



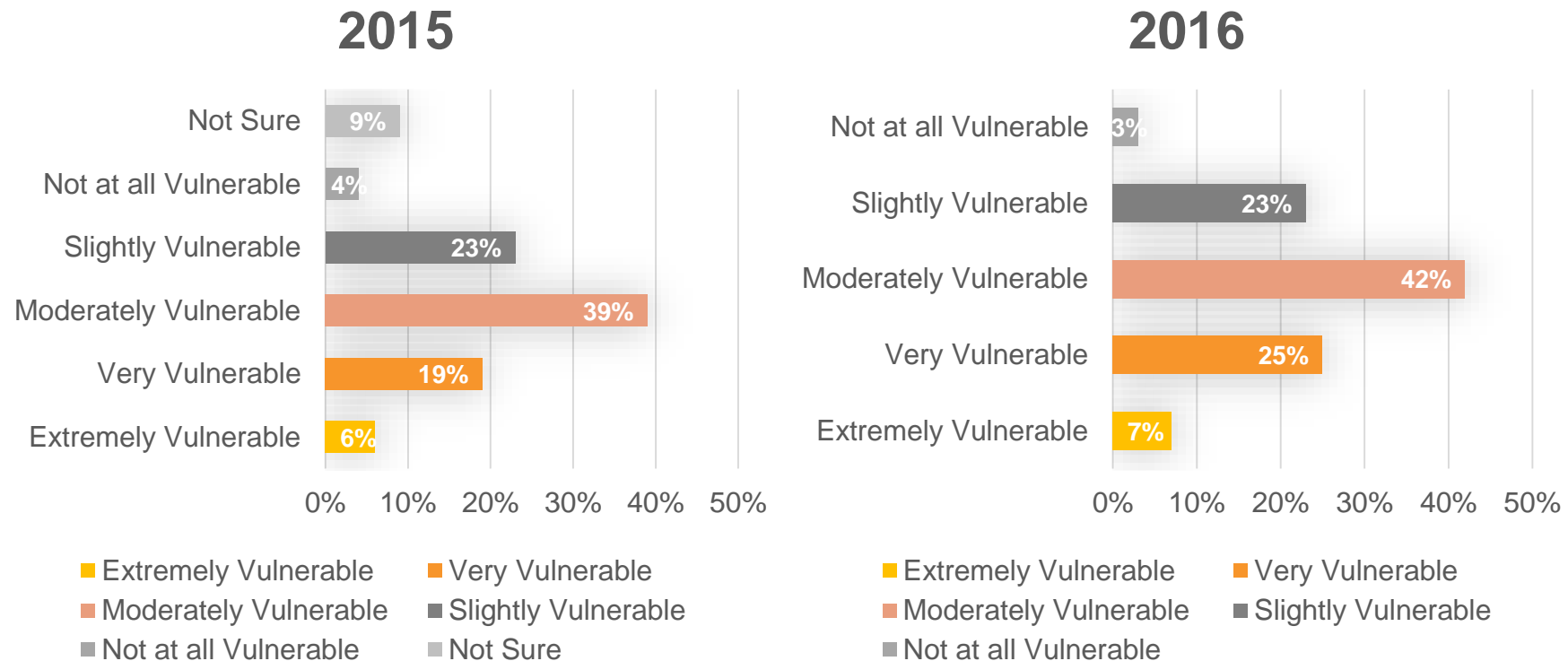
Insider Risk Detection & Prevention

STROZ FRIEDBERG

Scott Weber, Managing Director, Insider Threat Leader

Vulnerability*

74% of organizations feel vulnerable to insider threats — a substantial seven percentage point increase over 2015.

