Building extended teams
For Security Operations
(Win executive support)

David Nathans
Managed security for:

FORTUNE 500

Post breach recovery architect and CISO for:
Large breach retailer
Large international defense contractor

Partnership for peace

U.S. AIR FORCE
Too Many Secrets
Learn 1 thing today:

It’s not about secrets...
It’s about security
EVERYONE NEEDS TO CARE ABOUT SECURITY
WE’RE GOING TO NEED A BIGGER SOC.
Let’s build a bigger SOC
Is Human Resources a part of the SOC?

Abortion
Adult/Mature Content
Alcohol
Alternative Spirituality/Belief
Art/Culture
Auctions
Audio/Video Clips
Brokerage/Trading
Business/Economy
Charitable Organizations
Chat (IM)/SMS
Child Pornography
Computer/Information Security
Content Servers
Controlled Substances
Dynamic DNS Host
E-Card/Invitations
Education
Email
Entertainment

Extreme
File Storage/Sharing
Financial Services
For Kids
Gambling
Games
Government/Legal
Hacking
Health
Humor/Jokes
Informational
Internet Connected
Devices
Internet Telephony
Intimate
Apparel/Swimsuit
Job Search/Careers
Malicious Outbound
Data/
Botnets
Malicious
Sources/Malnets
Marijuana
Media Sharing

Military
Mixed Content/Potentially Adult
News/Media
Newsgroups/Forums
Non-Viewable/Infrastructure
Nudity
Office/Business Applications
Online Meetings
Peer-to-Peer (P2P)
Personals/Dating
Personal Sites
Phishing
Piracy/Copyright Concerns
Placeholders
Political/Social Advocacy
Pornography
Potentially Unwanted Software
Proxy Avoidance
Radio/Audio Streams
Real Estate
Reference
Religion

Remote Access Tools
Restaurants/Dining/Food
Scam/Questionable/I Legal
Search Engines/Portals
Sex Education
Sexual Expression
Social Networking
Society/Daily Living
Software Downloads
Spam
Sports/Recreation
Suspicious
Technology/Internet
Tobacco
Translation
Travel
TV/Video Streams
Uncategorized
Vehicles
Violence/Hate/Racism
Weapons
Web Ads/Analytics
Web Hosting
Human Resources is responsible for:

People and policy

- Codes of conducts
- Ethical behavior policy
- Harassment policies
- Acceptable use policies

Escalation point for a policy violation
Services for legal:

- e-Discovery
- Data protection
- M&A Audits
- Privacy protection
- Risk evaluations

Escalation point for data loss or breach activity
Partnership with Audit:

- PCI DSS
- Sarbanes Oxley
- FISMA
- GLBA
- HIPPA
- Internal risk
- FCC / FDA
- More...

Necessary evil

Overlapping?
make it easy
Product Security:

- SDLC
- BSIMM
- Vulnerability Management
- Scanning
- Customer IR

Help advise, recommend and develop easy to understand threat and risk registers
3rd party support

Not everyone is as secure as you

Provide *useful* guidelines, standards and offer support

Monitor everything
Finance Support

How are you saving the company money

Defense in-depth without overlap

Demonstrate maturity

Protect the money chain
Challenge them
Employ them
Make them part of the team
IT as a customer (really!)

Give them good usable data

Let them play with your toys
Learn 1 thing today:
It’s not about secrets
It’s about security