GFS Client Summit: Technology & Cyber Security

Scott Murray
Chief Technology Officer
Northern Trust

Barb O'Malley
Client Delivery Systems, C&IS Technology Engagement Manager
Northern Trust

NORTHERN TRUST

TECHNOLOGY ORGANIZATION CHART

CTO
Scott Murray

Provide contemporary platforms and optimized processes that are aligned with Northern Trust's business strategy, enabling growth and providing key functional capabilities to our partners and clients

Application Development

EMEA CTO
Fund Accounting
Transfer Agency
Joerg Guenther

C&IS
Accounting
Info Delivery
Barb O'Malley
Client Onboarding
(Paul D'Ouville)

Wealth Management
Internet
Mobile
Shari Jarmy

Operations
Enterprise Risk
Rob Page

Asset Servicing
James Anderson

Finance
HR
Stanis Thiruthuvadoss

Asset Management
Treasury
FX
David Sohmer

Chief Info Security Officer
Kevin Novak

Security & Control
Steve Locke

Architecture & Innovation
Len Hardy

Cross Business Technology
Lori Rago

Infrastructure
Vijay Luthra

Infrastructure Services
Rick Kellemen

SCOTT S. MURRAY, EXECUTIVE VICE PRESIDENT
CHIEF TECHNOLOGY OFFICER

Scott Murray is Chief Technology Officer at Northern Trust. Scott is a member of the Northern Trust Operating Group and Business Leadership Council. He is responsible for the technology infrastructure and applications development for Northern Trust's global business. Scott joined Northern Trust in July 2011.

Prior to assuming the role of Chief Technology Officer, Scott worked 7 years at JPMorgan Chase Bank and 2 years at predecessor Bank One. He worked as Managing Director in several capacities, including Chief Technology Officer for Bank One Capital Markets as well as Global Chief Information Officer for JPMorgan's Treasury Services business unit.

Scott also worked 16 years in senior technology roles in Asset Management and Asset Servicing at Kemper Financial Services (later Scudder Kemper Investments, Zurich Insurance, Deutsche Bank via a series of mergers). Prior to Kemper, he also worked as technology consulting manager for Andersen Consulting (now known as Accenture).

Scott serves on Client Advisory Board of a leading Silicon Valley technology venture capital firm and is on the board of the Pritzker Military Museum and Library.

Scott received a B.S. degree in industrial management from Purdue University and a M.B.A. degree from the University of Chicago.

BARBARA K. O'MALLEY, SENIOR VICE PRESIDENT
CLIENT DELIVERY SYSTEMS, C&IS TECHNOLOGY ENGAGEMENT MANAGER

Barb is currently the Technology Engagement Manager for the C&IS business unit. As Engagement Manager she has responsibility for all services provided to the C&IS business unit by the Technology organization. Barb previously was responsible for Architecture, Research & Development group providing R&D services to the Technology organization.

Prior to her current position Barb was Director of Business Applications with a focus on client delivery and asset servicing applications.

Barb joined Northern Trust in 1984, was named a Trust Officer in 1989, Second Vice President in 1993, Vice President in 1996, and Senior Vice President in 2001 . Barb has devoted the majority of her years at Northern Trust to working on client reporting and delivery initiatives including the initial Passport implementation in 1995.

Barb received a B.S. in applied computer science from Illinois State University.

HOW WE INNOVATE

Tapping into Silicon Valley's best and brightest to create an enhanced user experience.

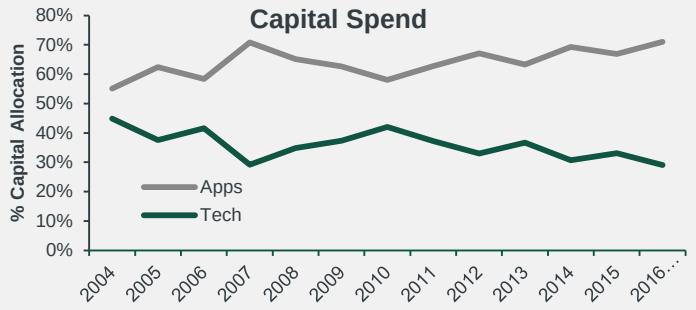
Internal innovation lab focused on user experience