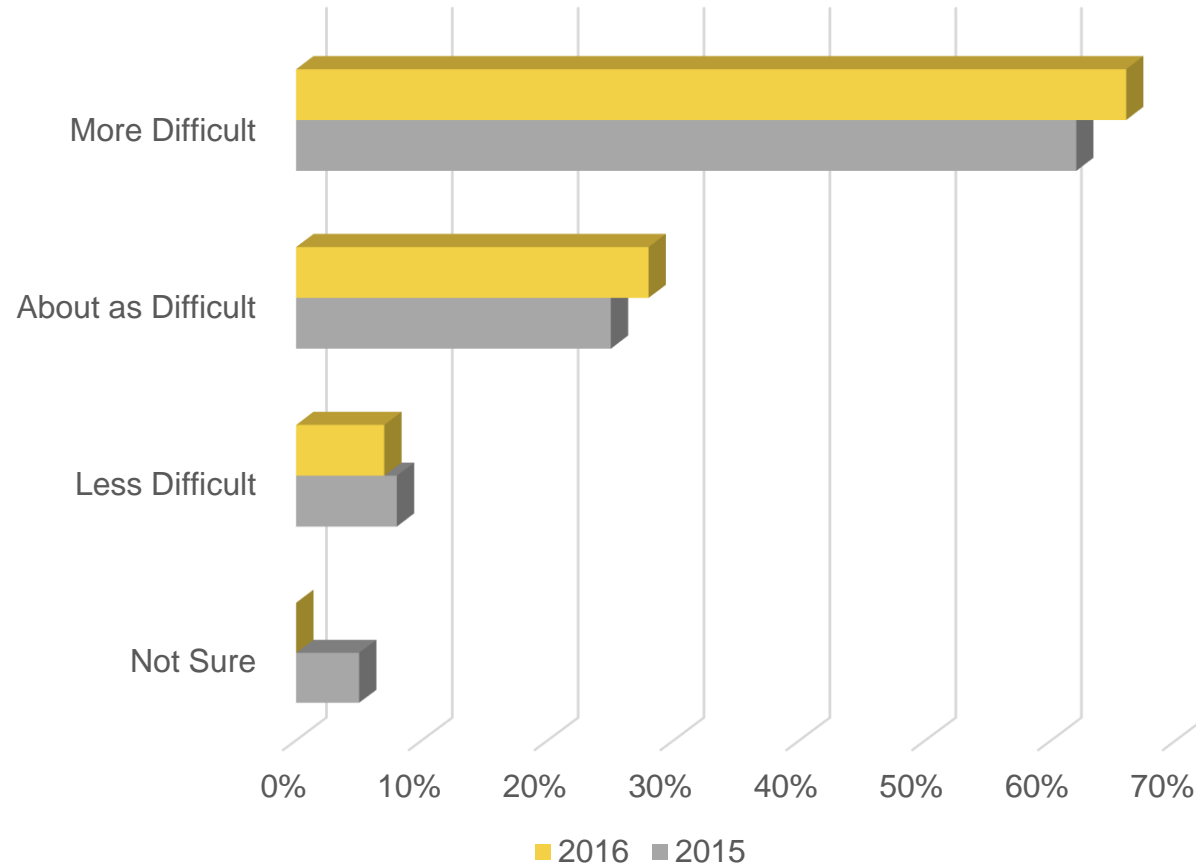


*Insider Threat Spotlight Report 2016, Page 34

*Insider Threat Spotlight Report 2015, Page 29

External vs. Internal*

A majority of respondents (66 percent) have a harder time detecting and preventing an insider attack versus an external cyber attack, up slightly from 2015.

