Security from the Inside Out: What is your Insider Risk?

WILLIAM TAM
Director of Sales Engineering, Cloud Security, APAC and Office of CISO
NEW COMPANY, UNIQUELY FORMED TO OFFER A NEW APPROACH TO SECURITY

Commercial Leader with Content Security & DLP Cloud / On-Premise / Hybrid

Pioneer on Cyber Frontlines with Financial Resources Deep Understanding of Threat Detection

Networking Innovator with Advanced Evasion Prevention Security at Scale

Cloud Security Leader with Visibility, Control and Security in the Cloud

FORCEPOINT

POWERED BY Raytheon
WHAT IS AT RISK?

MOTIVATION

THREAT ACTORS

CIB
(Motors)

INSIDERS
(Malicious)

Hacktivists
(Ideology/Politics)

TARGETS

SMB / SUP

END USERS

PUBLIC SECTOR

INFRAS.
(Disruption)

FRAUD
(Financial Gain)

OBJECTIVES

IMPACT

VULNERABILITIES

IMPACTS

EFFECTS

Copyright © 2017 Forcepoint. All rights reserved. | 3
WHAT IS AT RISK?

MOTIVATION

INSIDERS
(Accidental / Malicious)

CYBER-CRIMINALS
(Money/ROI)

HACKTIVISTS / NATIONS
(Ideology/politics)

SMB / SUPPLIERS

ENTERPRISES

PUBLIC SECTOR

INFORMATION
(Identities & IP)

INFRASTRUCTURE
(Disruption / Safety)

FRAUD
(Financial Gain)

IMPACT

VULNERABILITIES

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

BRAND

FINANCIAL

IMPACTS

EFFECTS
INFORMATION SECURITY FUNDAMENTALS

DATA

NETWORKS

USERS

Cloud Apps
Corp Servers
Websites
Email
Endpoint Media

Mobile
Office
Other Locations
Partners & Supply Chain
Customers

IN THE CLOUD, ON THE ROAD, IN THE OFFICE
**BUSINESS TRANSFORMATION**
- Increasingly Mobile Workforce
- Adoption of Cloud Infrastructure & expansion of supply chain
- Rapid IT delivery

**WORKFORCE SKILLS & RESOURCING**
- Shadow IT
- Security Awareness
- Lack of IT staff
- Static Budgets

**INDUSTRIALIZATION OF CYBERCRIME**
- Compromises Users & Their Data
- Increasingly Sophisticated Campaigns

**INCREASING REGULATORY SCOPE**
- Breach Notification
- Consumer Rights Over Their Data
- Higher Penalties
- Infrastructure Scope

Enable Business Innovation and Agility  
Protect the Brand
INFORMATION SECURITY PROGRAM FOCUS

PRE-BREACH

POST-BREACH

INCIDENT

TIMELINE
INFORMATION SECURITY PROGRAM FOCUS

DEFEND

- Understand my security & risk posture
- Protect critical data from malicious attack and misuse

DETECT

- Provide rapid detection of insider threats

RESPOND

- Reduce response times to insider incidents to comply & protect my brand

RECOVER

- Get back to ‘normal’ and learn from event – feed into ‘prepare’

PRE-BREACH

- Risk management

POST-BREACH

- Response planning

INCIDENT TIMELINE
ADDRESSING THESE CHALLENGES REQUIRES A NEW APPROACH

OUTSIDE ATTACKS

INSIDER THREATS

Defend

Initial Compromise

Lateral Movement

Breach

Detect

Respond

Recover

Get Back To Normal

Reduce “Dwell Time” (when threats are in your network)

to minimize theft and damage

Copyright © 2017 Forcepoint. All rights reserved.
ADDRESSING THESE CHALLENGES REQUIRES A NEW APPROACH

Protect as much as possible

DEFEND

OUTSIDE ATTACKS

INSIDER THREATS

Average time to identify MALICIOUS outsider attacks¹

256

Average time to identify UNINTENTIONAL insider breaches¹

158

Reduce “Dwell Time” (when threats are in your network) to minimize theft and damage

Source: Ponemon 2015

TIMELINE

10

1Source: Ponemon 2015
USER BEHAVIOR PERSONAS THAT POSE RISK TO AN ORGANIZATION

INTENTIONAL USER  22%
ACCIDENTAL INSIDER  68%
COMPROMISED INSIDER  10%

Source Ponemon 2016
COST OF AN INSIDER BREACH

Average Cost Per Incident

Intentional User: $347
Accidental Insider: $207
Compromised Insider: $493

Average Annualised Cost

Intentional User: $1,228
Accidental User: $2,292
Compromised User: $776

Source: Ponemon 2016
TECHNOLOGIES CHANGE

PEOPLE ARE THE CONSTANT IN SECURITY
Inadvertent Behaviors
Poorly communicated policies and user awareness

