The Insider Threat Actor

Briefing Prepared for:
North Carolina Department of IT

October 18th 2018
Who am I

- United States Military Academy
- US Army Signal Corp Officer
- VP 13+ Years Financial Services
- CIO/CISO 3+ Years Bulk Fuel Distributor
3+ Years:

Senior Manager
Threat Intelligence Support
Secureworks: A brief introduction
Intelligent Security Solutions

Counter Threat Unit™ research team
- Focused on emerging threat trends
- Rapid countermeasure development

Current SOC locations
- Atlanta, Georgia
- Chicago, Illinois
- Providence, Rhode Island
- Edinburgh, Scotland
- Kawasaki, Japan
- 24x7, 365 days/year
- SOCs manned with all teams, working from a single queue
- Disaster recovery
- No client dependency on one SOC

Security Center of Excellence

250B
Events processed daily

~4,400
Clients

59
Countries

900+
Incident response engagements last year

1,800+
Consulting engagements performed annually

59
Countries

2,300
Employees

Powered by the Counter Threat Platform™
Agenda

• What is Insider Threat?

• What are the different types of Insider Threat?

• What can we do to address Insider Threat?
Insider Threat

The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

Source: CERT
According to the Ponemon Institute’s “2018 Cost of Insider Threats” report, the average cost of insider-caused incidents was $8.76 million in 2017 — more than twice the $3.86 million global average cost of all breaches during the same year.
History of Insider Threat

William Duer (1743-1799)
Secretary of the Treasury 1789
Insider Threat continues to be a challenge

Source: CNBC

Horizon Air tragedy highlights airline insider threat vulnerability

The recent theft and subsequent crash of the Horizon Air Bombardier Q400 turboprop airplane by a Horizon Air employee shocked the aviation security world.

The employee, Richard "Beau" Russel, was a 20-year-old ground service agent (baggage handler/airport taxi operator) who had worked at Horizon Air (parent company Alaska Airlines Group) for 3.5 years. On Aug. 10, he climbed

Source: New York Times

Reality Winner, Former N.S.A. Translator, Gets More Than 5 Years in Leak of Russian Hacking Report

Tesla's alleged rogue employee is exactly what Congress is worried about with self-driving cars

- An ex-Tesla employee is accused of stealing code from maximum used in a company factory. In order to stoke all intellectual property from the carmaker.
- Congress has been holding frequent hearings and launching new legislative efforts around keeping the systems that run autonomous vehicles safe.
- The alleged insider's demonstration of how much damage a malicious insider with coding skills can cause.

Kate Foeken

10/20/2017 2:01:20 PM

Source: CNN
2017 Observed Threats by Secureworks

900+ Engagements, 50TB of evidence collected

- Insiders: 8%
- Nation-state Sponsored Threat Actors: 9%
- Financially Motivated Criminals: 83%

Together, Business Email Compromise, Ransomware, and Banking Trojans accounted for 1/3 of all incidents Secureworks supported in 2017.
Verizon 2018 Data Breach Report

According to CERT 30% of Insider Incidents are detected by non-technical means.

- **75%** Outsiders
- **25%** Internal Actors
Ponemon Institute

Average of 2+ Months to contain an insider incident

All types of insider attacks are increasing annually

Average cost of an incident involving a negligent employee in 2018
$283,281

Average cost of an incident involving a malicious employee in 2018
$607,745

Average of 2+ Months

Limited External Distribution: Ponemon Institute

Average of 2+ Months to contain an insider incident

All types of insider attacks are increasing annually

Average cost of an incident involving a negligent employee in 2018
$283,281

Average cost of an incident involving a malicious employee in 2018
$607,745

Classification: Secureworks / Confidential – Limited External Distribution
Can you spot the inside threat?
Potential Motivations for Insider Threat
Categories of Insider Threat

- Unintentional Insider
- Insider Collusion
- Malicious Insider
- Disgruntled Employee
Unintentional Insider

IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!

Human Error

Classifications: Secureworks/Confidential - Limited External Distribution
Insider Collusion

- Greg Chung
  - Employer: Boeing Company (30+ years)
  - 3000+ pages of technical documents

- Jason Smathers
  - Employer: AOL
  - 92 Million customer names and email addresses
  - In 2003 for $28k provided list to spammers to promote gambling site

- Reality Winner
  - Employer: Pluribus International Corp. – subcontractor for NSA
  - Smuggled a TS Government report out in her pantyhose
Malicious Insider

- Anita Collins
- Roman Catholic Archdiocese of NY
- 8 Years – Accounts Payable

- Embezzled over $1M over seven years

- Linda Lee Clark, 68 Grandmother
- SCICAP Credit Union
- 37 Years- Book Keeper

- Embezzled over $2.4M
Disgruntled Employee

- Martin Tripp
- Tesla
- Upset he didn’t get promotion
- Altered Tesla Code
- Sent “large” amounts of data to unknown parties

- Jo Vito Venzor
- Employer- Lucchese Bootmaker

- Fired from job, took an hour to remove from building
- 1 hour later all IT systems ceased functioning
I'm just a riddle, wrapped in a mystery, inside an enigma...
...cloaked in bacon.
\[ \Delta V = \sum [(P_x - P_y) \times W_n] \]
Possible Insider Threat Behaviors

- Remotely Access Network while on vacation
- Works odd hours - wants overtime/weekends
- Unnecessarily copies materials
- Interest in matters outside job duties
- Signs of Vulnerability (financial, drug, mental health, gambling)
- Large amounts of external email or network activity
- Failed attempts at accessing resources
- Recent Disciplinary Actions
- Foreign contacts/travel
- Social Media Posts

Consectetur adipiscing elit, sed do eiusmod tempor incididunt.
Winning Combination

Top→Down + Bottom→Up Approach

- Policies
- Procedures
- Standards
- Work Instructions
- Employee
- Front Line Supervisor
- Manager
- Senior Management
Known Issues
- Policy Violations
- Unauthorized Changes

Suspicious Events
- Unusual work activity
- Unknown error
- Unrecognized events

Normal Activity
- Authorized
- Scheduled
Partnership Across the Organization

Insider Threat

Human Resources

Business

Security
Not just a technology solution to solve...
Right Size Access
Trust, But Verify

STUDIES SHOW THAT COMPANIES WITH A HIGH LEVEL OF TRUST IN EMPLOYEES ALSO PERFORM THE BEST.

IF YOU EVER START PERFORMING WELL, I'LL TRUST YOU, TOO.

THIS DIDN'T GO THE WAY I HOPED.

WHAT KIND OF SCAM ARE YOU TRYING TO PULL?
Periodic Attestation/ Random Spot Checks/ 2 Party Review
See something, Say Something

Positive Incentives more impactful than consequence driven management
Don’t forget the simple things....
Final Thoughts

There is no single approach that can mitigate all categories of human risk.

Start with Data Protection - Identify and classify assets. Build monitoring and safeguards.

Managers - Get to know your people

Keep HR/Security/IT in the loop with employee actions (Probation/Termination, etc)

Establish a culture of self reporting is acceptable.
Questions

Jeremy Manning
Advisory Security Engineer
Secureworks | Counter Threat Unit(CTU)
jmanning@secureworks.com /www.secureworks.com
O:+1 770.870.3160 /C:+1 832.817.8239