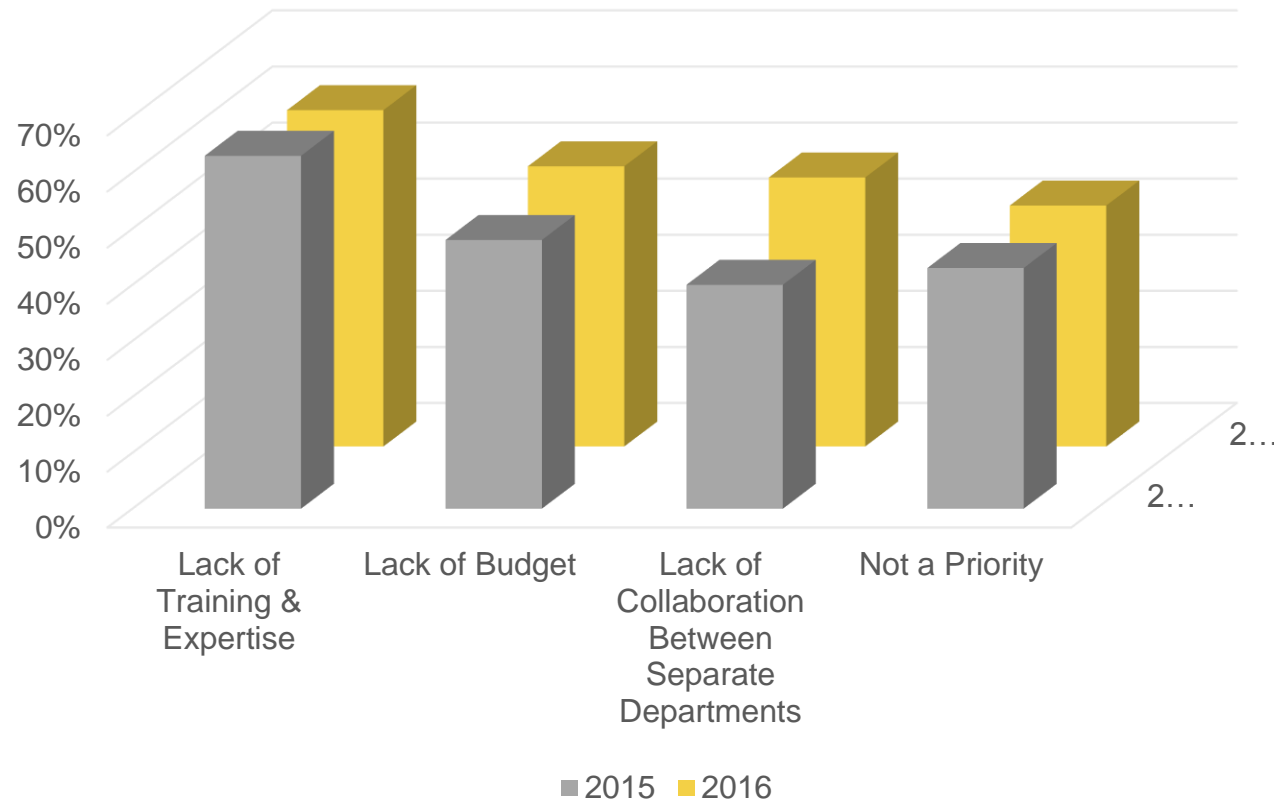


*Insider Threat Spotlight Report 2016, Page 18

*Insider Threat Spotlight Report 2015, Page 14

Barriers to Proper Management*

In 2016, the lack of collaboration was the barrier with the highest gain since 2015, moving up 10 percentage points.

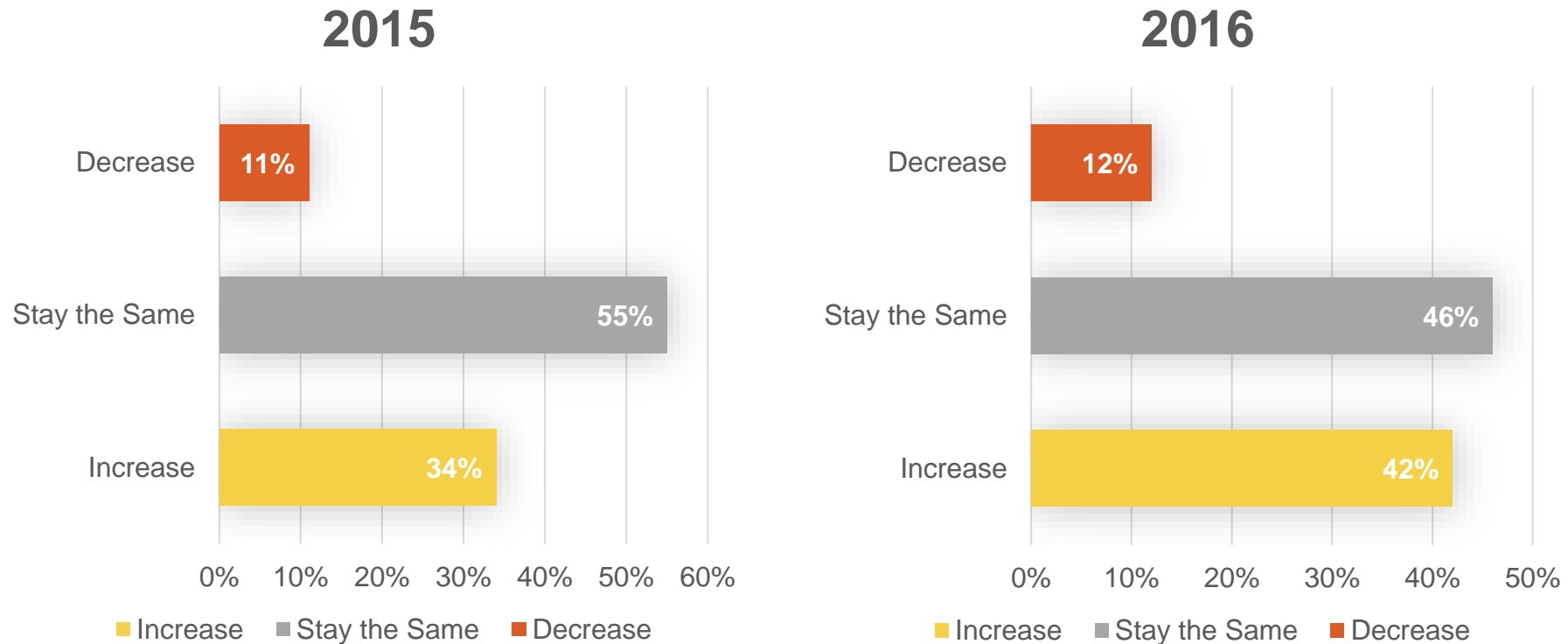


*Insider Threat Spotlight Report 2016, Page 26

*Insider Threat Spotlight Report 2015, Page 24

Budget Trends*

In 2016, 42% of organizations expect a budget increase to address the insider threat problem, up 8% from 2015.

