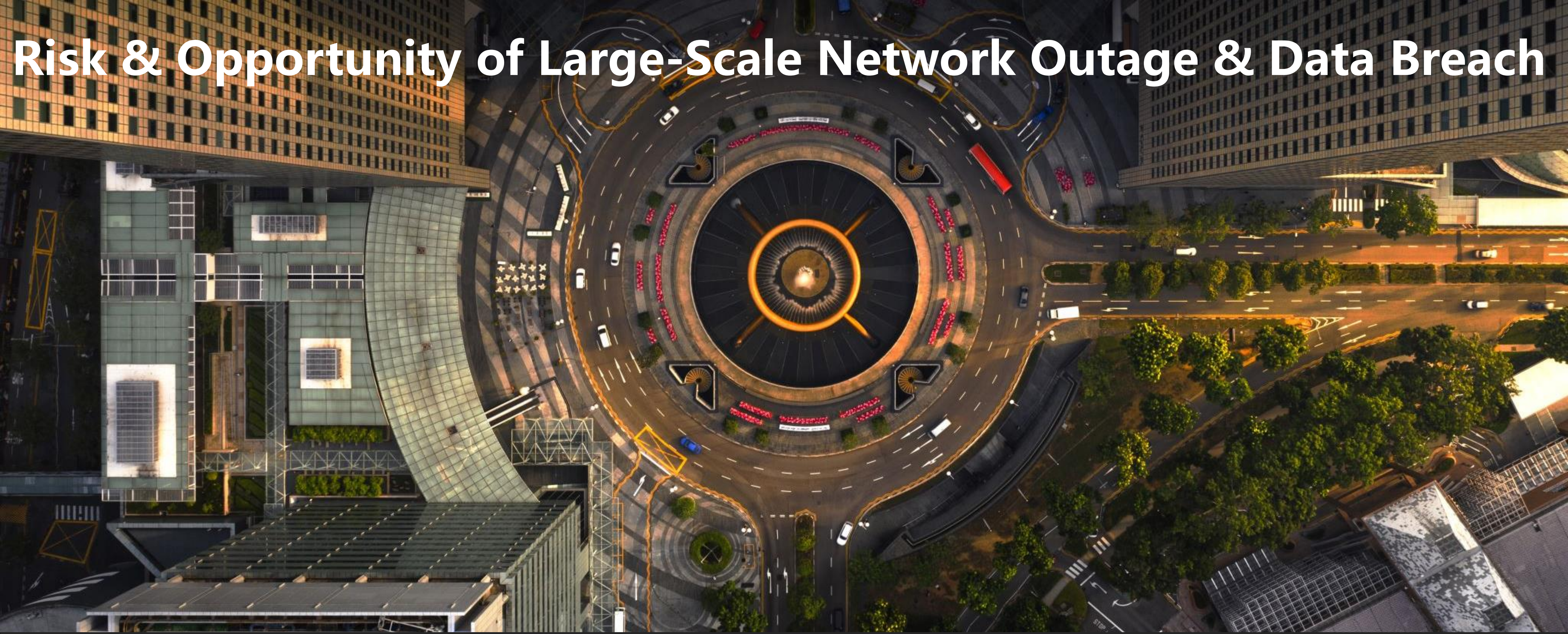
Risk & Opportunity of Large-Scale Network Outage & Data Breach

