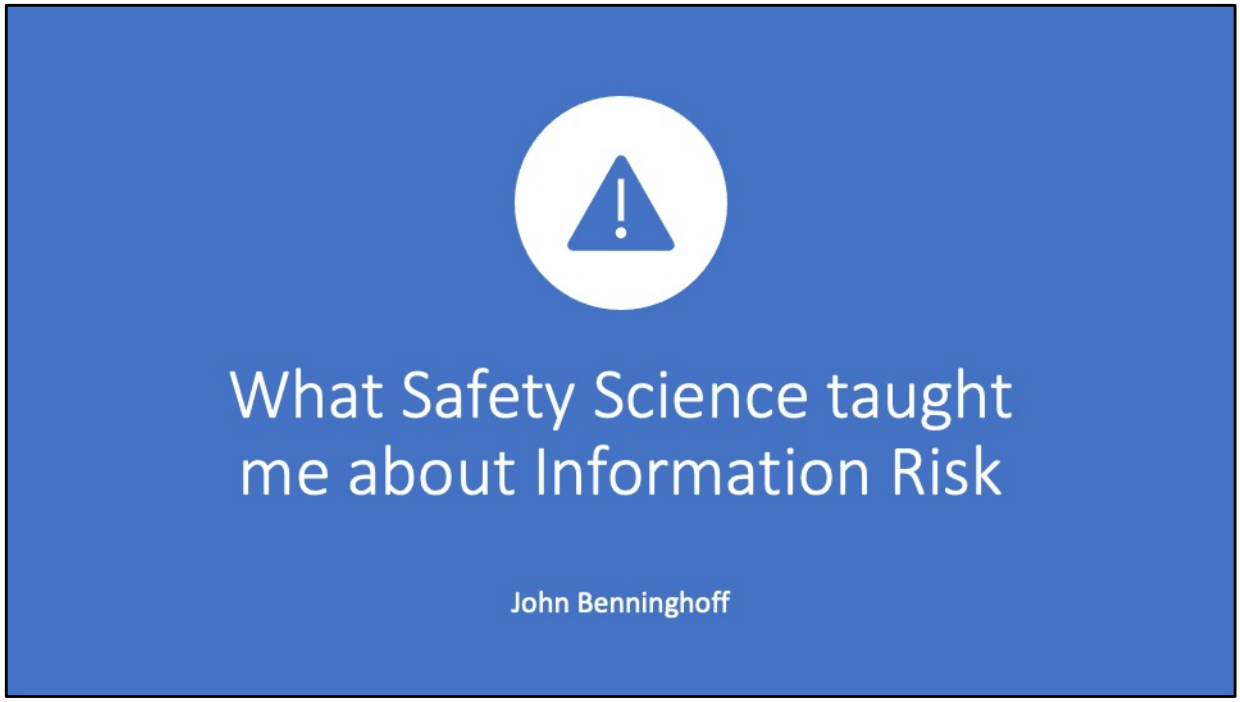
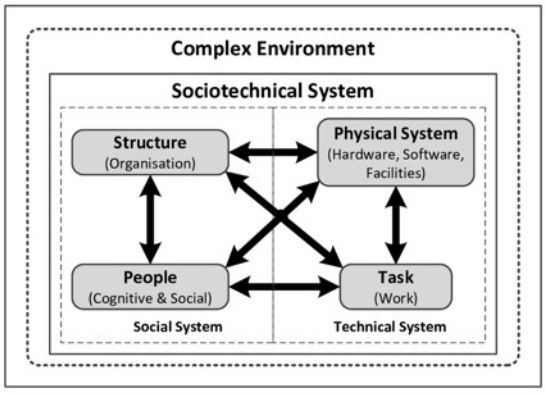


Hello, I'm John Benninghoff, and I lead the Site Reliability Engineering team at Cigna; before that, I led the Application Security Team.

Talk: https://societyinforisk.org/page-18117#Benninghoff21

What's my story? Me on upper left, wife Jolene and our dog Gertie. Started security after attending SANS Network Security 1998. First spoke about applying safety to technology at 1st conference of the Society of Information Risk Analysts 2012. MSc in safety science (managing risk and systems change) 2018-2021.

