Security and Compliance

Gerald Beuchelt
Chief Security Officer

Demandware, Inc.

600+ Active eCommerce Sites

150+ Customers

13 Data Center Locations

16M+ Items Processed Monthly

Security and Compliance

Why Compliance?

PCI-DSS 2.0

PA-DSS

SSAE16

Service Organization Controls (SOC)

ISO 2700x

Inhibitors and Enablers

Other Frameworks

Cobit

NIST

FFIEC

SEI CMM

Concerns: North America

Concerns: Europe

Concerns: Asia/Pacific Rim

Is it enough?

Static vs. Dynamic Threat Assessment

Compliance vs.
Risk Management

Threat Actors

Threats

Vulnerability

Exploit

Risk

Risk = Likelihood x Impact

(of threat having detrimental effect on organization)

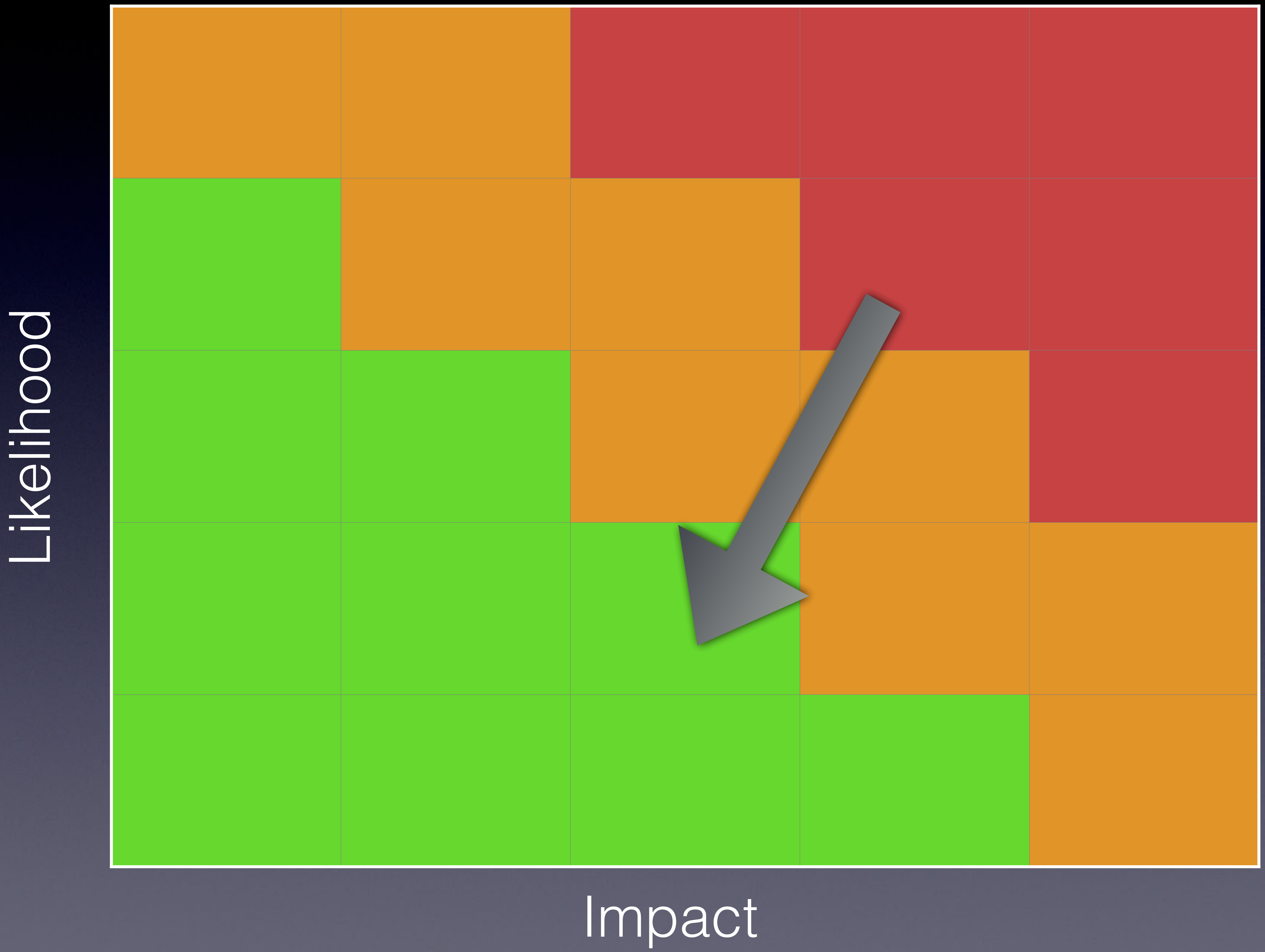
Risk Heat Map

Likelihood

🟧	🟧	🟥	🟥	🟥 Very High
🟩	🟧	🟧	🟥 High	🟥
🟩	🟩	🟧 Medium	🟧	🟥
🟩	🟩 Low	🟩	🟧	🟧
🟩 Very Low	🟩	🟩	🟩	🟧

Impact

Risk Mitigation



Alternative Risk Treatments

Avoidance

Transfer

Acceptance

Example - Fashion Retailer:

DDoS by Anonymous

'Retaliation' for Bangladesh

Risk Treatment Plan:

Lower Profile

Heighten Defenses

Residual Risk

Risk Management in

Information Assurance

Augmenting Controls

Q&A