



Cybersecurity Headline News - Changing the Story

Zulfikar Ramzan
Chief Technology Officer, RSA

Twitter: @zulfikar_ramzan



NIST Cybersecurity Innovation Forum

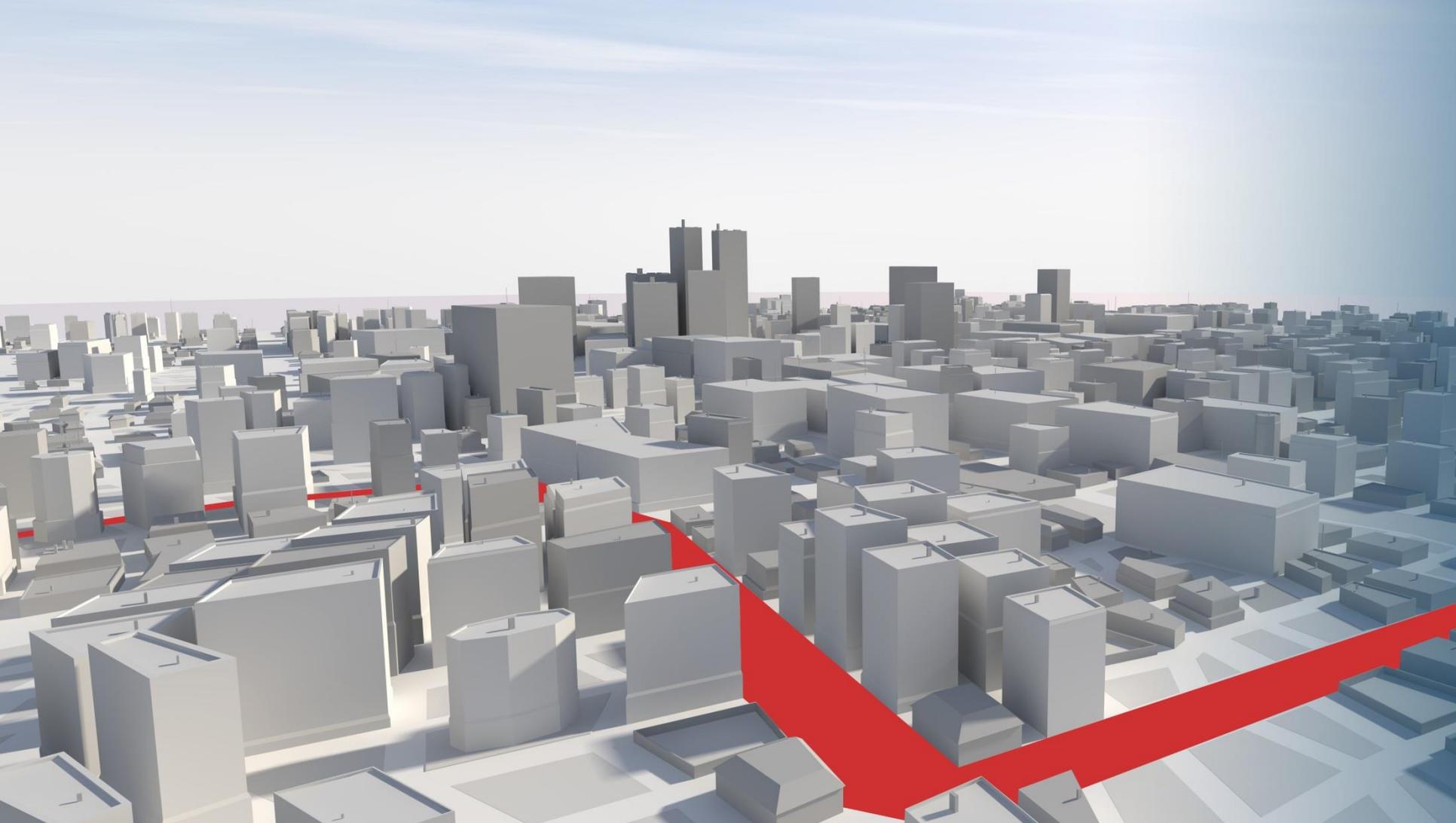


WALL ST

MAIN ST







technology
operations
inflection point
point

ATTACKERS HAVE

EVOLVED



Why Are Intrusions Successful?



*Threats are targeted.
macro-distribution
supplanted by micro
distribution*

Blackhole ^β		STATISTICS	THREADS	FILES
EXPLOITS	LOADS	% ↑		
Java Rhino >	16144	83.36	<div style="width: 83.36%;"></div>	
PDF LIBTIFF >	1923	9.93	<div style="width: 9.93%;"></div>	
PDF ALL >	497	2.57	<div style="width: 2.57%;"></div>	
Java OBE >	366	1.89	<div style="width: 1.89%;"></div>	
HCP >	225	1.16	<div style="width: 1.16%;"></div>	
FLASH >	124	0.64	<div style="width: 0.64%;"></div>	
MDAC >	87	0.45	<div style="width: 0.45%;"></div>	

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

ACCESS
REDEFINED

INTELLIGENCE DR
SECURITY

Juniper
RSA

JUNIPER
NETWORKS

JUNIPER
NETWORKS

Cafe
SAVOR...

Got PKI?