SANS: https://www.sans.org
SIRA: https://societyinforisk.org, SIRACon 2012: https://vimeo.com/44519848
TCD: https://psychology.tcd.ie/postgraduate/msc-riskandchange/, image: https://commons.wikimedia.org/wiki/File:Trinity_college_library.jpg



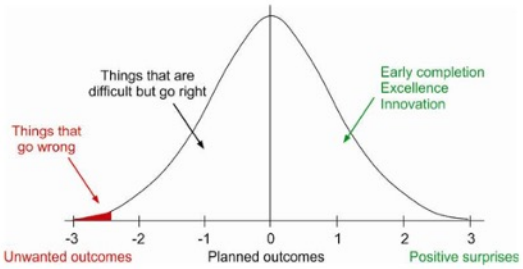


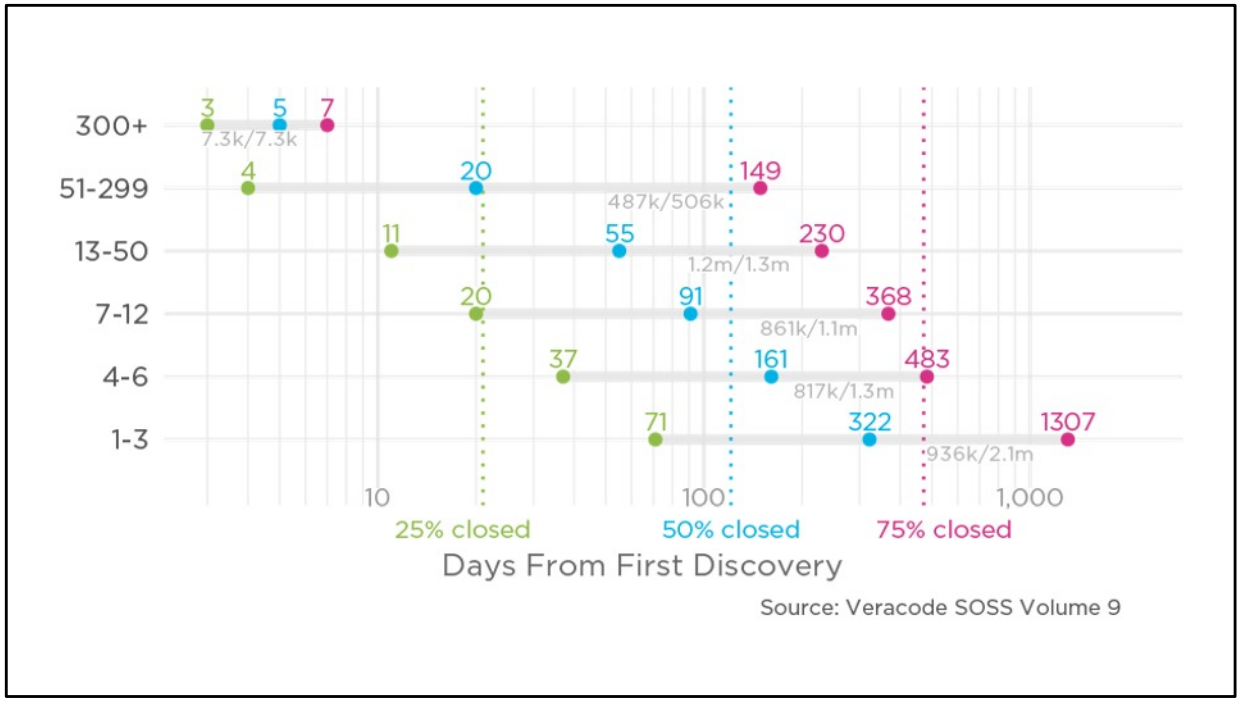
Figure 9: Event probability and safety focus

Some ideas from safety science: organizations are sociotechnical systems. all failures are systems failures. resilience improves through performance.

Resilient systems fail less often and recover faster
We can't have a science of non-events, and must instead study the full range of performance, 'working safely (or securely')
We don't care about how many breaches, only that the system resists threats and recovers faster (since we don't control the environment), "how do we defend better?"
Thus, we need to improve the security performance of the system (we also don't care about component performance, only performance of the system as a whole; stopping a phishing email from installing malware vs stopping a person from clicking the link
Shifts from managing risk to managing performance
Forsgren, Google DORA research – also shows how performance in productivity, reliability, availability and security all move *together.* In my own research, I've found that the best teams do *everything* right (there is no trade-off)!