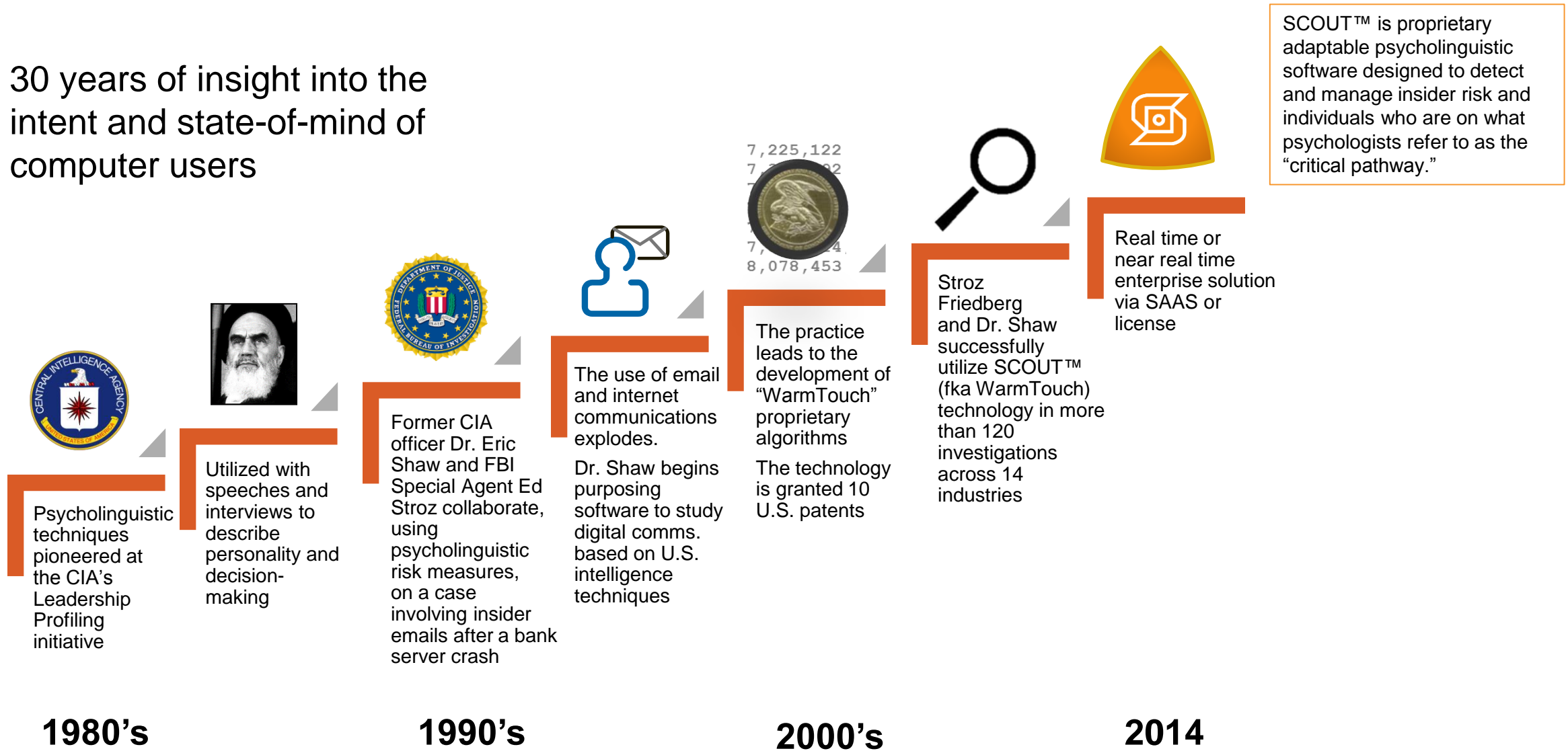


*Insider Threat Spotlight Report 2016, Page 31

*Insider Threat Spotlight Report 2015, Page 24

SCOUT™: A chronology

30 years of insight into the intent and state-of-mind of computer users



Insider risk detection

Carelessness, accidents,
substance Abuse

Workplace
violence

Suicide &
mental health risk

Espionage &
IP theft

Sexual
misconduct

Unwanted resignations &
“bad leavers”

Sabotage

Conspiracy

**Insider
risk**

A circular diagram with a yellow ring and a central image of a city at night, surrounded by eight text labels representing different types of insider risks. The labels are: Carelessness, accidents, substance Abuse; Workplace violence; Espionage & IP theft; Unwanted resignations & “bad leavers”; Conspiracy; Sabotage; Sexual misconduct; and Suicide & mental health risk.

