Redesigning the IT Department

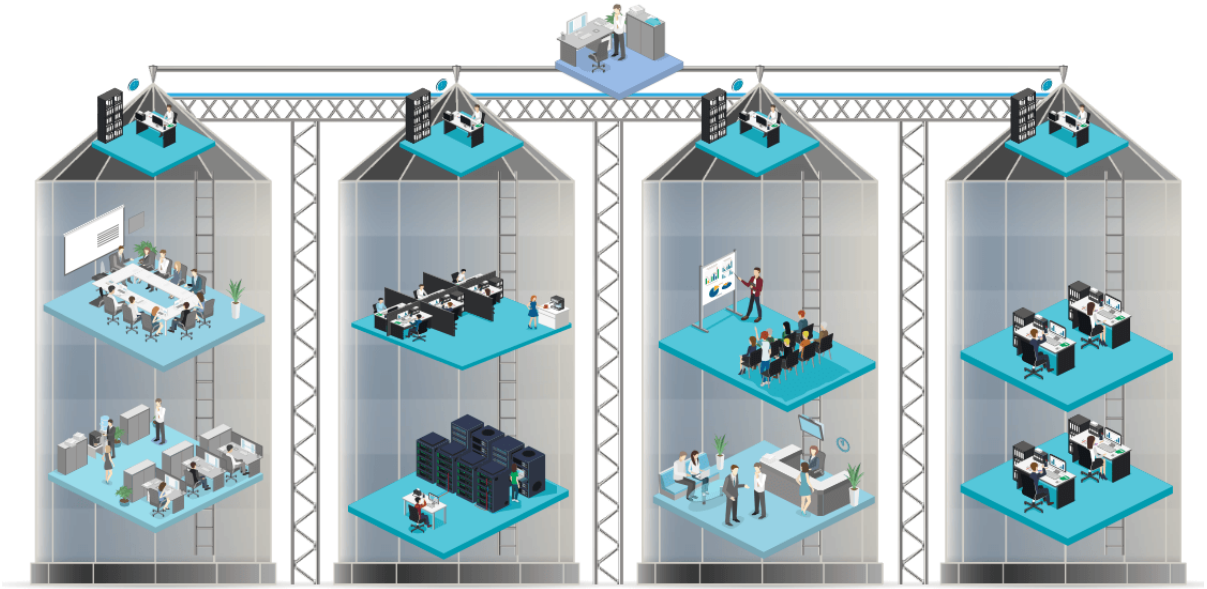
And The Evolving Roles of Security

Jonathan Borgesen
Client Security Principle

Silo

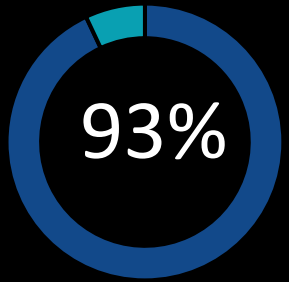
“an isolated grouping, department, etc. that functions apart from others especially in a way seen as **hindering communication and cooperation**.”

IT Has Been Siloed For Too Long



The blame game needs to stop

What is the impact?



Of CIOs say IT’s ability to maximize value for the business is hindered by challenges such as:

