

Unconventional

Observations Born From BlackHat

Dan Jacobs

Senior Security Architect, GSA TTS



1/ whoami

2/ whois

3/ BlackHat Journey



“The strangest thing about security is that it so rarely has anything to do with security.”

- Bruce Schneier, BlackHat 2003



“The strangest thing about security is that it so rarely has anything to do with security.”

- Bruce Schneier, BlackHat 2003

Takeaway: Sometimes the best security solution is not a security solution at all.



“Computers and computer security is viewed incorrectly as a "technical issue" that is better left to the technicians. Several of the common errors we find in our security testing, and how these technical issues are actually human errors...”

- Keith Rhodes, BlackHat 2003



“Computers and computer security is viewed incorrectly as a "technical issue" that is better left to the technicians. Several of the common errors we find in our security testing, and how these technical issues are actually human errors...”

- Keith Rhodes, BlackHat 2003

Takeaway: Many of problems we face as a security community are not technical - they are human.



“Cooperation across competitors and researchers can be indeed be very productive.”

- Dan Kaminsky, BlackHat 2008



“Cooperation across competitors and researchers can be indeed be very productive.”

- Dan Kaminsky, BlackHat 2008

Takeaway: Agencies operating in a vacuum should expect to suffocate.



UNIVERSITY OF
CAMBRIDGE

— DEPARTMENT OF —
COMPUTER SCIENCE
AND TECHNOLOGY

“Many interesting and important new applications of game theory have been discovered over the past 5 years in the context of research into the economics of information security. **Many systems fail not ultimately for technical reasons but because incentives are wrong.**”

- Anderson, Moore, 2007



UNIVERSITY OF
CAMBRIDGE

— DEPARTMENT OF —
COMPUTER SCIENCE
AND TECHNOLOGY

“Many interesting and important new applications of game theory have been discovered over the past 5 years in the context of research into the economics of information security. **Many systems fail not ultimately for technical reasons but because incentives are wrong.**”

- Anderson, Moore, 2007

Takeaway: Take time to question if the incentives are aligned to your goals.

5/ tail

In your cloud security journey, the greatest challenge may be to change the narrative away from incentivizing product-heavy, siloed security models (which might look good on dashboards) and toward outcome-based, cooperative systems directly aimed at relevant threats.

Thanks!

Contact me: daniel.jacobs@gsa.gov

Contact us: connectcoe@gsa.gov

Work Together: coe.gsa.gov

