RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Lessons from Building an Information Security Function

SESSION ID: STR-W03B

James Shira

Group Chief Information Security Officer
Head of Technology and Architecture (CTO)
Zurich Insurance Group

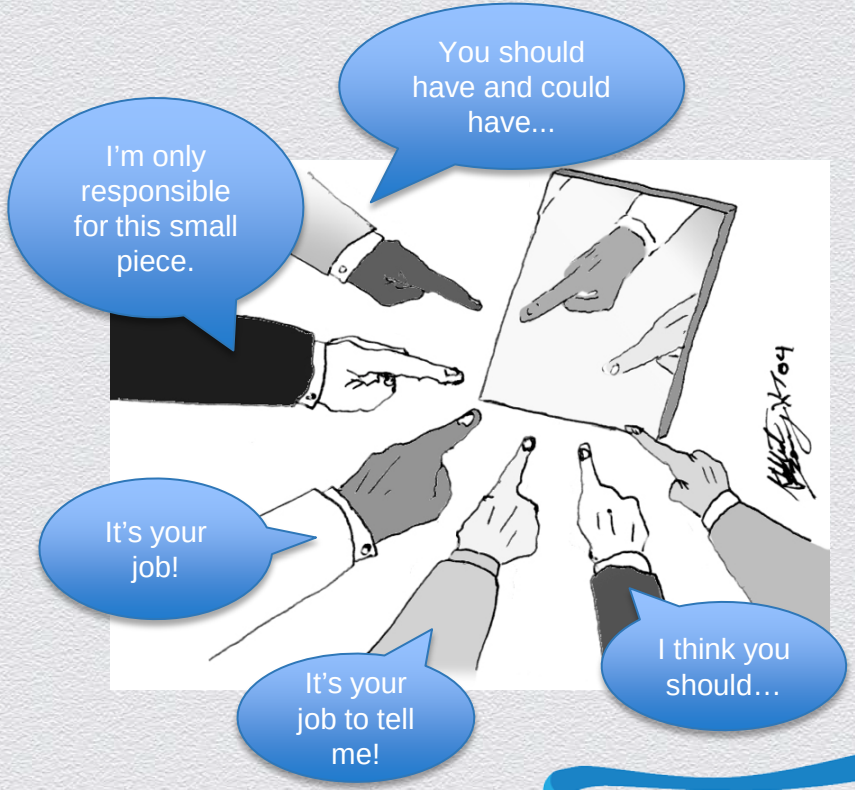
- Background
- Transformation
- Conclusion

Presenter's Company Logo – replace on master slide

Background

Challenges Zurich Faced

- Disparate information security resources and capabilities across Group IT
- Mindset of “advising” with no delivery or execution
- Lack of clearly defined accountability and responsibility
- Constant cross team blaming when issues occur



Presenter’s Company Logo – replace on master slide

Issues we all face

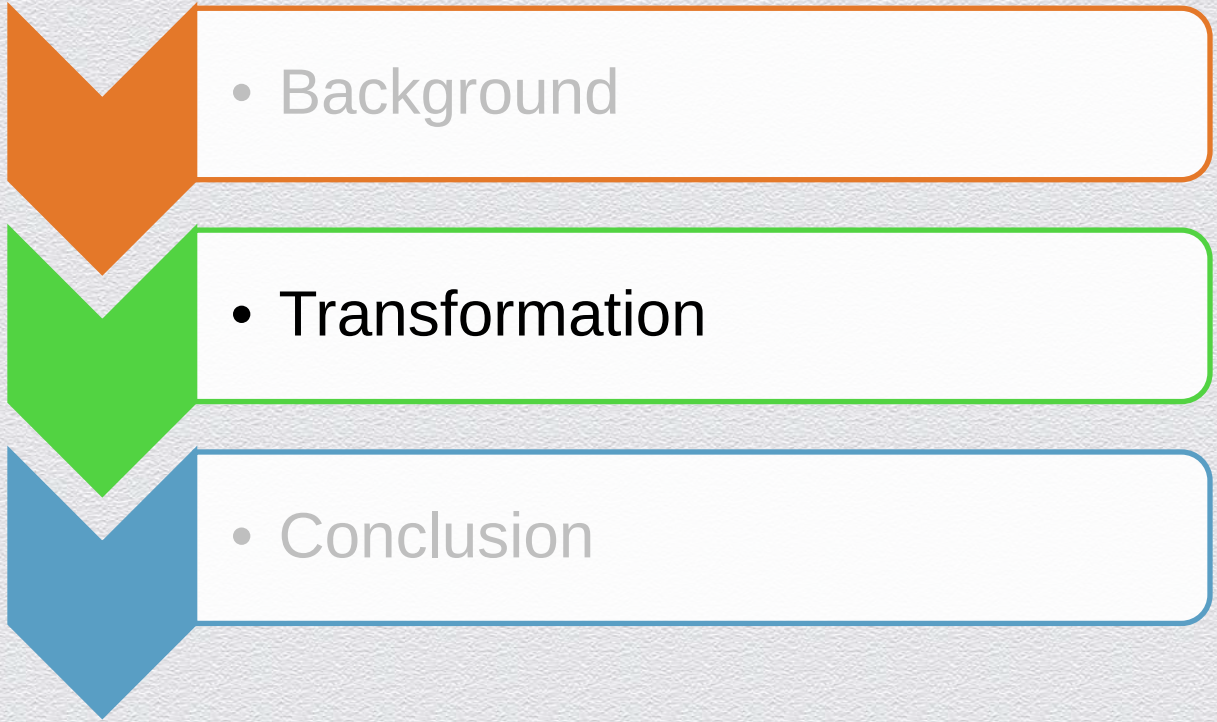
Complex IT policies and environments

Vast and disjointed internal and external requirements

Difficulties measuring effectiveness of security

Strained partnership with the business

Presenter's Company Logo – replace on master slide



Presenter's Company Logo – replace on master slide

Transformation started with a focus on "Effectiveness"