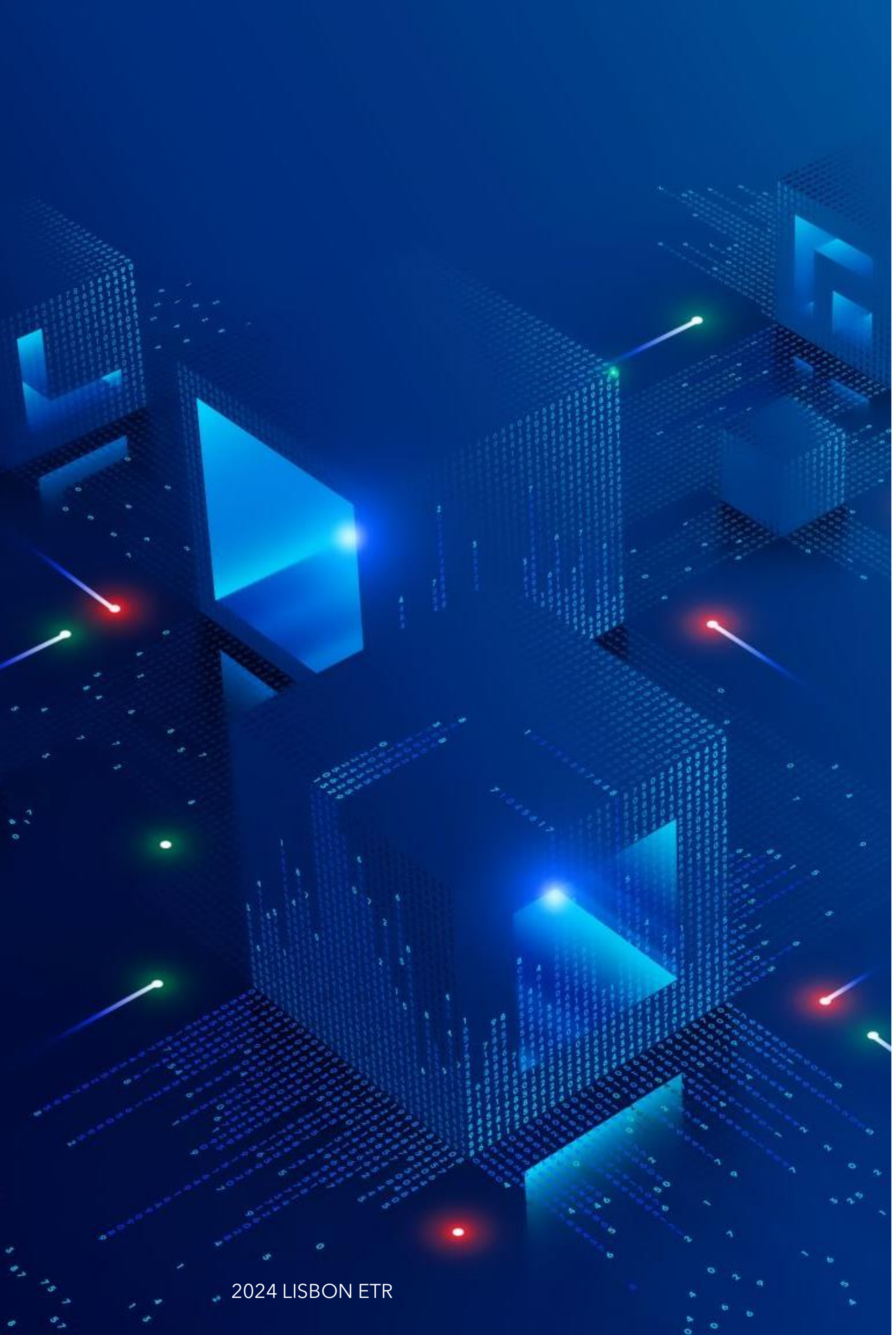


2024 IEEE CQR Emerging Technology Reliability Roundtable

LISBON, PORTUGAL, MAY 21-22, 2024

DAVID H. LU, VICE PRESIDENT (RETIRED), NETWORK SYSTEMS, AT&T

INDUSTRY EXECUTIVE CONSULTANT & VISITING PROFESSOR



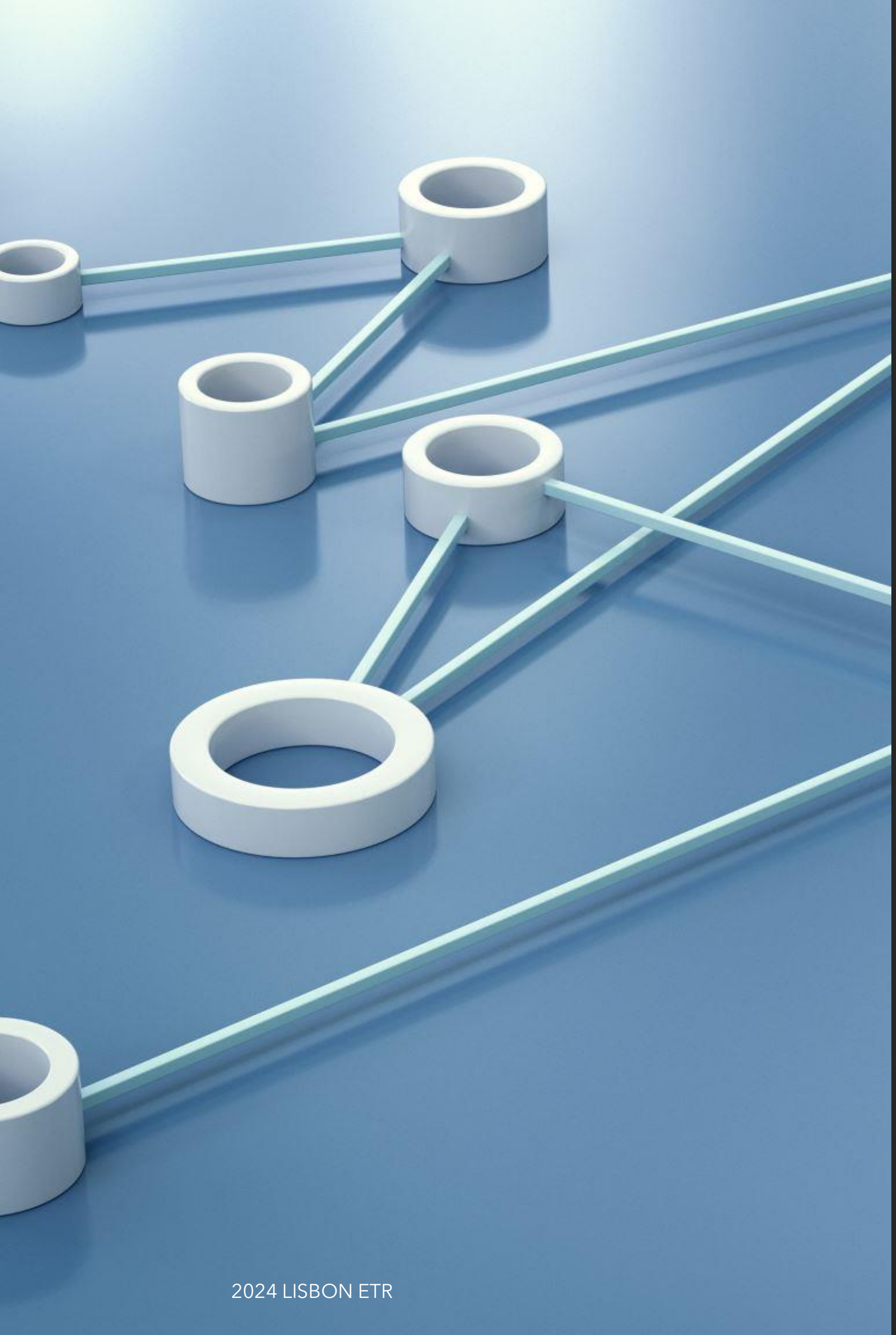
2024 LISBON ETR

Emerging Technology Impact to Communication Networks & Humanity

- Rapid development cycle with new technologies and applications.
- AI enabled technology advancements bringing new architecture and new ideas that were not possible before.
- Ecosystems are becoming much more interdependent and integrated; hence the reliability/security of each element poses enormous risk/impact to the ETE services.
- The way we live, learn, and interact with each others and devices, are changing rapidly at a pace that people may not be able to easily adopt to these changes.
- The true impact to social, economical, regulatory, global infrastructure and standards intertwined with opposing geo-political views are yet to be fully understood.

Disclaimer Statement for this talk

The following case study is based on publicly available information, and the possible root cause analysis and recommendations are based on author’s observation, hence should be used **only** as simple/general reliability and security case studies, not as actual root causes and in reference of any specific company.



Recent Industry Incident Risks & Opportunities

- ❑ Impactful network outage triggered by configuration change and worsened by operation implications that can be easily mitigated with AI driven automation.
- ❑ User Data Breach
- ❑ 2020 Christmas Nashville Bombing

Recent industry outage RCA public view & observations

- Simple but fatal manual configuration change error occurred in mobile core network cloud.
- No post change validation, or if there was, then not adequate to catch the obvious problem.
- Monitoring tools and auto-ticketing function were either turned off or not in use (delay in action).
- System generated alerts were either ignored or not picked up until it was too late.
- The architecture and routing rules allowed the traffic overload to propagated through, hence impact a large part of national footprint.

Opportunities to prevent and mitigate outage/impact!

Perform routing post CM (change mgmt) testing like any IT regression testing.

Turn on catch all “rules” for close monitoring in the period immediately following the CM – any traffic pattern discrepancies, network event anomalies, network behavior not expected, etc.

