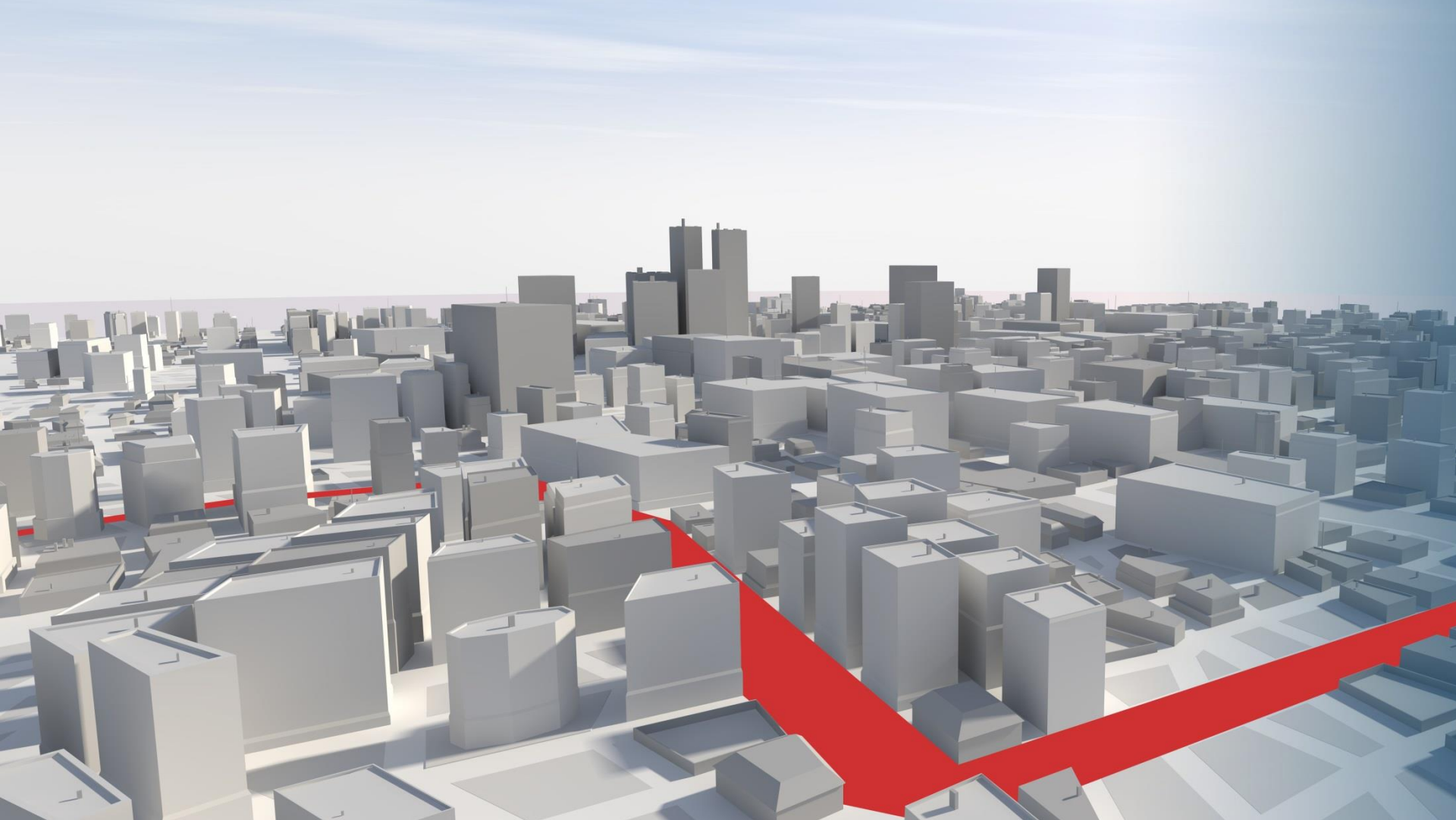
Cybersecurity Headline News - Changing the Story