Presenter's Company Logo – replace on master slide

What We've Done

Simplify and Rationalize

- Reduced over 2,000 aspirational controls down to 128
  - Rationalized against internal and external requirements
  - Grounded controls to funding
  - Followed evidenced based approach to demonstrating controls

"Assess Once, Satisfy Many"

Presenter's Company Logo – replace on master slide

What We've Done

Centralized Accountability

- Consolidated security functions under one team
  - Promoted Ownership of accountability and outcomes
  - Minimized politics and the "blame game"
  - Aligned objectives and incentives

Ownership drives "right behaviors"

What We've Done

Heavy focus on operations and hygiene

- Improved hygiene of existing environment
  - Consolidated 7 perimeter entities
  - Removed 171,154 stale accounts
  - Achieved IAM processing within 99% of SLA
  - Lockdown of local admin by 90%+
  - Secured over 41,292 open shares
  - Hardened systems configuration

Before the "cool" things can be done, the basics need to be effective

Presenter's Company Logo – replace on master slide

What We've Done

Built-out security capabilities

Zurich deployed many security capabilities within the environment, each of which must be utilized to its fullest

- Global logging
- USB lockdown
- Privileged account vaulting
- Application code scanning
- Whole disk encryption
- Secure backup tape handling
- Token-less two-factor VPN
- Secure file transfer
- Data loss prevention
- Consistent anti-virus
- Identity & Access Management solution
- Network monitoring and discovery

Avoid "feature surplus" when deploying technologies

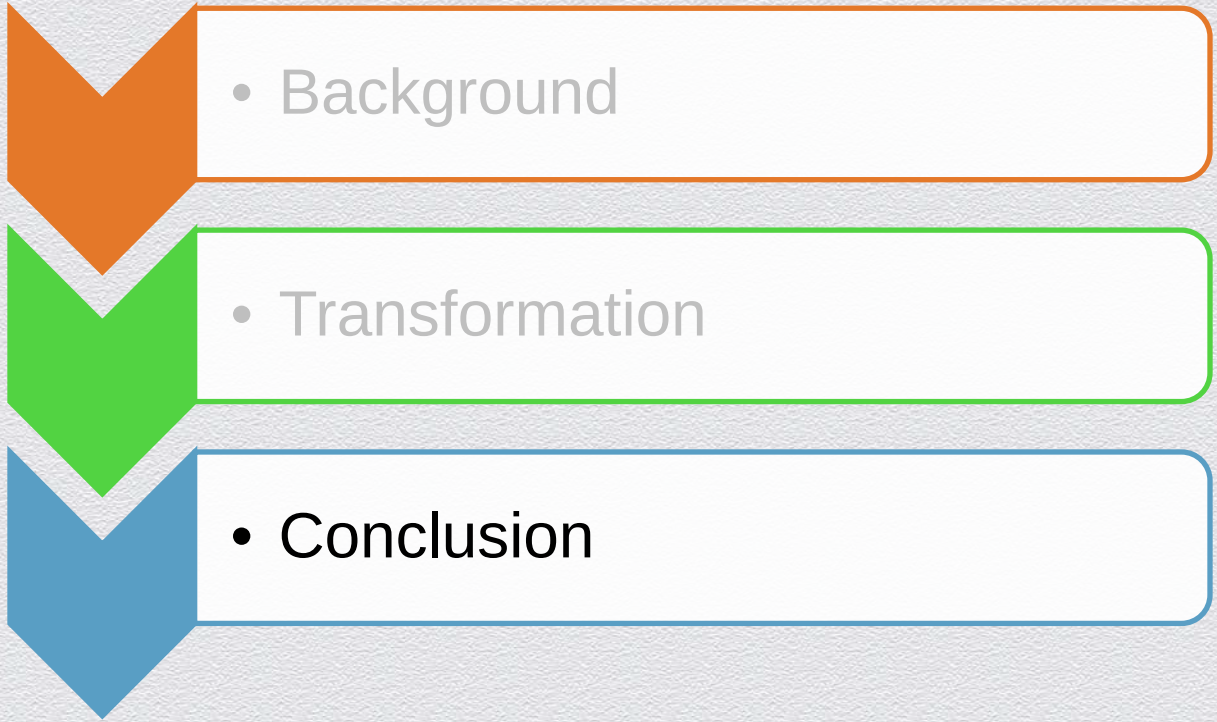
Presenter's Company Logo – replace on master slide

What's Next For Us?

- Zurich will finish the multi-year journey of transforming the information security function by:
  - Completing deployment of capabilities
  - Operationalizing security operations "hubs"
  - Transitioning from a change agent to a steady state

- As the Group CISO and newly appointed CTO, future goals now also include:
  - Leveraging change momentum to influence IT at a broader scale
  - Supporting IT's fit-for-future strategy through innovation and effectiveness

Presenter's Company Logo – replace on master slide



Presenter's Company Logo – replace on master slide

Conclusion

- Zurich's information security posture required **proactive** action to become **effective**
- The results of an information security team's transformation and its **positive external contributions** to the organization can result in a CISO holding a larger role within the organization
- Careers can be driven forward through pragmatic problem solving, measurable accountability, and **leading** change

Presenter's Company Logo – replace on master slide

Q&A

Questions

Presenter's Company Logo – replace on master slide

Thank You

James Shira
CISO@Zurich.com