Broken Business Process
Data where it shouldn’t be, not where it should be

Rogue Employee
Leaving the company, poor performance review

Criminal Actor Employees
Corporate espionage, national espionage, organized crime

Malware Infections
Phishing targets, breaches, BYOD contamination

Stolen Credentials
Credential exfiltration, social engineering, device control hygiene

ACCIDENTAL INSIDER
MALICIOUS INSIDER
COMPROMISED INSIDER
CASE STUDIES
PEOPLE AT THE CENTER OF SECURITY BREACHES

Over 10,000 records outside company control as EMPLOYEES leave or retire with data on personal devices

Fined $1M when a departing EMPLOYEE stole data on 730,000 client accounts

Vendor EMPLOYEE has credentials stolen, exposing 56M credit cards

ACCIDENTAL INSIDER
MALICIOUS INSIDER
COMPROMISED INSIDER
The complexity is growing exponentially...

- Mobile workers
- On-site employees
- Partners
- Supply chain
- Customers

DATA EVERYWHERE

- Public cloud
- SAAS – Salesforce...
- Private cloud
- Websites
- Endpoint media

USERS ANYWHERE

- Legitimate copying of data
- Data theft
- Poor business processes

MANY BEHAVIORS
Our systematic approach enables a broad view… focusing on the one constant with the knowledge of intent.
YOU MUST UNDERSTAND INTENT TO INTERPRET AN ACTION

John A.
Senior Developer
Top 10 Hedge Fund

Copies code to removable media

GOOD EMPLOYEE
- Leaving on monthly business trip
- Regularly takes work home
- Complies with company policies

MALICIOUS INSIDER
- Received bad performance review
- Stockpiling sensitive files on personal USB drive
- Copying customer details and requirements
You must understand intent to interpret an action & identify impersonators.

Roberto S.
Geological Engineer
Global Petrochemical Company

Credentials are compromised

- Regular remote worker
- Escalating privileges
- Off hour working times
- Remote connection from foreign country

GOOD EMPLOYEE

COMPROMISED INSIDER
BUILDING AN INSIDER THREAT PROGRAM

People
- Identify insider threat problem
- Build Legal/HR coalition
- IS policy & strategy review

Technology
- Define requirements
- PoC detection
- Prove theory
- Learn normal behaviour
- Identifier outliers
- Risk scoring – threat vs. asset

Process
- Offer education
- Share metrics by dept. & enlist volunteers
- Agree culture

People
- Enforcement
- Set actions on objective for tactical wins
- Manage risk

Technology
- Offer education
- Share metrics by dept. & enlist volunteers
- Agree culture

People
- Identify insider threat problem
- Build Legal/HR coalition
- IS policy & strategy review

Technology
- Define requirements
- PoC detection
- Prove theory
- Learn normal behaviour
- Identifier outliers
- Risk scoring – threat vs. asset

Process
- Offer education
- Share metrics by dept. & enlist volunteers
- Agree culture

People
- Enforcement
- Set actions on objective for tactical wins
- Manage risk

Technology
- Offer education
- Share metrics by dept. & enlist volunteers
- Agree culture

People
- Identify insider threat problem
- Build Legal/HR coalition
- IS policy & strategy review

Technology
- Define requirements
- PoC detection
- Prove theory
- Learn normal behaviour
- Identifier outliers
- Risk scoring – threat vs. asset

Process
- Offer education
- Share metrics by dept. & enlist volunteers
- Agree culture

People
- Enforcement
- Set actions on objective for tactical wins
- Manage risk

Technology
- Offer education
- Share metrics by dept. & enlist volunteers
- Agree culture
REQUIREMENTS FOR INSIDER THREAT PROGRAM

DETECT which individuals are behaving in ways that pose the greatest potential risk

RAPIDLY and thoroughly understand that user’s potentially risky behavior and the context around it
BALANCE PROTECTION OF WORKERS PRIVACY WITH PROTECTION OF DATA

PROTECTION EMPLOYEE PRIVACY

PROTECTION OF DATA
TECHNOLOGIES TO ADDRESS THE INSIDER THREAT

DATA LOSS PREVENTION (DLP) + USER BEHAVIOUR ANALYTICS (UBA) = Complete Data Protection
DLP EVOLUTION