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

Improve
functionality
around attribution
in cyberspace

Establish clear
boundaries
separating
intelligence from
information
assurance efforts
for foreign
adversaries

Draw distinctions
from intelligence
objectives versus
objectives of
system operators

Government Defense of Private-Sector Networks

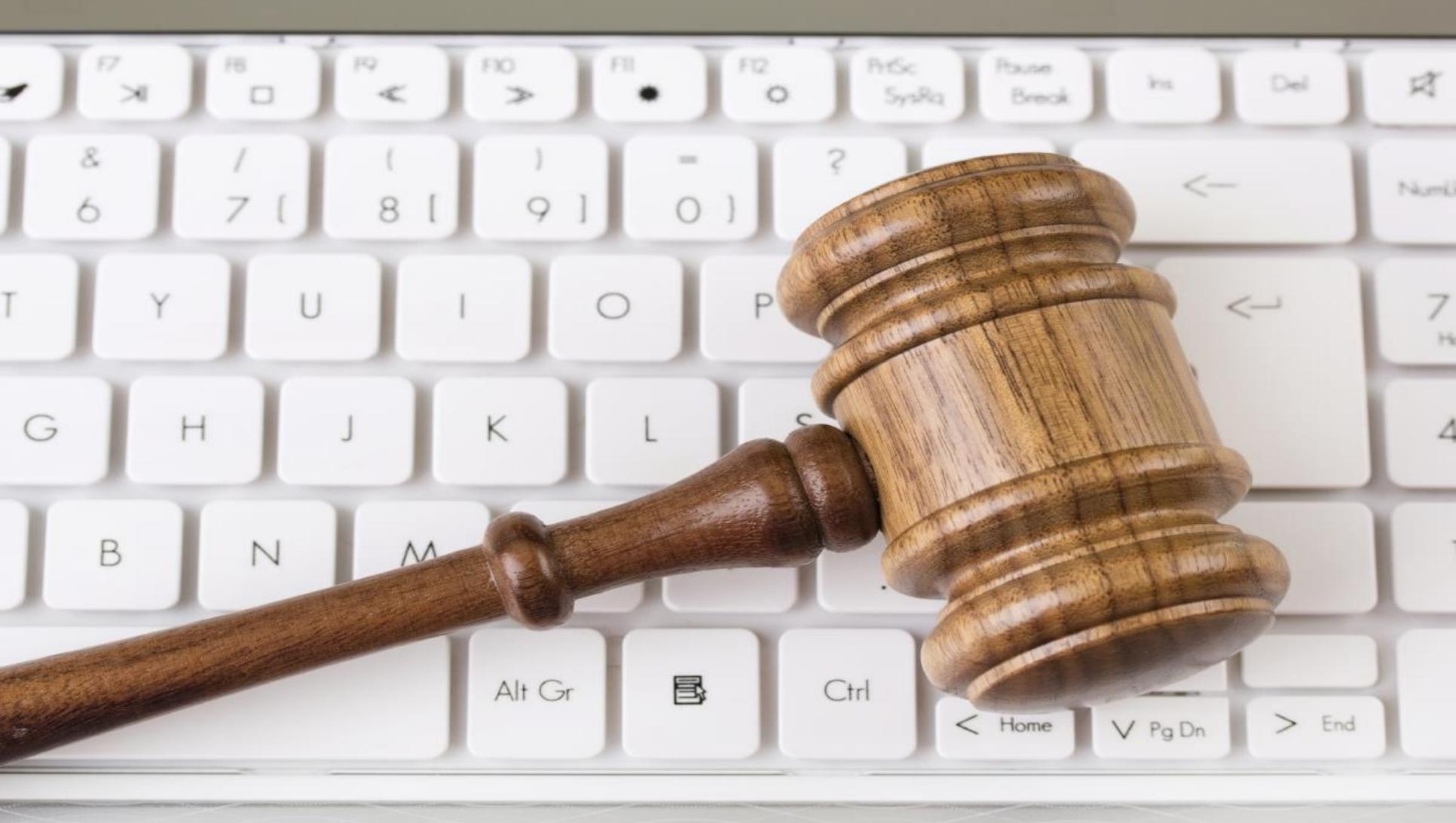
Are we truly monitoring to enable better defenses?

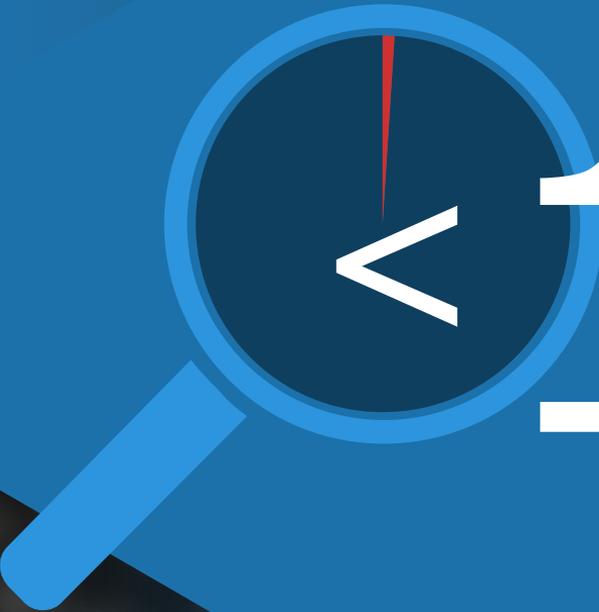
What is the communication chain upon compromise?

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...."





<

1%

of successful advanced
threat attacks are spotted
by SIEM systems

Source: 2014 Verizon Data Breach Investigation Report



We need transparency into...

Breaches
(e.g., whether
PII was
involved)

What threat
environment
looks like (to
extent it can
be shared)

What investor
risks look like

What good
security and
effective
protective
measures are

Understanding
risks faced by
corporate
decision
makers &
investors

S T A N D A R D S

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

EMC, RSA, the EMC logo and the RSA logo are trademarks of EMC Corporation in the U.S. and other countries.