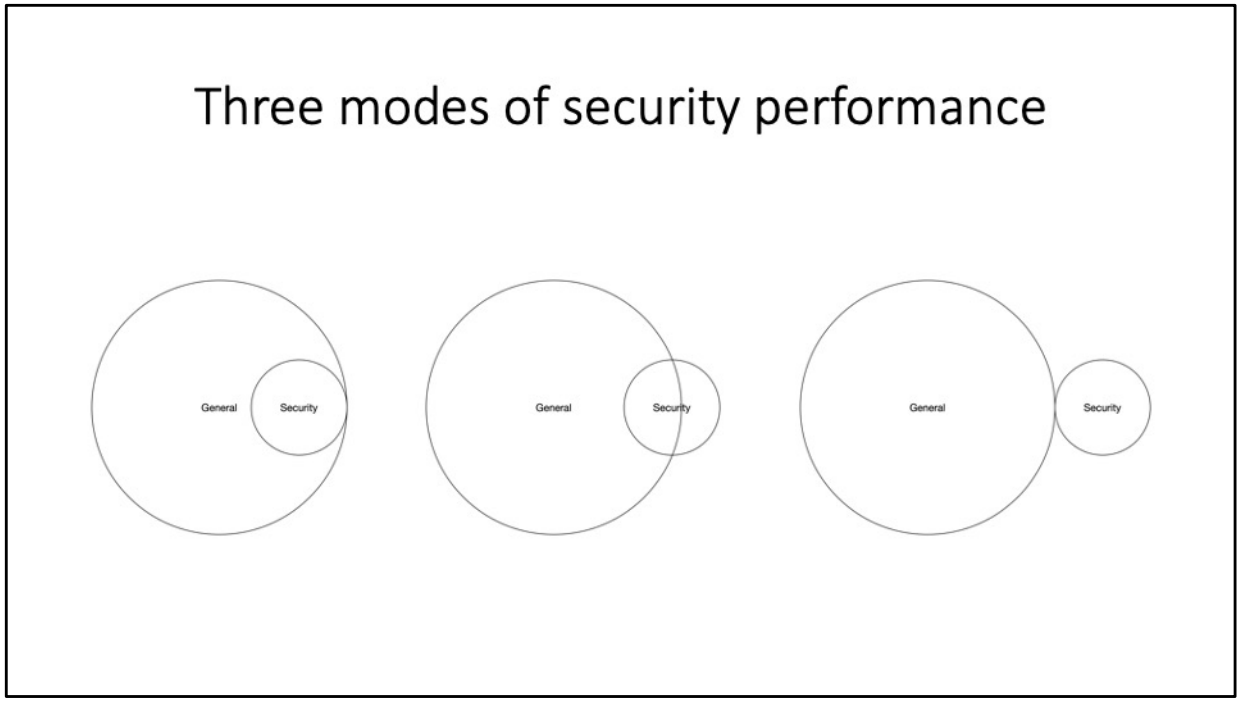
STS: https://en.wikipedia.org/wiki/Sociotechnical_system, image:

https://www.researchgate.net/publication/306242078_Assessing_the_impact_of_new_technology_on_complex_sociotechnical_systems
Cook, R. I. (1998). *How complex systems fail*. Cognitive Technologies Laboratory, University of Chicago. https://www.researchgate.net/publication/228797158_How_complex_systems_fail
Leveson, N. (2011). *Engineering a safer world : systems thinking applied to safety*. MIT Press. https://mitpress.mit.edu/books/engineering-safer-world
Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering : concepts and precepts*. Ashgate.
Hollnagel, E. (2014). Is safety a subject for science? Safety Science, 67, 21-24. https://doi.org/10.1016/j.ssci.2013.07.025
Hollnagel, E., Wears, R. L., & Braithwaite, J. (2015). From Safety-I to Safety-II: a white paper. The resilient health care net: published simultaneously by the University of Southern Denmark, University of Florida, USA, Macquarie University, Australia. (image 2)
Forsgren, N., Humble, J., & Kim, G. (2018). Accelerate : the science behind DevOps : building and scaling high performing technology organizations (First edition. ed.). IT Revolution.
Forsgren, N., Smith, D., Humble, J., & Frazelle, J. (2019). 2019 Accelerate State of DevOps Report. DORA & Google Cloud. https://research.google/pubs/pub48455/