Zulfikar Ramzan
Chief Technology Officer, RSA

Twitter: @zulfikar_ramzan

RSA


WALL
MAIN ST

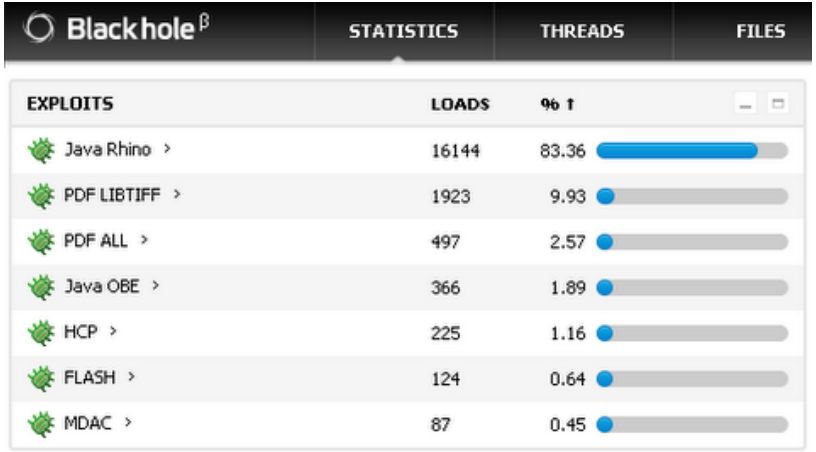



technology
operations
inflection
point


ATTACKERS HAVE
EVOLVED

Why Are Intrusions Successful?

Threats are targeted. macro-distribution supplanted by micro distribution



Powerful attack toolkits available w/ tiered pricing, 24x7 customer support


INTELLIGENCE DR
SECURITY
RSA
Got PKI?
JUNIPER

Public-Private Partnerships *Offer a* ***Constructive Opportunity*** *in our ongoing efforts to thwart common cyber-adversaries.*

*Without clearly defined **roles and responsibilities**, it's unlikely that we'll ever develop appropriate expectations of one another.*

Role of the Intelligence Community

Government Defense of Private-Sector Networks

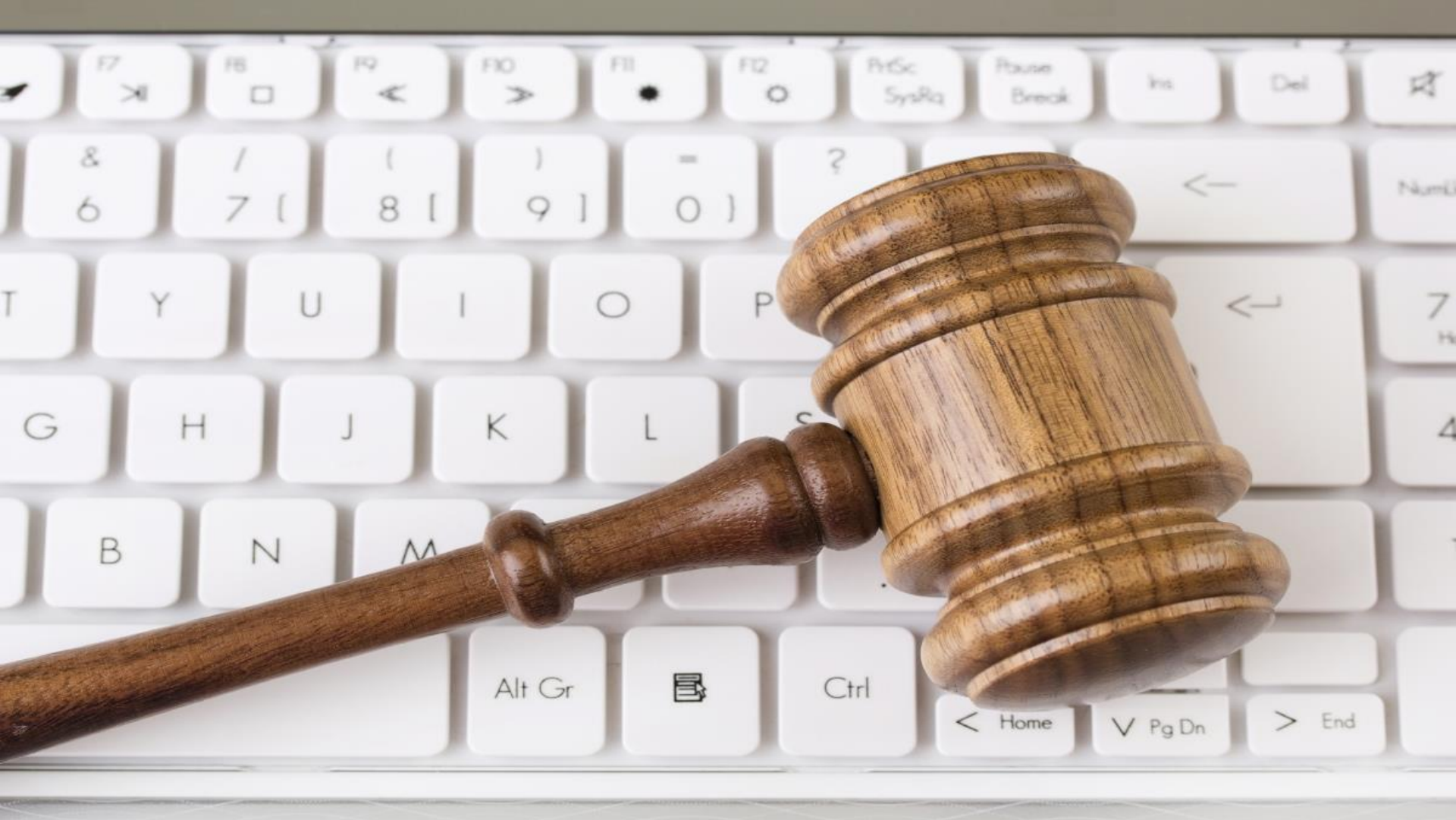
Are we truly monitoring to enable better defenses?