The critical pathway to insider risk

Organizational context

Personal predispositions

- + Personality or social skills issues
- + Previous rule violations
- + Social network risks
- + Psychological conditions
- + Suspicious travel

Stressors

- + From personal life
- + Professional
- + Financial

Concerning behaviors

- + Interpersonal conflict
- + Technical violation
- + Security incident
- + Financial stress
- + Personnel
- + Mental health/addiction
- + Social network
- + Travel

Maladaptive organization response

Plans recruitment

Attack planning, possible planning, attack action

Mitigating factors

Event

Recent SCOUT client contributors

- + Prevented IP loss at financial firm with discovery of developer attempting to set up side business marketing data processing innovation developed on company time
- + Identified key player risks for burn-out, job searches and compliance violations in time to allow interventions
- + Identified source of anonymous leaks to regulators and press
- + Identified source of anonymous harassment, threats to leadership
- + Identified cases of acute suicide risk in time for interventions
- + Investigative support in cases of fraud, leadership extortion, former insider masquerading as outside hacker

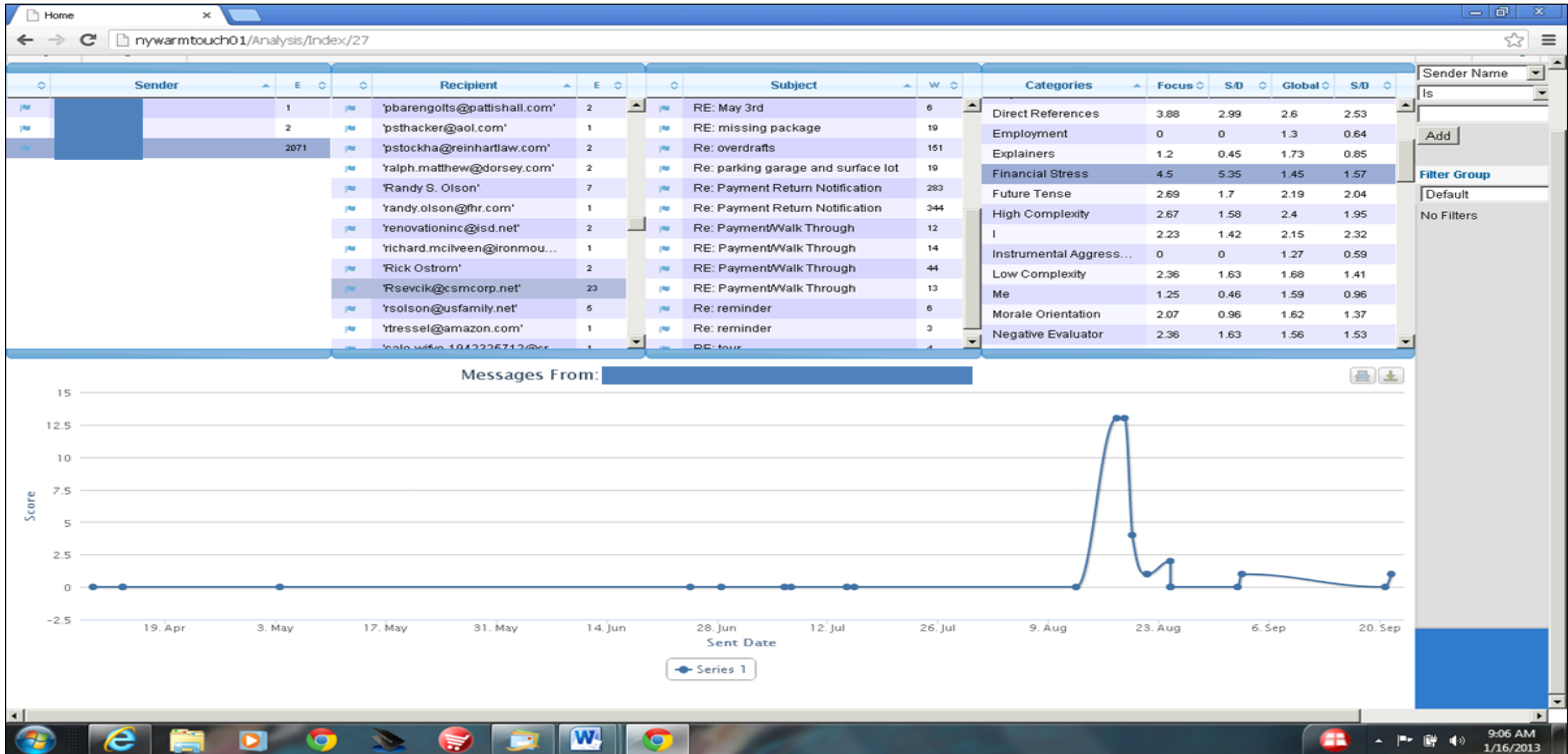
SCOUT supports privacy and ethical practices