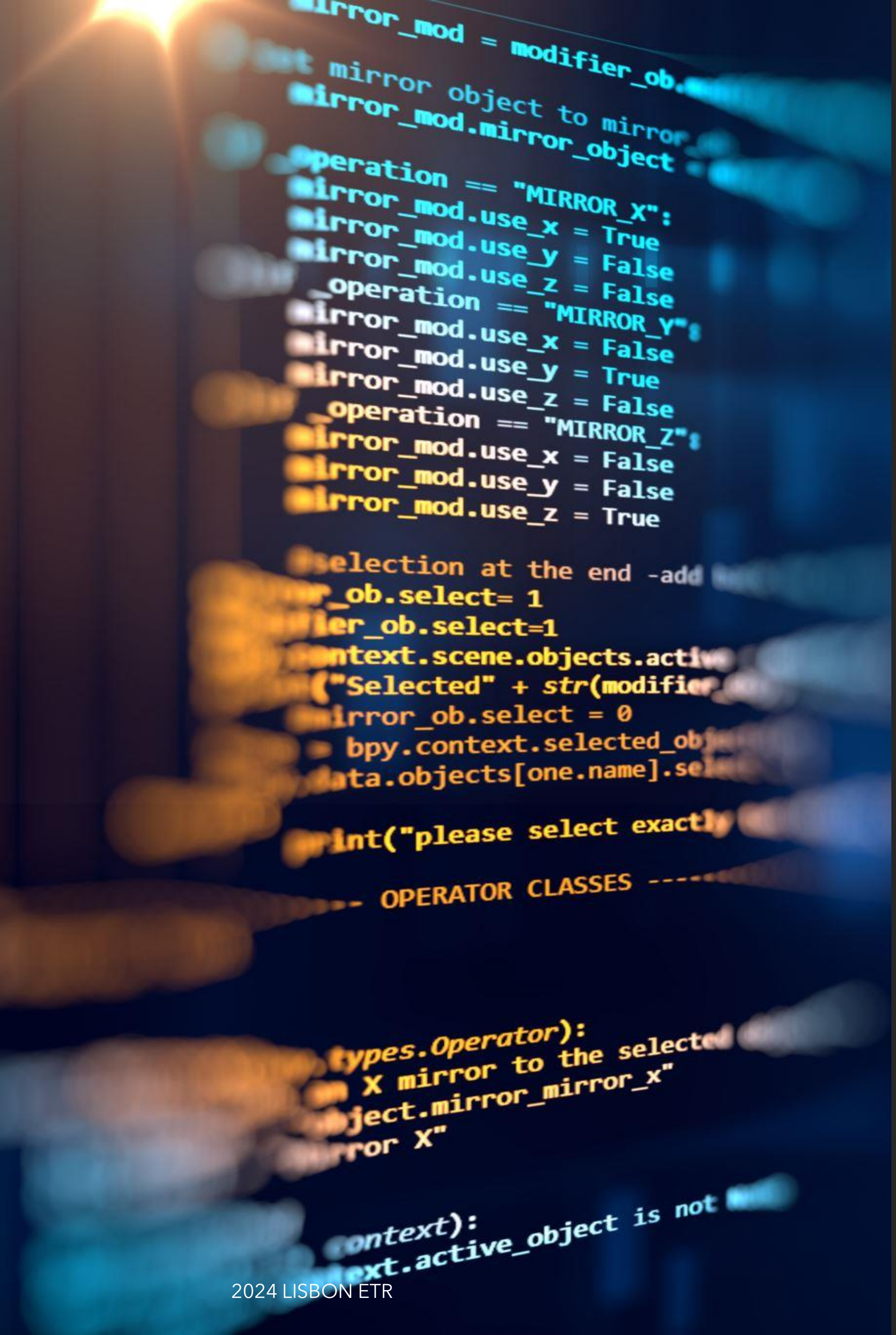
High level of alerts mandatory post CM and implement AI driven self corrections.

Any AI triggered automation would repeat the same testing and monitoring process.

Auto-traffic management to block the propagation of overload.

Strengthen network performance/traffic AI analytics to launch self-healing capabilities.