What evidence is there that shows a link between better performance and better security?
The “wow!” plot: Veracode SOSS graphic shows how frequent testing (general performance) is correlated with security performance (faster closure)
Y axis shows the number of scans per year
X axis shows how many days it takes to close 25/50/75% of vulns

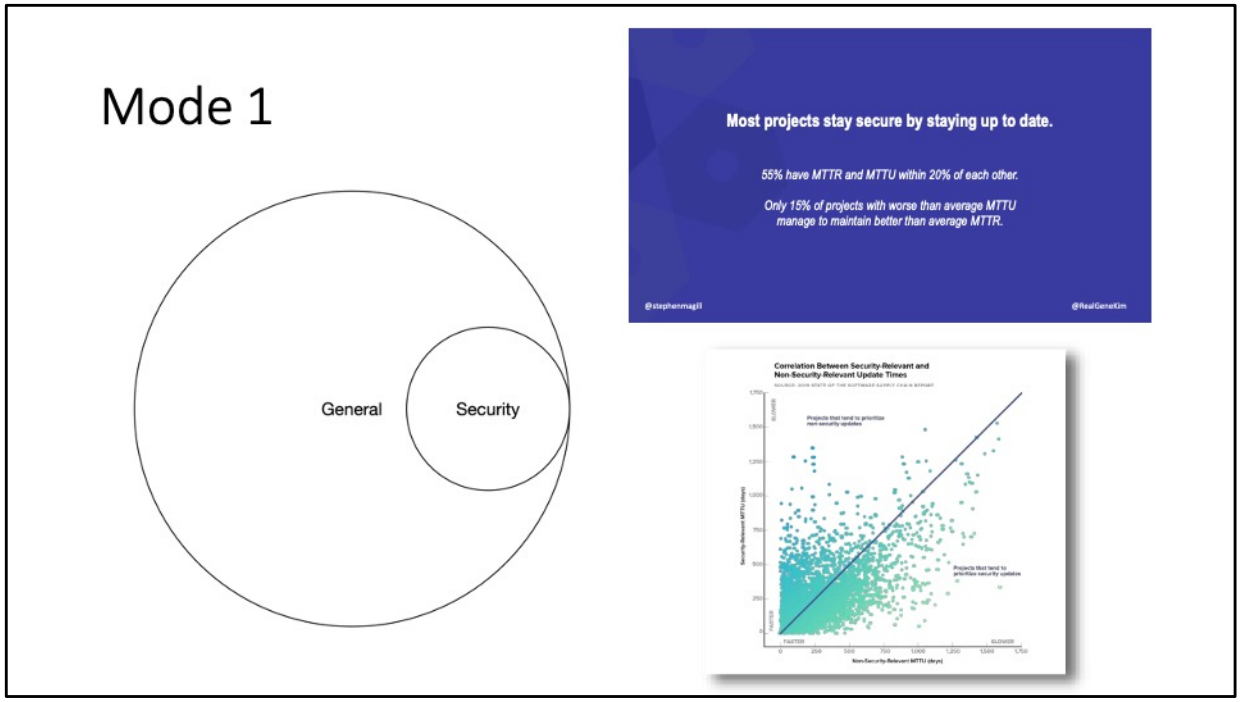
Veracode. (2019). State of Software Security Volume 9. https://www.veracode.com/sites/default/files/pdf/resources/ipapers/state-of-software-security-volume-9/index.html



The model is an attempt to explain the relationship between general performance on technology activities, and provide insights to improving performance (and thus working securely)
How do we fit in with the larger picture?

Mode 1: Security is entirely contained within general performance
Mode 2: Security is partly outside of general performance
Mode 3: Security is entirely outside of general performance

Over time, performance transitions from mode 3 to mode 2 to mode 1 (really, general performance grows and absorbs security)
Transition of vulnerability management to automated upgrades over time