- + There is no widespread invasion of employee privacy. Communications are selected for screening based on statistical resemblance to criterion groups. Usually this involves human review of less than .0001% of communications.
- + Sensitivity and selectivity of review is subject to organizational choice.
- + Review criteria based on empirical resemblance to criterion groups, with demonstrated sensitivity as published in peer review journal.
- + Management of privacy can be adjusted based on organizational preferences to include anonymity of communications.
- + Review of selected communications is recommended to be handled by a trusted multi-disciplinary team to include licensed clinicians trained in rules of confidentiality within organizational practice.

Targeted approach

Search Filtering Results by Category (63,530,222 Messages from 117,954 Senders)	Mean Score	SD	Search Value	Remaining Messages	Remaining Senders
Me	.09	1.4	>5	34,817	>1,000
Negatives	.10	1.0	>4	25,970	>1,000
You	2.0	1.5	>5	20,774	>1,000
Victimization	2.3	1.8	>5	2,028	315
Negative Feelings	.27	1.3	>4	1,901	283
Negative Evaluators	1.9	1.7	>4	1,898	283
Employment	1.9	1.2	>2	748	142
Religiousness	2.1	1.5	<5	611 (.00096%)	116 (.098%)

Drill down on financial stress (1/2)



Drill down on financial stress (2/2)

nywarmtouch01/Analysis/Index/27

Count	From	Subject	Count	Category	Count	Score	Score
1	'Randy S. Olson'	RE: way on	7	Anger	1	0	1.08
2	'randy.olson@mr.com'	RE: missing package	1	Anxiety	0	0	1.12
2071	'renovationinc@isd.net'	Re: overdrafts	2	Articles	10	0	2.84
	'richard.mcilveen@ironmou...'	Re: parking garage and surface lot	1	Communicator Group	1	0	2.21
	'Rick Ostrom'	Re: Payment Return Notification	2	Dehumanize	0	0	1
	'Rsevck@csmcorp.net'	Re: Payment Return Notification	23	Depressed	0	0	1
	'rsolson@usfamily.net'	Re: Payment/Walk Through	5	Direct References	9	0	2.6
	'ytressel@amazon.com'	RE: Payment/Walk Through	1	Employment	0	0	1.3
	'sale-wjfy-1942325712@cr...'	RE: Payment/Walk Through	1	Explainers	1	0	1.73
	'sammi123@q.com'	RE: Payment/Walk Through	1	Financial Stress	13	0	1.45
	'sarkozi@thshlaw.com'	Re: reminder	1	Future Tense	5	0	2.19
	'sashahardenjer@hotmail.c...'	Re: reminder	1	High Complexity	5	0	2.4
	'Scolamiero, Joe'	RE: tour	2	I	5	0	2.15

From: [Redacted] ID: 423214

Send Date: [Redacted]

To: [Redacted] Open in New Window

CC: [Redacted] Filter: Exclude Email

BCC: [Redacted] Exclude Email Globally

Subject: Re: Payment Return Notification Toggle Compare

Rose: My apologies.. That is so bizarre. We will get in touch with the bank and take care of this immediately. [Redacted]

subject: FW: Payment Return Notification [Redacted] I have just received two non-sufficient notices for your rent payments. Your balance due at CSM is \$1790. They have charged each check individually. I will be able to have my accountant adjust the late fee off one of the checks, but unfortunately the NSF was charged by the bank on each check. When she adjusts the one \$50 late fee, your actual total due will be \$1740, payable by money order or cashiers check and due immediately. If you have any questions or I can help please stop in to see me. You two have done so well keeping your credit history in order while you were here, I would hate to see that change now. I will forward the other notice as well. Thanks, Rose Sevck/Community Manager/Hill City Apartments/425 N 2nd Street, Minneapolis, MN 55401/Phone:

9:19 AM 1/16/2013

Case Study: Disgruntlement

Total Messages: 1558782 | Total Senders: 28269 | Current Filter Message Count: 0

Groups

All

Search Filter

Person

Sender Name

Contains

Enter Criteria

Logical Operator:

Sender Name Contains 'zimm'

Select Group...