What is the communication chain upon compromise?

What is the decision chain around determining which traffic to block from which threat actors?

What kind of performance implications might a government defensive method introduce, in particular with respect to latency?

"the DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence…significant consequences may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact…."

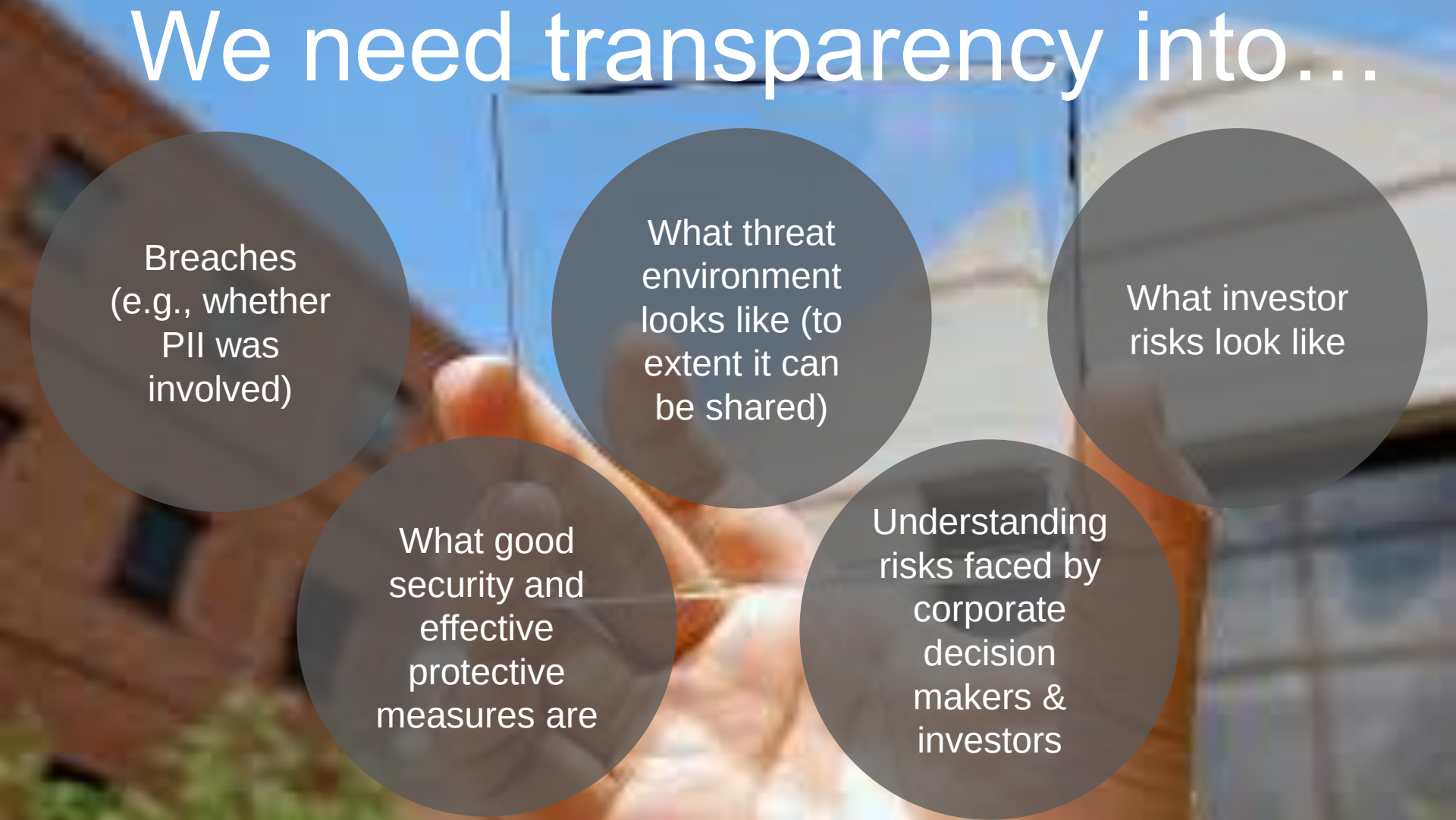

F7
F8
F9
F10
F11
F12
PrtSc
SysRq
Pause
Break
Ins
Del
&
6
/
7
(
8
)
9
=
0
?
T
Y
U
I
O
P
G
H
J
K
L
B
N
M
Alt Gr
Ctrl
Home
Pg Dn
End

< 1%

of successful advanced threat attacks are spotted by SIEM systems

Source:2014 Verizon Data Breach Investigation Report

We need transparency into…




STANDARDS

Role of the Private Sector

Take ultimate responsibility for its own cyber defenses

Develop critical technologies and drive rapid cybersecurity innovation

Be a more active participant in the cyber strategy and policy debate

Information Sharing

Who is being asked to share?