Implement new and simplified AI driven network architecture

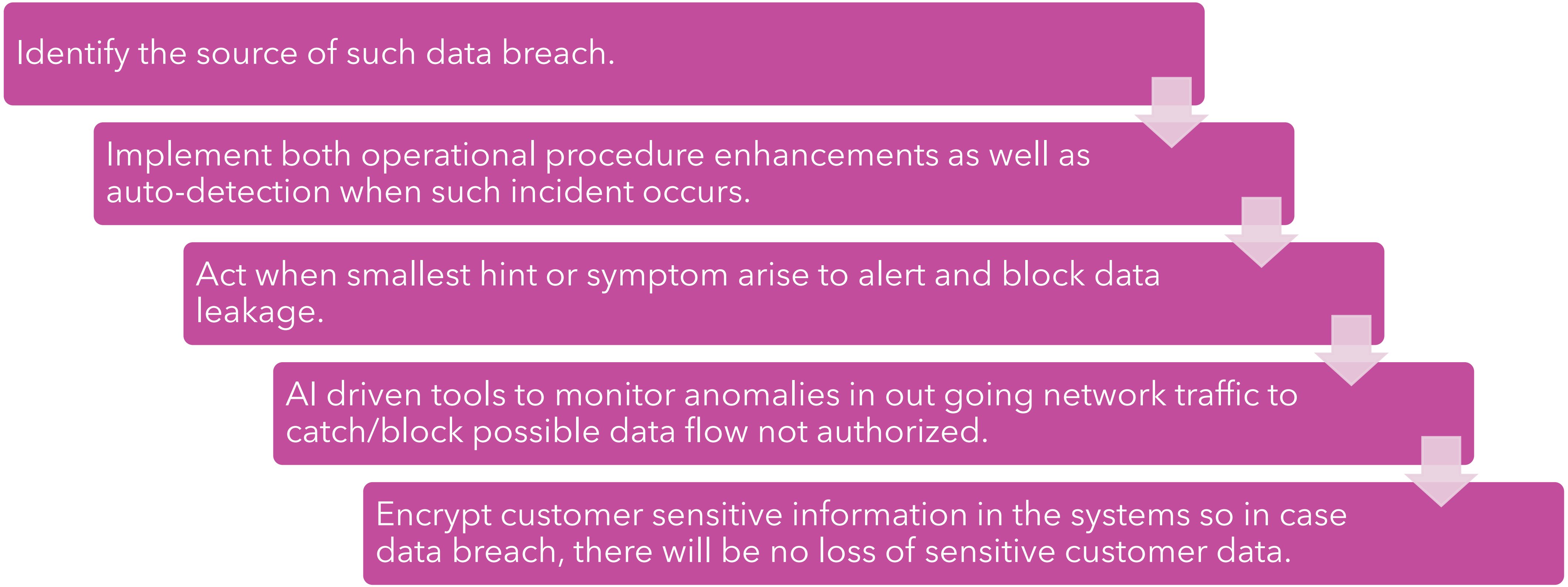


```
irror_mod = modifier_ob.
t mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

election at the end -add
_ob.select= 1
ier_ob.select=1
ntext.scene.objects.active
("Selected" + str(modifier
irror_ob.select = 0
 bpy.context.selected_ob
ata.objects[one.name].se

int("please select exactly

-- OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
ject.mirror_mirror_x"
rror X"

ontext):
xt.active_object is not
```

User Data Breach
Public View & Observations

- Millions of existing and former customer data breach to dark web.
- No source of the breach identified so far.
- Fortunately, the impact to operation was minimal and being actively investigated.
- Possible source of the data breach included vendor to the service provider, security breach to its network, or to its customer information DB, etc.
- Current cyber-security protection and monitoring mechanism in place are not adequate!
- Full impact and RCA are being performed.

Opportunity to prevent and mitigate data breach



Identify the source of such data breach.

Implement both operational procedure enhancements as well as auto-detection when such incident occurs.

Act when smallest hint or symptom arise to alert and block data leakage.

AI driven tools to monitor anomalies in out going network traffic to catch/block possible data flow not authorized.

Encrypt customer sensitive information in the systems so in case data breach, there will be no loss of sensitive customer data.

2020 Nashville Christmas Bombing

- Earlier Morning of Christmas Day, 2020.
- The explosion took away the entire wall and the building facing the street.
- The network office went out of services after battery drained due to the electrical supply damage on the wall.
- No damage to network devices and full service restored after the recovery of electrical power.
- Diversified network hub design implemented after the incident.

Open Dialog