J. W. Mayo
CONSULTING

jwmc-llc.com

Tao of Risk – The Art of Cyber Security

Joseph W. Mayo

J. W. Mayo Consulting, LLC

joseph.mayo@jwmc-llc.com

Agenda

- Nefarious Threat Impact
- How Do We Manage This Risk?
- Build a Culture of Resilience

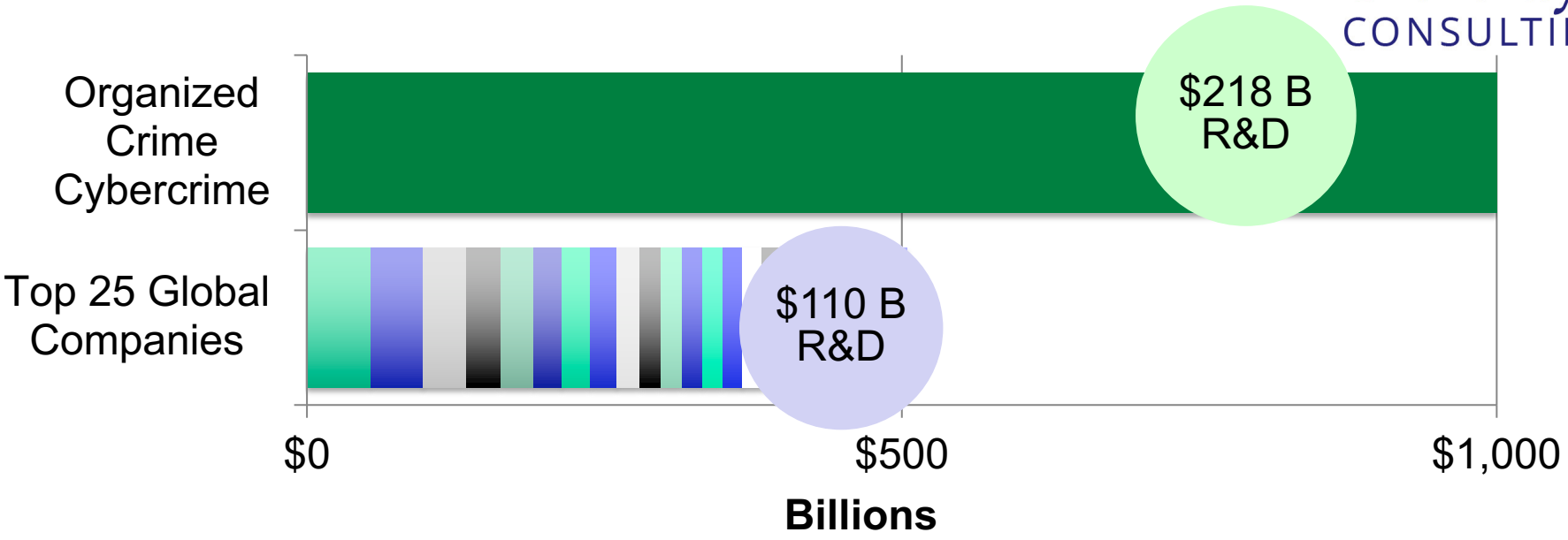
joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Nefarious Threat Impact

joseph.mayo@jwmc-llc.com

Well Capitalized Threat



- Apple
- Agricultural Bank of China
- JP Morgan Chase
- Verizon Communications
- Alphabet
- Bank of America
- Wal-Mart
- IBM
- ICBC
- Bank of China
- Wells Fargo
- Novartis
- Samsung Electronics
- Citi Group
- HSBC Holdings
- Bank of Communications
- China Construction Bank
- Berkshire Hathaway
- Toyota
- China Mobile
- Exxon Mobile
- Johnson & Johnson
- AT&T
- Microsoft

joseph.mayo@jwmc-llc.com

Well Capitalized Threat

- 1 kilo of fentanyl produces 500,000 pills
  - Street value of 1 pill is ~$30
- 50-60 kilos per day
- 44 ports of entry (POE)
- 50 kilos * 500,000 pills *44 POEs * 365 = $13.9T
- US annual GDP is $20.9T

- Does not include revenue from cocaine, heroin, counterfeit products, human trafficking, etc.

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

How Do We Manage the Risk?

joseph.mayo@jwmc-llc.com

How Do We Manage the Risk?

J. W. Mayo CONSULTING

- Accept the fact that we can't buy our way out of the problem
- Accept the fact that the perimeter will be breached
  - Be prepared for this inevitability
- If you can imagine it, the Threat has the money to do it
- We must think differently

joseph.mayo@jwmc-llc.com

How Do We Manage the Risk?