What are they being asked to share?

Specifically when and how are they being asked to share it?

How will this shared information be used?

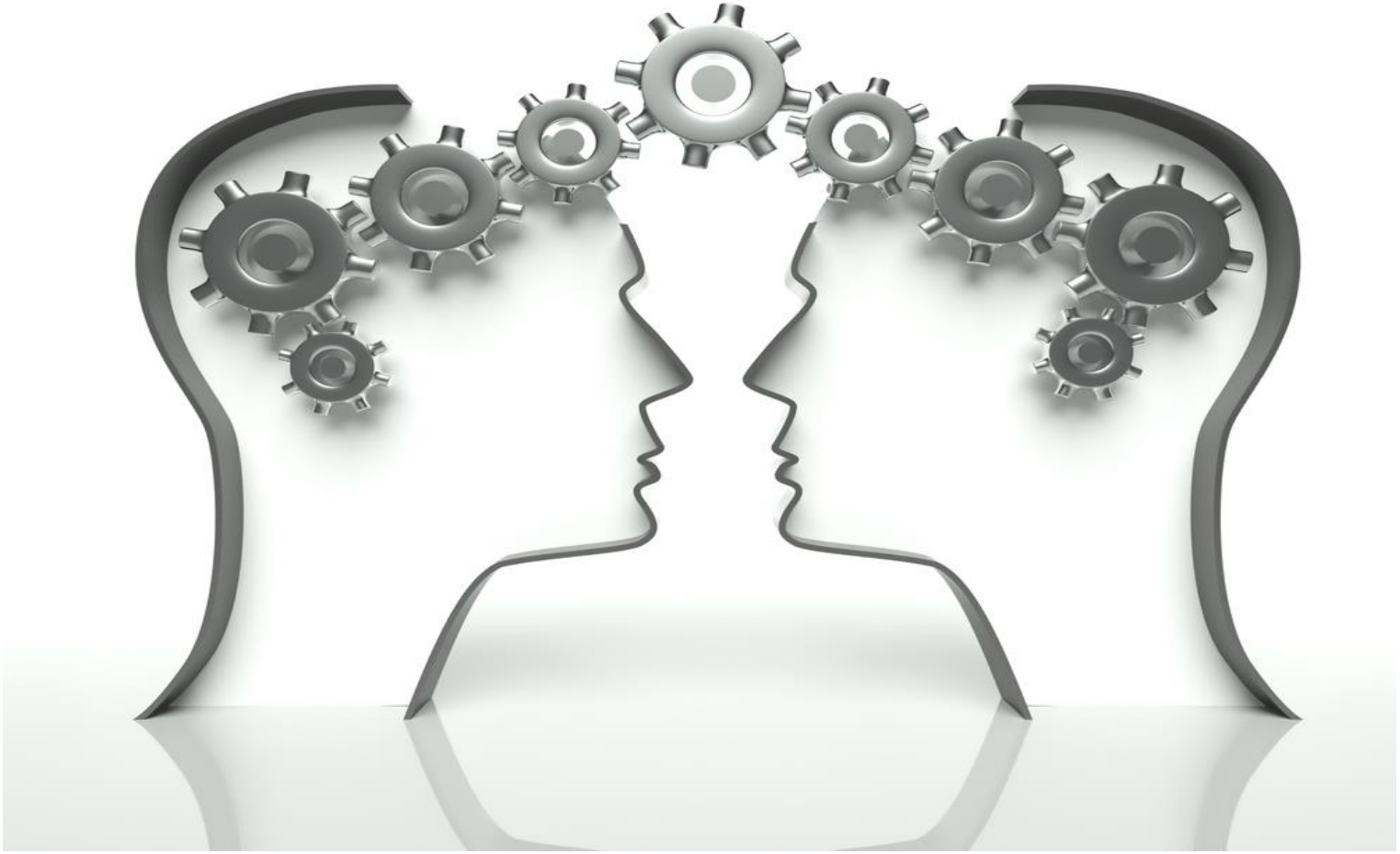
How will it be protected from disclosure, both legally and operationally?

Who will have access to it?

What are the liabilities and assurances that can be provided in support of the answers to these questions?

Why should this information be shared?

What is the value proposition for the sharing or disclosing party?



EMC²