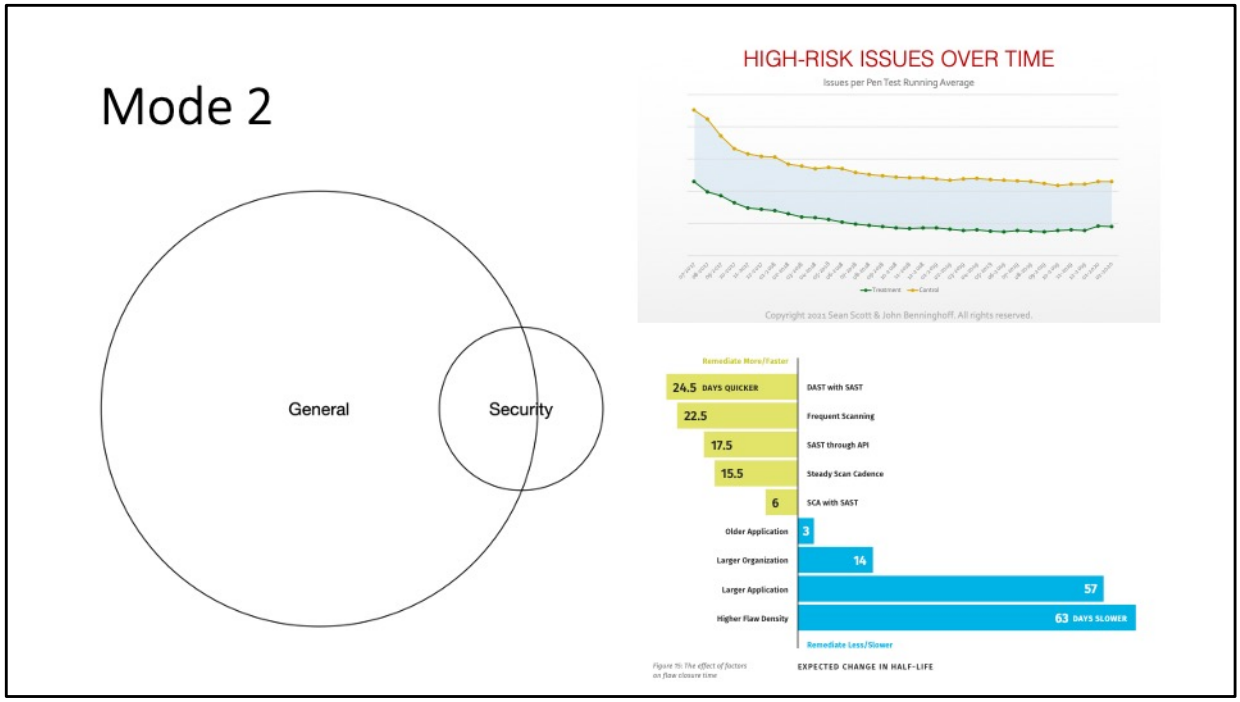


Gene Kim work with Stephen Magill: Java dependencies in Maven ecosystem, security is achieved through staying up to date
That is, good security is a side effect of good maintenance, not a separate activity
2021 Security Outcomes: the biggest factor in security program success: proactive refresh of technology.
As does Jay Jacobs' work on the correlation between SSL/TLS vulnerabilities and likelihood of breach. (which reflected **maintenance**)

<u>Implications</u>
Org: shift responsibility for patches and dependencies to engineering teams; then your VM program becomes an indicator of your maintenance performance
You: start with maintenance! Begin your day by updating your homebrew, applying updates. Start development by updating dependencies.
Challenge: "what about solarwinds?" supply chain management is a mode 3 activity

Magill, S., & Kim, G. (2019). A data-driven look at practices behind exemplar open source projects. https://www.youtube.com/watch?v=YoWkuFzEYFs
sonatype, galois, & IT Revolution. (2019). 2019 State of the Software Supply

Chain. https://www.sonatype.com/en-us/2019ssc
The 2021 Security Outcomes Study. (2020). Cisco, YouGov, Cyentia. https://www.cisco.com/c/en/us/products/security/security-outcomes-study.html