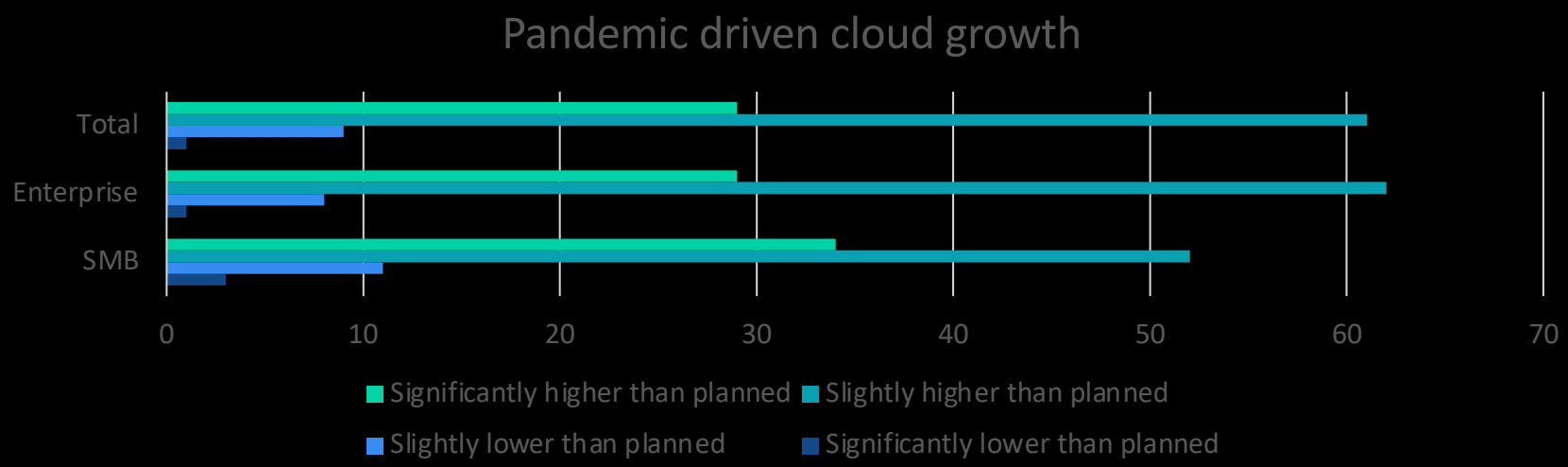
49%
IT and business teams working in silos

49%
Limited visibility and data into users' perspectives on how digital services are performing

36%
Limited visibility into the business value that results from changes to digital

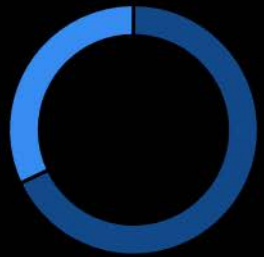
IT objectives have changed

Digital Transformation



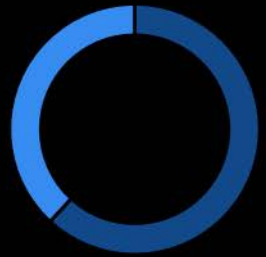
Cloud Risk

68%



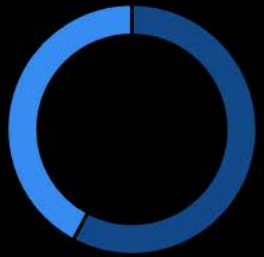
Misconfiguration of cloud platform / wrong setup

58%



Unauthorized access

52%



Insecure interfaces / APIs

How Security Needs to Adapt

Leadership
Prioritize security and give the team the proper resources

Information Risk Council
Cross functional committee charged with security program initiatives

