
40%
50%
60%
Social engineering
52%
Insider threats
40%
Advanced persistent threat (APT)
39%
Cybercrime
32%
Unpatched systems
31%
Malware
30%
DDoS
25%
Ransomware
20%
Mobile malware
19%
Watering hole
2%
None of the above
1%
Total Respondents: 2920


Passive Defense
Active Defense
ICS Supplier or Cyber Service Provider
Part-time Plant ICS Staff
Full-time Plant ICS Staff
Full-time ICS Cyber Operations Group
Cybersecurity Management Solutions
Level of Protection
Physical Security, Security Practices, Access Control Asset Inventory, Device Hardening, Device Mgmt
Secure
DMZ's, Firewalls, Unidirectional Gateways, Anti-Malware
Defend
App Whitelisting, Zone Firewalls, Device Firewalls
Contain
SIEM, Anomaly & Breach Detection,
Monitor
Threat Intelligence, Incident Mgmt
Manage
Program Maturity