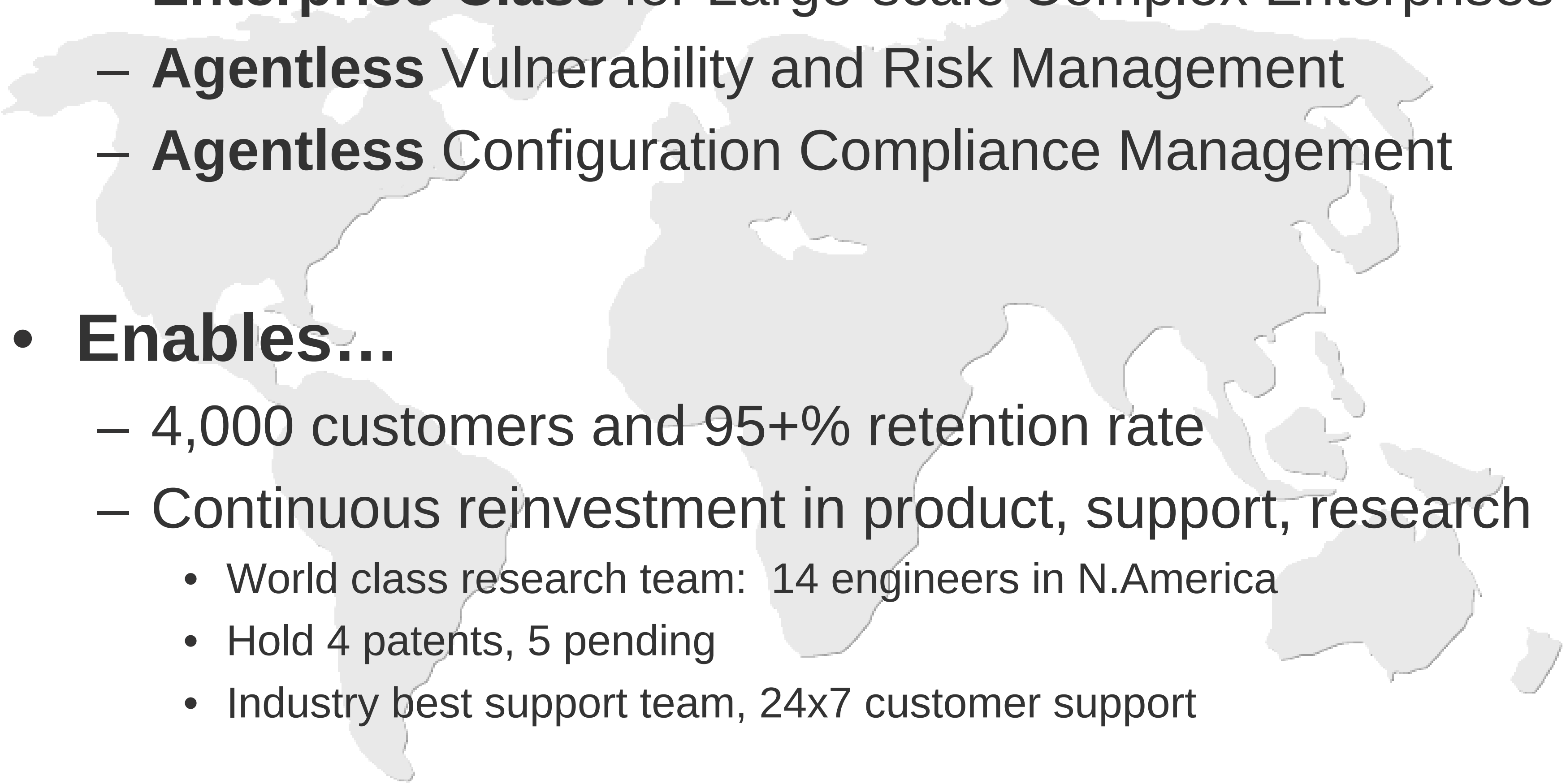
How Security can Change the Behavior of Other IT Groups (For the Better)

Keren Cummins
Director, Federal Market
nCircle
Proactive Network Security

Overview

- A little about nCircle
- A lot about the experiences of two customers



- **nCircle’s Focus…**
  - – **Enterprise-Class** for Large-scale Complex Enterprises
  - – **Agentless** Vulnerability and Risk Management
  - – **Agentless** Configuration Compliance Management