Search Mode:

SPAM

Scores by Filter

Senders [13]

Sender 1	725
Sender 2	1851
Sender 3	824
Sender 4	70
Sender 5	46
Sender 6	35
Sender 7	12
Sender 8	5
Sender 9	2
Sender 10	2
Sender 11	1
Sender 12	1
Sender 13	1

Recipients [674]

Recipient 1	10
Recipient 2	6
Recipient 3	412
Recipient 4	130
Recipient 5	18
Recipient 6	1
Recipient 7	28
Recipient 8	21
Recipient 9	1
Recipient 10	40
Recipient 11	57
Recipient 12	3
Recipient 13	2
Recipient 14	2

Messages [413]

Message 1	355
Message 2	54
Message 3	1572
Message 4	26
Message 5	22
Message 6	337
Message 7	381
Message 8	46
Message 9	442
Message 10	400
Message 11	269
Message 12	580
Message 13	1018

Categories

Category	Focus	S/D	Global	S/D
Dehumanize	0.65	1.6	0.723...	0.647...
Direct References	22.49	20.02	0.296...	1.011...
Disgruntlement	50.92	72.25	670.3...	618.0...
Disgruntlement Lo...	105.65	162.02	828.5...	768.0...
Employment	17.03	14.54	0.883...	0.434...
Financial Stress	16.16	10.96	1.143...	0.905...
Instrumental Aggr...	3.11	5.49	0.427...	0.333...
Me	1.79	2.81	0.283...	0.906...
Religiousness	0	0.07	1.268...	0.799...
Sexuality	1.02	1.99	0.850...	0.580...
Substance Abuse	7.7	2.34	1.237...	0.905...
Suicide	2.6	4.6	0.576...	0.727...
Trapped	0.16	0.39	1.332...	1.138...
Unintentional	4.0	8.88	1.037...	0.838...

Messages From: [Sender] -> To: [Recipient]