2003

- Pre-defined Compliance Policies
- Data Fingerprints

2010

- Endpoint fingerprints
- Cloud & Mobile DLP
- OCR & Cumulative (DRIP) DLP
- C2, Geo-Location & Reputation

2016

- Incident Risk Ranking
- Behavioral Analytics & Risk Indicators
DATA LOSS PREVENTION – ARCHITECTURE

DISCOVER
Data at Rest

ENDPOINT
Data in Use

CLOUD
Data In Use, in Motion & at Rest

NETWORK
Data in Motion

Cloud

Email

Database

Network

Printer

Storage

Web

Media

Email

FTP

IM

IM

Active Sync

Active Sync

FTP

Storage

Web

Email

FTP

Discover Files

Monitor File Permissions

Monitor Uploads

Discover
Files

Uploads

Discover
Files

Copyright © 2017 Forcepoint. All rights reserved.
DATA LOSS PREVENTION IS A TOOL FOR RISK REDUCTION

- **Visibility**
- **Remediation**
- **Notification**
- **Prevention**

Incidents Per Week
SECURITY ANALYTICS - INCIDENT RISK RANKING
DATA LOSS PREVENTION (DLP) + USER BEHAVIOUR ANALYTICS (UBA)

IN THE CLOUD, ON THE ROAD, IN THE OFFICE
MATURING AN INSIDER THREAT PROGRAM

**Behavioural Audit**
- Discrete user activities with relationships
- Metadata Collection & Aggregation
  - "Who does what & how often?"
  - "What does normal behaviour look like?"
  - "Which activities appear to be unusual?"

**Indicators of Risk**
- User behaviours believed to be indicators of risk
- Alert Aggregation
  - "What can our other existing IT systems tell us about a user’s potential risk profile?"

**Risk Scoring**
- Risk-based prioritization scoring of activity
- Behavioural Analytics
  - "Which users have performed the most potentially risky activities?"

**Forensic Context**
- Visibility into & context around user behaviour
- Contextual Data Collection
  - "You’ve identified a user as potentially risky, now what?"
  - "What was the context so we know how best to respond?"

**Remediation**
- Ability to manage behaviours and reduce risk
- Integrated, automated remediation
  - "I’ve verified that a user has performed activities that expose us to risk, how can we now start to manage that risk?"
SureView® Insider Threat COMMAND CENTER

- Organization 30 Day Risks
- Top Daily Risks
- Top Riskiest People
COMMAND CENTER

SureView® INSIDER THREAT

Risk Score Activities

30 Day History

Filters

Activities

Risk Score Activities
VIDEO REPLAY
FORCEPOINT AP-DATA DLP TECHNOLOGIES

DATA-CENTRIC PROTECTION

LOW OPERATIONAL COSTS

COMPREHENSIVE COVERAGE

On-Premises
In the Cloud
At the Endpoint

AP-Data Gateway
AP-Data Discover
AP-Endpoint

DLP modules: AP-WEB & AP-EMAIL
FORCEPOINT SUREVIEW INSIDER THREAT TECHNOLOGIES

EARLY WARNING OF DATA THEFT

PROVIDE ATTRIBUTION & CONTEXT

REDUCE BURDEN ON IT SECURITY & OPERATIONS

SureView Insider Threat Endpoint

SureView Insider Threat Core
WHAT ROLE CAN DLP & UBA PLAY IN YOUR INSIDER THREAT PROGRAM?

PREPARE
- UNDERSTAND MY SECURITY & RISK POSTURE

DEFEND
- PROTECT CRITICAL DATA FROM MALICIOUS ATTACK AND MISUSE
- DEFEND against future user behavior risk by operationalizing what you’ve learned into prevention controls

DETECT
- PROVIDE RAPID DETECTION OF ADVANCED THREATS
- DETECT and identify users who exhibit risky behaviors

DECIDE
- REDUCE RESPONSE TIMES TO SECURITY INCIDENTS TO PROTECT MY BRAND
- DECIDE how best to respond based on informed context and visibility of risky user behaviors

DEFEAT
- GET BACK TO ‘NORMAL’ AND LEARN FROM EVENT – FEED INTO ‘PREPARE’
- DEFEAT risk arising from specific user behaviors by applying active security controls or user re-training

Be PREPARED & Discover Digital ‘Attack Surface’ & remediate data found in risky locations

INCIDENT
PROTECTING HUMAN POINT.