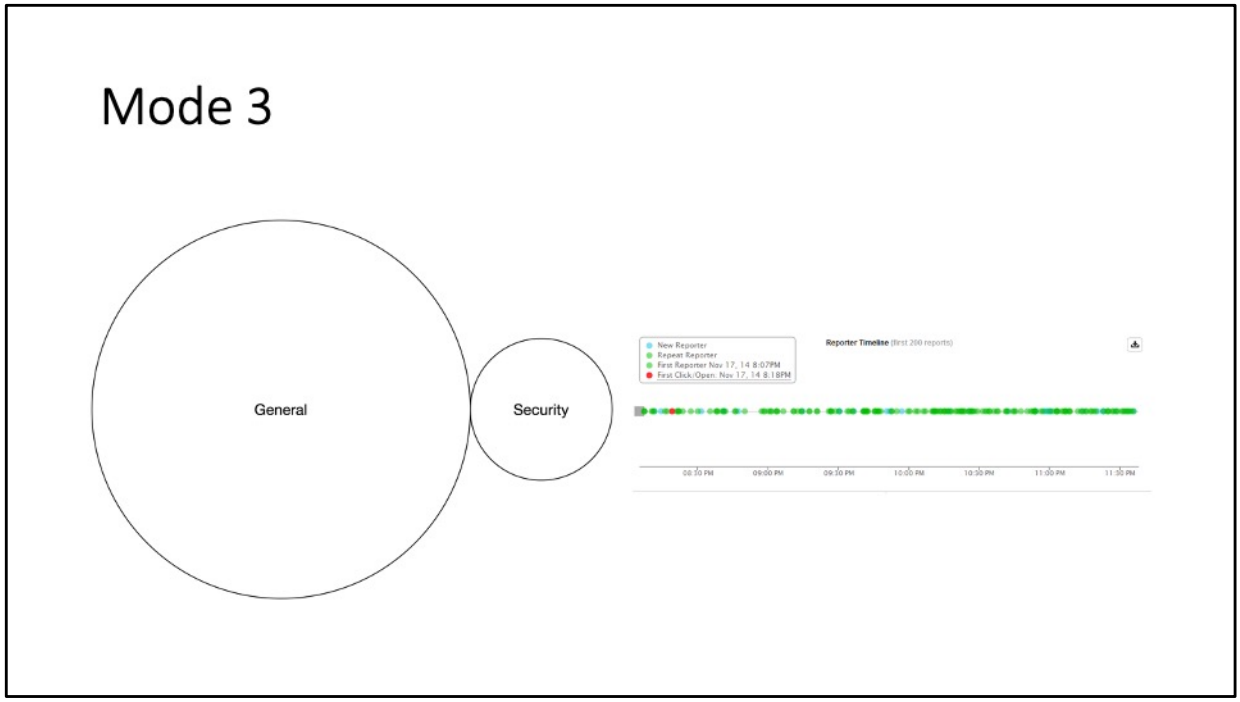


Past talk @ 2020: "Does our AppSec program work?" 50% reduction in new high pen-test findings, reduction in fix time, teams fixed essentially all high findings.
Why? As validated by Veracode State of Software Security 11, we enhanced testing with DAST, SAST, frequent scanning using and API.
We extended the team's testing and bug fix performance into security.

<u>Implications</u>
Org: train developers on how to prioritize, test, and fix security bugs (enhances their bug management performance), security team improves the system by adding security expertise
You (non-security): seek out a security engineer, learn from them
You (security): seek out engineers, learn how they work, help them work more securely by integrating security into what they do

Veracode. (2020). State of Software Security Volume 11. https://info.veracode.com/report-state-of-software-security-volume-11.html
https://safetyofwork.com/episodes/ep60-how-does-safety-ii-reimagine-the-role-of-a-safety-professional

Provan, D. J., Woods, D. D., Dekker, S. W. A., & Rae, A. J. (2020). Safety II professionals: How resilience engineering can transform safety practice. *Reliability Engineering & System Safety*, *195*, 106740. https://doi.org/10.1016/j.ress.2019.106740



Phishing is (or was) a new attack that our general performance is not equipped to deal with. My experience at a large Canadian bank in the early days of phishing: response team was busy every night taking down phishing domains until we hired a firm that had quickly stood up an outsourced takedown service.
PhishMe/Cofense presentation from Secure360 2015: Cofense built an anti-phishing system where user reports are checked by security experts; good reporters get a higher “credit score”. If there are enough high-credit reports, the system automatically blocks the link: what you see in the graph is that the first click comes after the early reports
This is a new systemic capability to resist phishing.

<u>Implications</u>
Org: task the security team with establishing new capabilities to defend against new types of attacks, building a system, not just a point defense (like Cofense)
You (security): research and build new capabilities for new attacks like supply chain attacks!

Image: Cofense, Secure360 2015

Questions?
Challenges?