Security Organization
CISO
APP/Network Security
GRC/Compliance

Engineering/Dev Ops

Dedicated Application Security

Information Technology

Dedicated Network and Infrastructure Security

HR

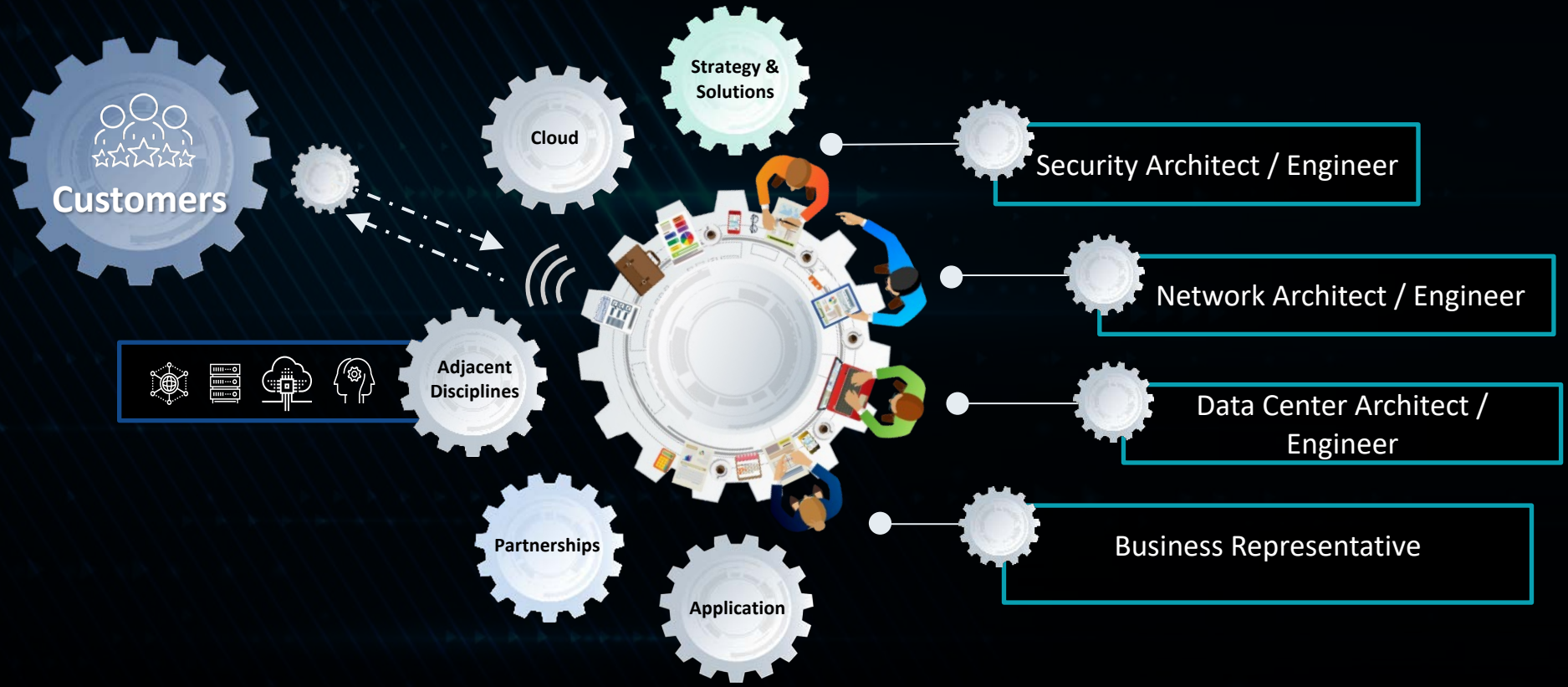
Security Champion

Finance

Security Champion

Modern IT

Functional Model



Step 1 – Understanding

Step 2 – How to Implement

Short staffed

- Tiger team – Create a group with representatives from the Business, Security, Networking, Data Center, and Cloud teams.

Managed Services

- Offset tasks – Managed services growth has exploded over the past three years due to their ability to assist organizations in doing more with less.

Consulting Services

- Bring in outside resources allocated for time that meets your requirements.

New Security Roles

Security Architect - Security engineers need to master their field and pursue depth of knowledge. Whereas **security architects need to stay focused across a broader range of domains** to fully understand the evolving threat and to acknowledge the emerging technologies required to protect organizations.

New Security Roles

DevSecOps – This is a trending practice in application security (AppSec) that involves introducing security earlier in the software development life cycle (SDLC). It expands the collaboration between development and operations teams to integrate security teams into the software delivery cycle.

New Security Roles

SecDevOps - Also known as rugged DevOps, SecDevOps is a set of best practices used to insert secure coding deep inside the DevOps development and deployment processes. It gets developers to think more about security principles and standards as they build their applications.

IT Needs to Modernize With The Business

e+
SECURITY