50 South Capital – Invested more than $1 billion in tech startups over the past 16 years

Joint exercises with private equity and technology teams held in Silicon Valley twice per year

- Evaluate emerging technologies
- Access the industry's best talent
- IT expertise supports investment decisions

Infrastructure capital efficiencies accommodate further business investments



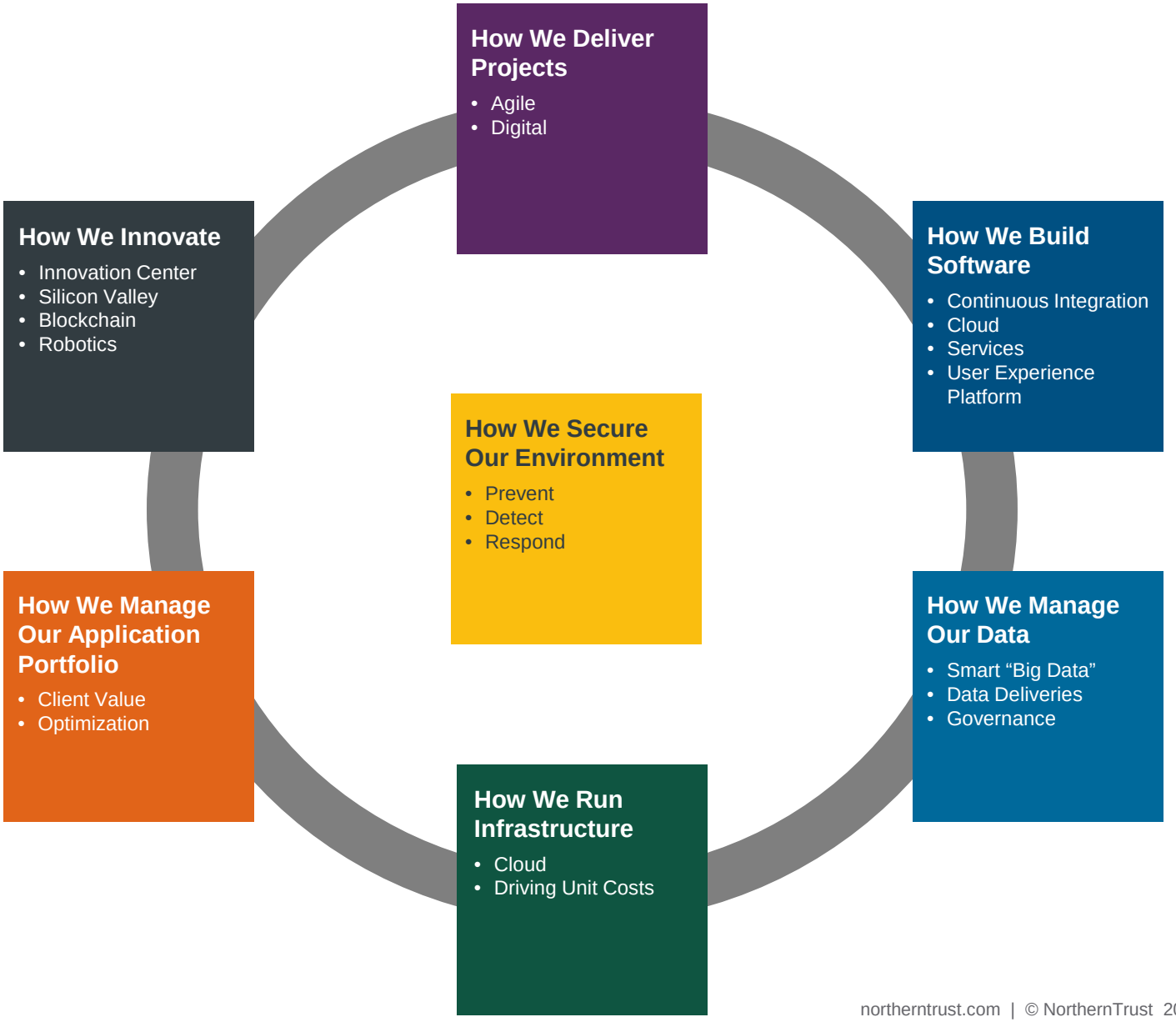
Silicon Valley exercises have resulted in multiple technologies that are now part of our platform:

Guardian Analytics	Cloudera
Nutanix	VCE Vblock
Atlassian	Splunk
Docker	MySQL
Stash	Jira
PandoraFMS	RabbitMQ
Cloud Foundry	Blockchain *

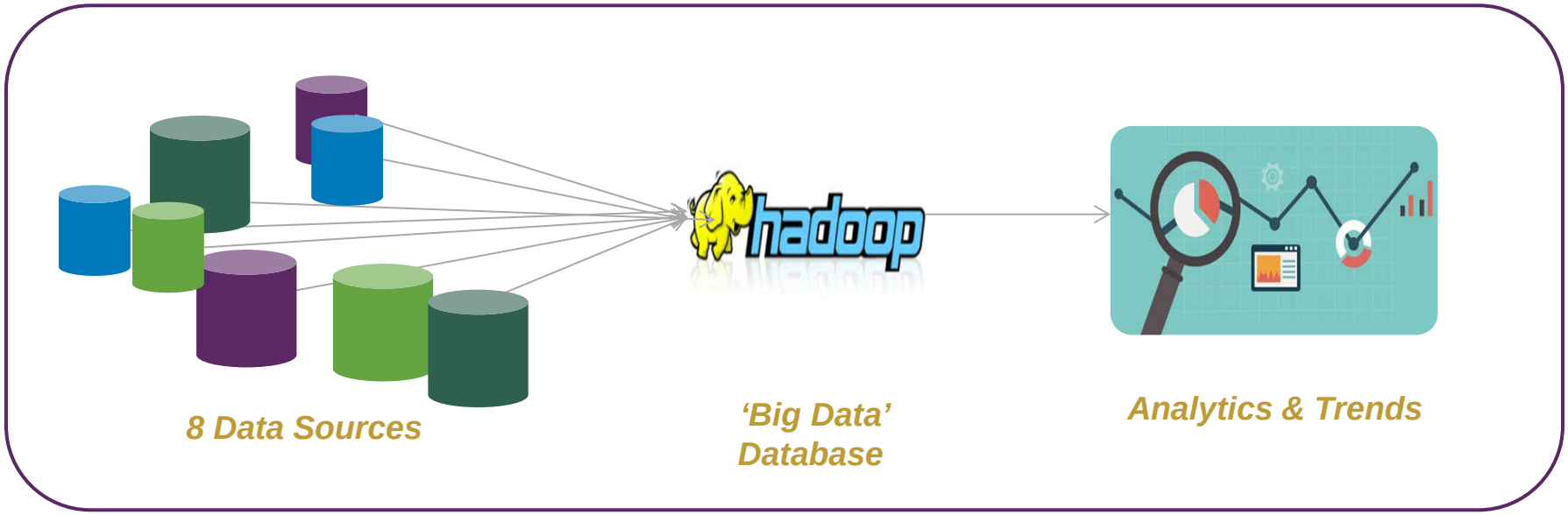
VC Start-Up Technologies

* In R&D

TRANSFORMING TECHNOLOGY TO ENABLE BUSINESS GROWTH



LEVERAGING THE POWER OF BIG DATA



"Northern Trust really knows how to pick Open Source software."
– Top 10 Venture Capitalist in the World

BLOCKCHAIN TECHNOLOGY

Leveraging new technology to explore streamlined solutions.

Promising use cases

Leveraging new technology to explore streamlined solutions

Identity and KYC

Northern Trust technology engagements

R3 banking consortium

- Numerous active projects amongst 40+ members
- Recent prototype of trading venue with instant settlement
- Improvements to blockchain performance and security