- **Enables…**
  - – 4,000 customers and 95+% retention rate
  - – Continuous reinvestment in product, support, research
    - World class research team: 14 engineers in N.America
    - Hold 4 patents, 5 pending
    - Industry best support team, 24x7 customer support

nCircle
Proactive Network Security

nCircle Customers by Industry

Financial Services & Insurance

Fiserv

KeyBank

HSBC

ZIONS BANK®
We Haven't Forgotten Who Keeps Us In Business®

MORLEY
Fund Management

ICBC
Insurance Corporation
of British Columbia

imb
IndymacBank®

AEGON

nab

BARINGS

بنك نور الإسلامي
NOOR ISLAMIC BANK

Lincoln
Financial Group®

Moody's Investors Service

First Republic Bank

Healthcare & Pharmaceuticals

Driscoll
CHILDREN'S HOSPITAL
CHILDREN'S MEDICAL CENTER OF SOUTH TEXAS

MATRIA
HEALTHCARE

BlueShield
of California

KU MEDICAL CENTER
The University of Kansas

Aurora Health Care

INTEGRIS
Health

Saint Luke's
Health System

AKZO NOBEL

UnitedHealthcare
Healing health care. Together.

Medtronic
Alleviating Pain · Restoring Health · Extending Life

OTSUKA AMERICA INCORPORATED
Otsuka America, Inc.

JOHN MUIR
HEALTH

THE
UNIVERSITY
OF CHICAGO
HOSPITALS

UPMC
University of Pittsburgh
Medical Center

Tenet

Energy & Utilities

PG&E

LA
DWP
Los Angeles
Department of
Water & Power

Dominion

Wisconsin Energy
Corporation

pjm℠

Chevron

Shell

CALIFORNIA WATER SERVICE CO.

elpaso

LCRA

Kansas City
Power & Light®
ENERGIZING LIFE

GREAT PLAINS ENERGY™

KEYSPAN

Government

Foreign Affairs and
International Trade Canada

California
Franchise
Tax
Board

MILLENNIUM CHALLENGE CORPORATION
UNITED STATES OF AMERICA
MCC

USDA

U.S. DEPARTMENT OF THE INTERIOR
BUREAU OF INDIAN AFFAIRS
1824

California Lottery

DEPARTMENT OF LABOR
UNITED STATES OF AMERICA

dhs
California
Department of
Health Services

Public Works and
Government Services
Canada

THE GREAT SEAL OF THE STATE OF MINNESOTA
1858

U.S. DEPARTMENT OF THE INTERIOR
MARCH 3, 1849

FEDERAL COMMUNICATIONS COMMISSION
FCC
USA

USAID
UNITED STATES AGENCY
INTERNATIONAL DEVELOPMENT

DCSA

DEPARTMENT OF LABOR
UNITED STATES OF AMERICA

DEPARTMENT OF WATER RESOURCES
STATE OF CALIFORNIA

Australian Government
Department of Employment and
Workplace Relations

STATE OF CALIFORNIA
DMV

Media & Leisure

groupm

DIRECTV®

BALLY
TOTAL
FITNESS

ACCOR

du

ESPN®

comcast

FOX
INTERACTIVE MEDIA™

News Corporation

Retail & Consumer Goods

KOHLER

GENERAL MILLS

Aaron's
SALES & LEASE OWNERSHIP For Less!

COSTCO

McCormick

BIG
LOTS!

Jean Coutu

ZALES
THE DIAMOND STORE®

TOYOTA

FUJITSU

HONDA

at&t

ADM

SAFEWAY

Factory
Card & Party
Outlet

Payless
SHOESOURCE®

Walmart.com™

Two Organizations, Same Story

Large Financial Institution;

Medium-sized Federal agency

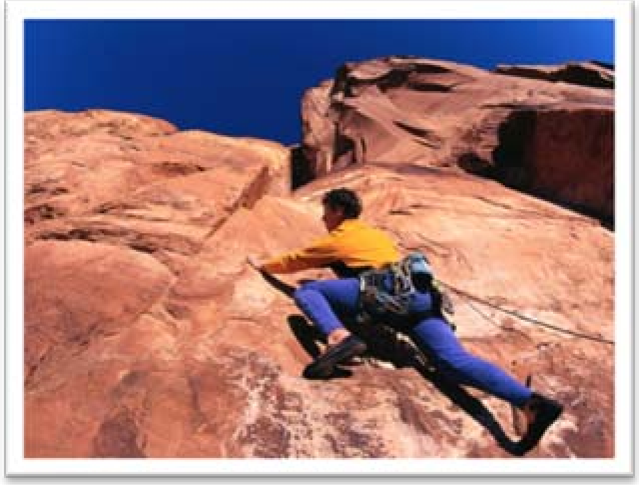
- A daily awareness of security risk throughout all of IT
- Asset owners willingly remediate security problems every quarter
- Other IT groups consult security before deploying a new technology

How did they accomplish this?