- Be proactive instead of reactive, focus on “What’s next”
- Sun Tzu
  - Security against defeat implies defensive tactics; ability to defeat the enemy means taking the offensive.
    - Defense avoids losing
    - Offense allows winning
- Expect that the perimeter will be compromised
- Anticipate the unexpected
- Consider the art of the possible, focus on resiliency

joseph.mayo@jwmc-llc.com

Be Proactive

J. W. Mayo CONSULTING

- Use fault injection to test cyber capabilities
- Spearfish to measure training effectiveness
- Cyber Monday approach
- Crack passwords to measure policy compliance & training effectiveness
- Honeypots
- Honeynet
- Predictive threat analysis using Big Data and AI

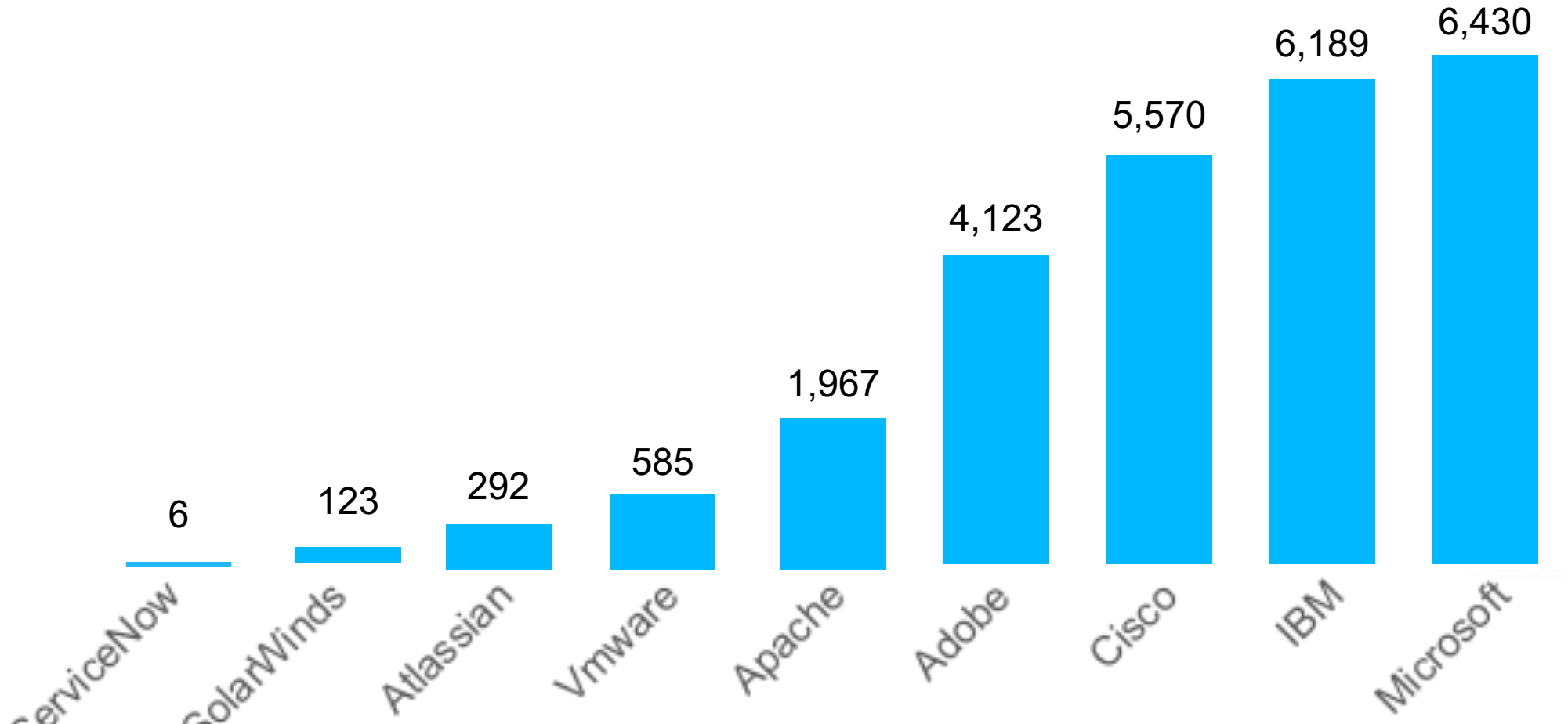
joseph.mayo@jwmc-llc.com

Be Proactive

- Reimagine detective controls
  - Forward-deploy detective controls
  - Collective learning is a form of detective controls
- Do not write off anomalies, consider them near-misses
  - At least 3 NotPetya variants were observed between April 2016 and June 2017

joseph.mayo@jwmc-llc.com

Common Vulnerability Enumeration (CVE)



joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Build a Culture of Resilience

joseph.mayo@jwmc-llc.com

A Resilience Culture

J. W. Mayo CONSULTING

- What is culture?
  - HP example
  - Keane example
- Most breaches are not intentional and are caused by poor personal security hygiene
  - Outreach
  - Training

joseph.mayo@jwmc-llc.com

Resilience Culture

- Build a culture
  - Tone at the top is critical
  - Identify and cultivate champions
    - Never pre-judge who your champions are
  - Have contests
  - Reward appropriate behavior
  - Practice collective learning w/industry
- Culture can be fragile

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Conclusion

joseph.mayo@jwmc-llc.com

Conclusion

- Bad guys are extremely well capitalized, we can't outspend them
- Threats will continue to evolve their tools, techniques, and tactics
- Culture will transcend platforms, software, and tactics
- Layered defense that includes hardware, software, and culture is key
- Risk based approach maximizes limited resources
- Focus on "what's next" instead of "here and now"

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Live Content Slide

When playing as a slideshow, this slide will display live content

Social Q&A for ISACA Maryland Chapter Virtual Conference

joseph.mayo@jwmc-llc.com

J. W. Mayo CONSULTING

Thank You!

• • •

Joseph W. Mayo

CMMI Associate, PMP, PMI-RMP, CRISC, RIMS-CRMP

joseph.mayo@jwmc-llc.com

@TaoOfRisk