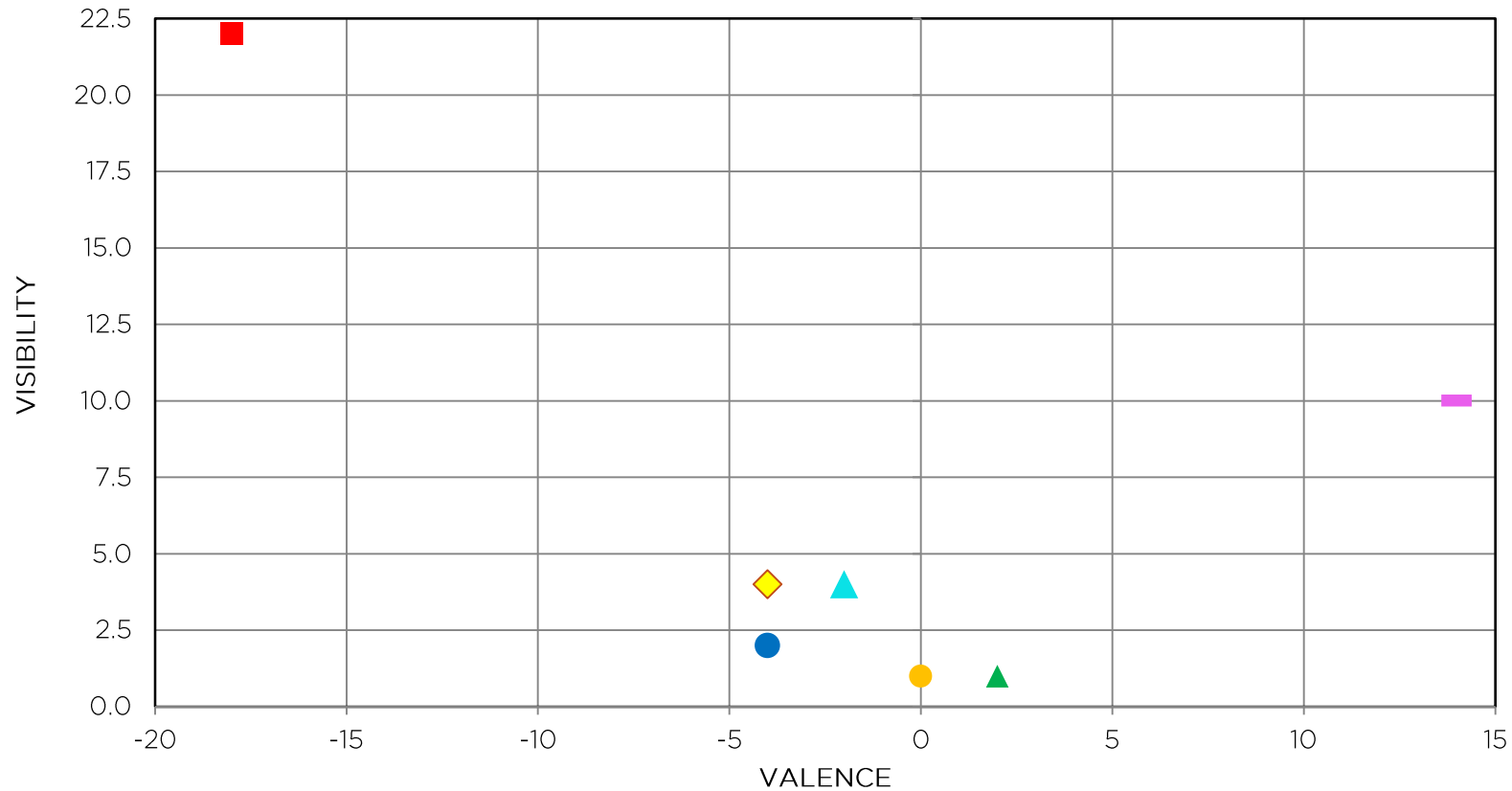
Score

Sent Date

Series 1

Valence: Social network risk

Determining conflicting or close relationships



■ HR Manager ◆ CoWorker_1 ● CoWorker_2 ▲ CoWorker_3 ● CoWorker_4 ▲ CoWorker_5 ■ Wife

Validation data corpus

We used the solution to analyze a body of available communication from known bad actors



PFC Manning

Chelsea Elizabeth Manning (born Bradley Edward Manning) is a trans woman and former US Army soldier convicted in July 2013 after releasing one of the largest set of classified documents ever leaked to the public



Bruce Ivins

Former senior biodefense researcher at the US Army Medical Research Institute of Infectious Diseases and the key suspect in the 2001 anthrax attacks



Corporate IP Thief

Corporate insider discovered stealing intellectual property during a client investigation



Hassan Abu-Jihaad

Born Paul R. Hall, former US Navy officer convicted of supporting terrorism in 2001 after disclosing the location of Navy ships and their weaknesses to an online Al-Qaeda forum while serving as a signalman on board the USS Benfold



Greg Smith

In his March 2012 resignation letter, printed as an op-ed in The New York Times, the former head of Goldman Sachs US equity derivatives business in Europe, the Middle East and Africa attacked GS and its leadership



Online Stalker

Anonymous online blackmailer outed and identified as a former employee during a client investigation



At-Risk Communications





Emails and chats containing "at-risk" content gleaned from client investigations

Embedded within Enron dataset

"Bad actor" & at-risk communications	Communications type	Total # communications	# Identified by SCOUT
Online Stalker	Email	17	14 of 17
Bruce Ivins	Email	5	5 of 5
Depressed	Chat	10	10 of 10
Anger	Chat	10	9 of 10
Financial Stress	Chat	10	9 of 10
Suicide	Chat	10	10 of 10
Substance Abuse	Chat	10	10 of 10
Work Stress	Chat	10	10 of 10
Actual Insiders	Email	13	13 of 13
Abu-Jihaad (Paul Hall)	Email	1	1 of 1
Bradley Manning	Chat	3	3 of 3
Greg Smith	Op-ed	1	1 of 1
Total dataset 10,100		100	95 of 100

Risk and the critical pathway

We can assess risk information against the Critical Pathway

CRITICAL PATHWAY	 MANNING	 AMES	 IVINS	 CORPORATE IP THIEF
Psychiatric disorders	Gender identity	Alcoholism	Multiple psych issues including Dissociative Identity Disorder	Signs of depression
Personality/social skills issues	Yes	Yes	Yes	Signs of narcissistic personality disorder
Previous violations	Juvenile delinquency	Juvenile delinquency	College vandalism, theft	Unknown
Social network risks	Hackers	Unknown	Family history of crime	Family connection interferes with work loyalty
Stressors	Personal, professional, financial	Personal, professional, financial	Personal, professional, financial	Marital, family, supervisor conflict, bad review, conflict with HR
Concerning behaviors	Multiple	Multiple	Multiple	Tardiness, missed meetings, circumventing supervisors, resigns
Maladaptive organizational response	Multiple	Multiple	No comment	HR inquiry escalates risk
Observed Insider Activity	Hacker and press contacts	Travel, spending	Lab violations	Lies about resignation, downloads during "vacation"

Processing capacity

METRICS	SCOUT™ solution capabilities
INGEST & SCORE	1.5 billion messages per day*
CAPACITY	Unlimited* messages
NODE ARCHITECTURE	Each node holds 250 thousand to 1 million messages Each server holds 5 to 200 nodes

Hardware

Recommended specifications for a single system:

- + 32 GB RAM
- + Dual 6-core processor or better

Software

Specifications for software hosted on a single system:

- + Windows 2012 server
- + Internet Explorer
- + IIS 6 or higher

*Based on one R710 dual processor server, scales linearly