Could you do this?

nCircle
Proactive Network Security

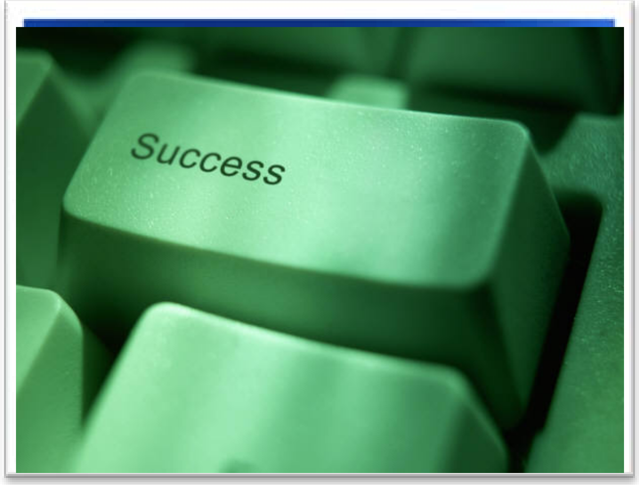
Common IT Security “Soft” Challenges



- Establishing trust
- Establishing common goals
- Achieving reactive results
- Creating a proactive process

→ Five Requirements for Success

5 Requirements for Success



- Building trust
- Building executive level support
- Establishing a common language
- Deploying a personal communications medium, and
- Measuring accountability

nCircle
Proactive Network Security

> “Your scanner knocked my system over!”
> “You seriously expect me to give you my credentials?”
> “This is going to slow down the network too much.”

1. Build Trust
   - Begin before solution deployment
   - Over-communicate
     - What you need to see and how often
     - Exactly when you’re going to be scanning what
     - What you can and cannot get without credentials
     - Share results, even if they’re raw
   - Burn-in phase
     - Start slow and without credentials
     - Use dedicated account for credentials
     - Monitor network usage
     - Be careful about scan windows

2. Build Executive-Level Support

- It all really comes down to the tone at the top
- It’s not “you either have it or you don’t”
  - There are ways you can make this more likely to happen
- Quantify and measure your progress
- Give management an effective vehicle for making changes

3. Establish a Common Language

- Risk means different things to different groups
  - Remediation activities also require distinct approaches
- Single risk metric
  - Allows comparison between distinct domains
  - Gives management team an effective (and easy-to-understand) tool for causing change
  - Gives asset owners an effective tool for demonstrating progress
  - Is quantifiable
- Calculation algorithm ultimately un-important
- Breadth of data sources is critical

4. Deploy a Personal Communications Medium

- Permit deconstruction of risk along any conceivable business dimension
  - Line of business, type of asset, applications, individual, geography, department, etc.
- Must have role-based access
  - "My" risk score
- Self-service distribution
  - Giving assets owners the flexibility to consume and act on data at their own pace and schedule

nCircle
Proactive Network Security

5. Measure Accountability

- All security issues ultimately refer back to humans
  - Cause and/or Solution
- Any behavior-changing solution must track responsiveness and accountability
  - Who is actively working to reduce risk and who is not?
  - How successful is a given remediation initiative?
  - What are the most serious, outstanding problems?
- The “who” component here can be departmental, geographic, functional, or individual

So, Back to the Agency and the Bank

- They base their process on an integrated risk score from nCircle
  - Combining vulnerability, configuration, and/or file integrity data
- Global dashboard by department
  - Aggregate asset risk scores are published to everyone
- Quarterly bonuses depend, in part, on meeting risk score goals
  - There is constant upward environmental pressure on risk
- IT groups at both institutions now:
  - Monitor risk daily
  - Aggressively work to reduce risk scores
  - Consult with IT Security before making configuration changes

Five Steps

1. Build Trust
2. Build Executive-Level Support
3. Establish a Common Language for Risk
4. Deploy a Personal Communications Medium
5. Measure Accountability

Questions? Comments?

- Contact Information

  Keren Cummins

  Director, Federal Markets

  nCircle Network Security

  (301) 379-2493

  kcummins@ncircle.com