Hyperledger Foundation

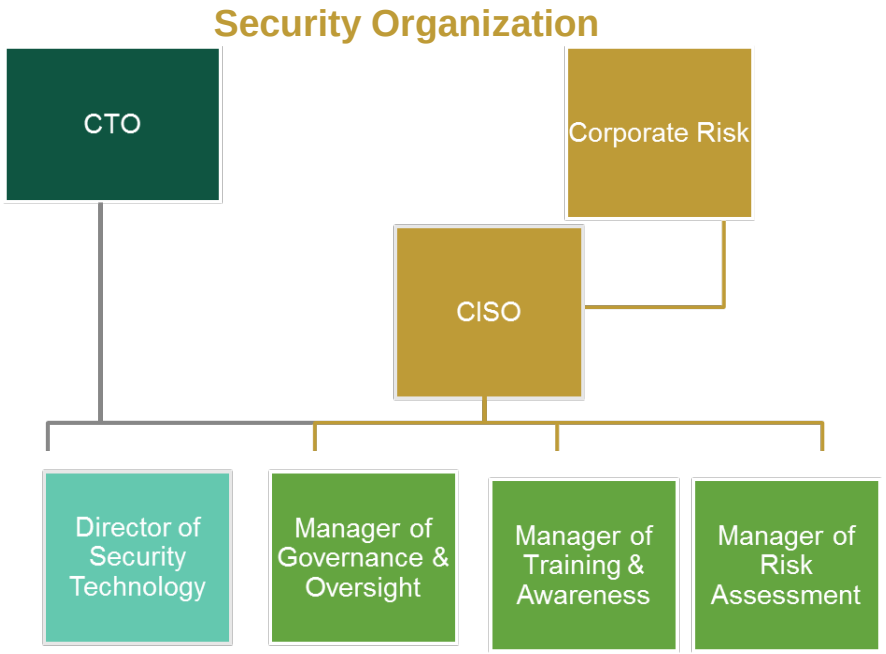
- Members from finance and technology, unlike R3
- Focused on blockchain interoperability and standards
- Great emphasis on improving privacy and security

NORTHERN TRUST'S APPROACH TO INFORMATION SECURITY

…begins at a governance level with its organizational structure and support from executive management and risk committees comprising members from across the business.

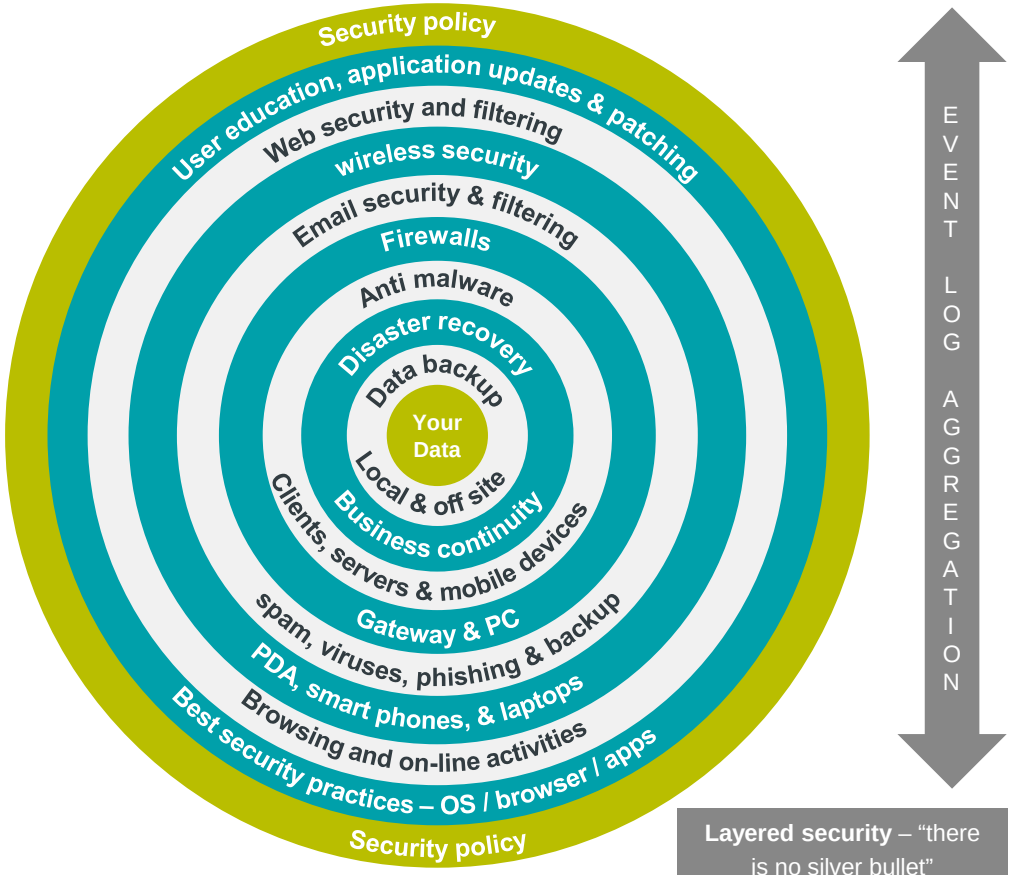
Risk is mitigated through:

- Strong governance process and culture of risk management
- Layered internal controls and detailed risk management practices
- Business unit compliance with policies, standards and guidelines, and external regulations
- Employees responsibility for promoting information security to safeguard information
- Comprehensive assessment of 3rd party vendors
- Regular use of third party security teams to assess effectiveness



SECURITY: LAYERED THREAT MITIGATION

Defense in depth *is an information assurance (IA) concept in which* ***multiple layers of security controls*** *(defense) are placed throughout an information technology (IT) system. Its intent is to provide* ***redundancy*** *in the event a security control fails or a vulnerability is exploited that can cover aspects of personnel, procedural, technical and physical for the duration of the system's life cycle.*



Layered security – "there is no silver bullet"

HOW WE SECURE OUR ENVIRONMENT: PEOPLE & BIG DATA

PREVENT | DETECT | RESPOND

Utilize the Power of People and Big Data Analytics for Detection

Talent

splunk>

"Finding Needles Faster"

Technology

Threat Intelligence

FLASHPOINT · RISKIQ · FINANCIAL SERVICES ISAC · SOLTRA

28+ Unique Data Sources

Juniper NETWORKS · Windows · McAfee · ORACLE DATABASE · BLUE COAT · SOURCEfire · CYBERARK · Linux · Firewall · RSA SecurID

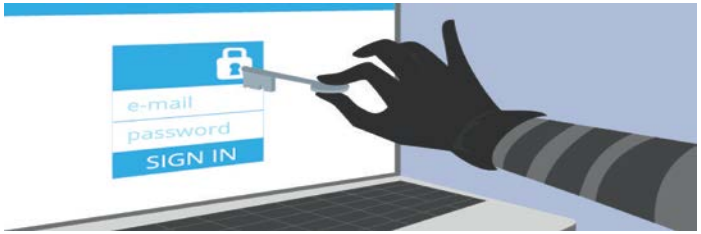
2.25B Events/Day

1TB Log Data/Day

SWIFT CYBER SECURITY CONTROLS

Following high-profile reports of incidents affecting members of their global payments network, SWIFT launched a security program to clearly define an operational and security baseline that members must meet to protect the processing and handling of their SWIFT transactions.

Compromises were generally a result of weak client side controls*



- Hackers gained access to and manipulated the SWIFT Alliance Access server software, which members can use to interface with SWIFT's messaging platform.
- Once in Bangladesh Bank computers, hackers took control of credentials that were used to log into the SWIFT system
- The bank's computer security measures were seriously deficient, lacking even basic precautions like firewalls and relying on used, $10 switches in its local networks.

Actions taken by Northern Trust

- Reviewed compromised SWIFT configuration and confirmed NT does not have the same configuration as the Central Bank of Bangladesh.
- Conducted an assessment against SWIFT security program requirements which demonstrated a high-level of compliance and robust control environment.
- Confirmed latest SWIFT patches have been implemented to current levels
- Implemented process whereby patches sent by SWIFT are applied same-day in test and put into production as soon as change windows allow.
- Active participation on the US SWIFT group subcommittee for technology by the Deputy CISO and Director of SWIFT Operations.
- Continuous review of investments in our security infrastructure, including isolation of certain systems, increased use of two-factor authentication, enhanced logging and monitoring, and additional anti-malware controls for computers accessing the SWIFT network.
- Engaged an independent firm to evaluate end to end SWIFT and Payment controls.

*http://www.reuters.com/investigates/special-report/cyber-heist-federal/

TECHNOLOGY DIFFERENTIATION: RECOGNITION

Northern Trust is recognized for our continual investment in technology.

Top Wealth Management Mobile Application

Best Private Cloud Initiative

Best Infrastructure Initiative

Best Analytics Initiative

CIO 100

QUESTIONS