Presentation by

Dr. Phil Legg

Associate Professor in Cyber Security

Cybercrime and insider threat: Can AI save us from these adversaries?

October 2018

UWE Bristol | University of the West of England

Cybercrime: Current Landscape

- *"global cybercrime damages predicted to cost $6 trillion annually by 2021"*
- *…bitcoin mining. … 8,500 percent increase in the detection of coinminers. …many cybercriminals are more than happy to just use a victim's computer power and resources to mine cryptocurrencies instead of stealing any personal data or money."*
- *"ransomware has taken center stage, stealing the limelight from most other forms of malware."*

https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

Cybercrime: Current Landscape

- *Globally, cybercrime was the 2nd most reported crime in 2016. (Source: PWC), and more than 50% of all crimes in the UK. (Source: National Crime Agency).*
- *An attacker resides within a network for an average 146 days before detection. (Source: Microsoft)*
- *Most network intrusions—63 percent—are the result of compromised user passwords and usernames. (Source: Microsoft)*
- *At 91.6 percent, "Theft of Data" continues to be the chief cause of data breaches in 2016 counting total by identities stolen. "Phishing, Spoofing, and Social Engineering" were a distant second at 6.4 percent. (Source:Symantec)*

https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

Insider Threat: Current Landscape

- 90% of organizations feel vulnerable to insider attacks.
  - The main enabling risk factors include too many users with excessive access privileges (37%), an increasing number of devices with access to sensitive data (36%), and the increasing complexity of information technology (35%).
- 53% confirmed insider attacks against their organization in the previous 12 months (typically less than five attacks).
- 27% of organizations say insider attacks have become more frequent.
- Data Loss Prevention (DLP), encryption, and identity and access management solutions. To better detect active insider threats, companies deploy Intrusion Detection and Prevention (IDS), log management and SIEM platforms.

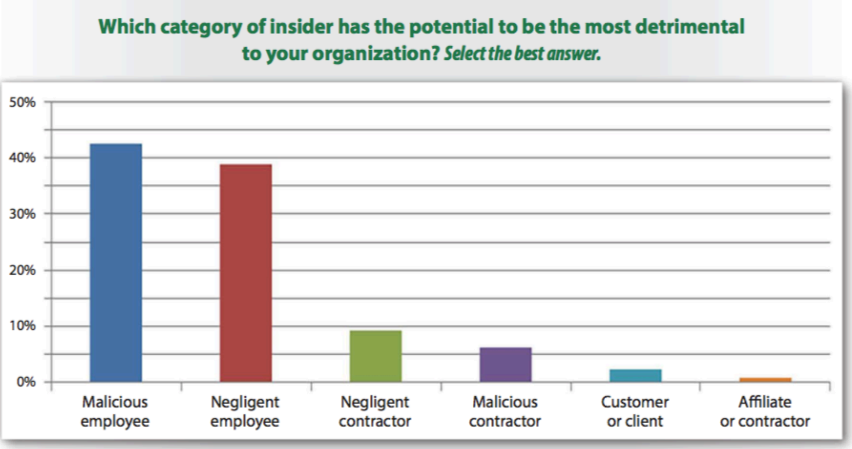
https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

Insider Threat: Current Landscape

- Almost **58%** of organizations that had security incidents over 2017 blamed them on insiders.
- **45%** respondents, whether or not they experienced a security incident, still see their own employees as the biggest threat to security.
- The majority of respondents have only partial visibility into what is happening in the cloud, and only **28%** of organizations have visibility into IT staff activity.

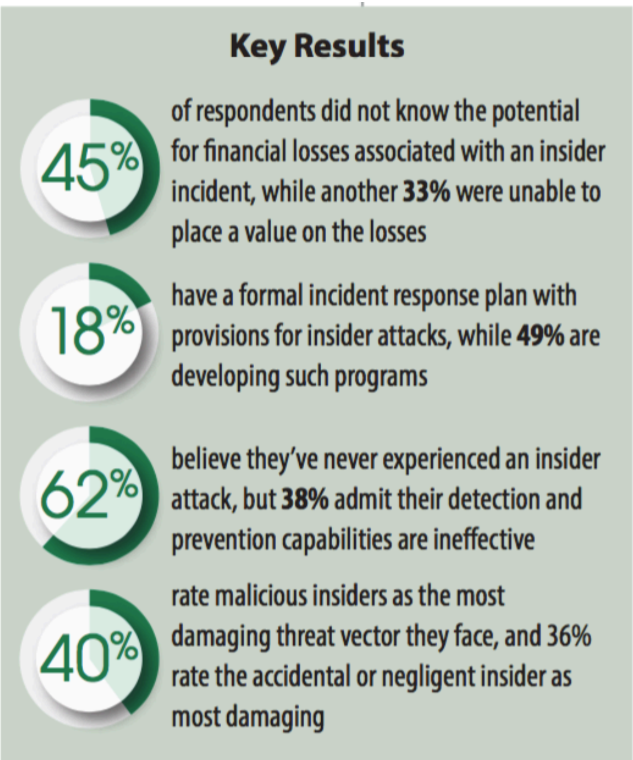
https://itsecuritycentral.teramind.co/2018/04/03/insider-threat-research-reports-and-sur
top-facts/

Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey



Which category of insider has the potential to be the most detrimental to your organization? *Select the best answer.*

Figure 11. Malicious and Negligent Employees Potentially Damaging



Key Results

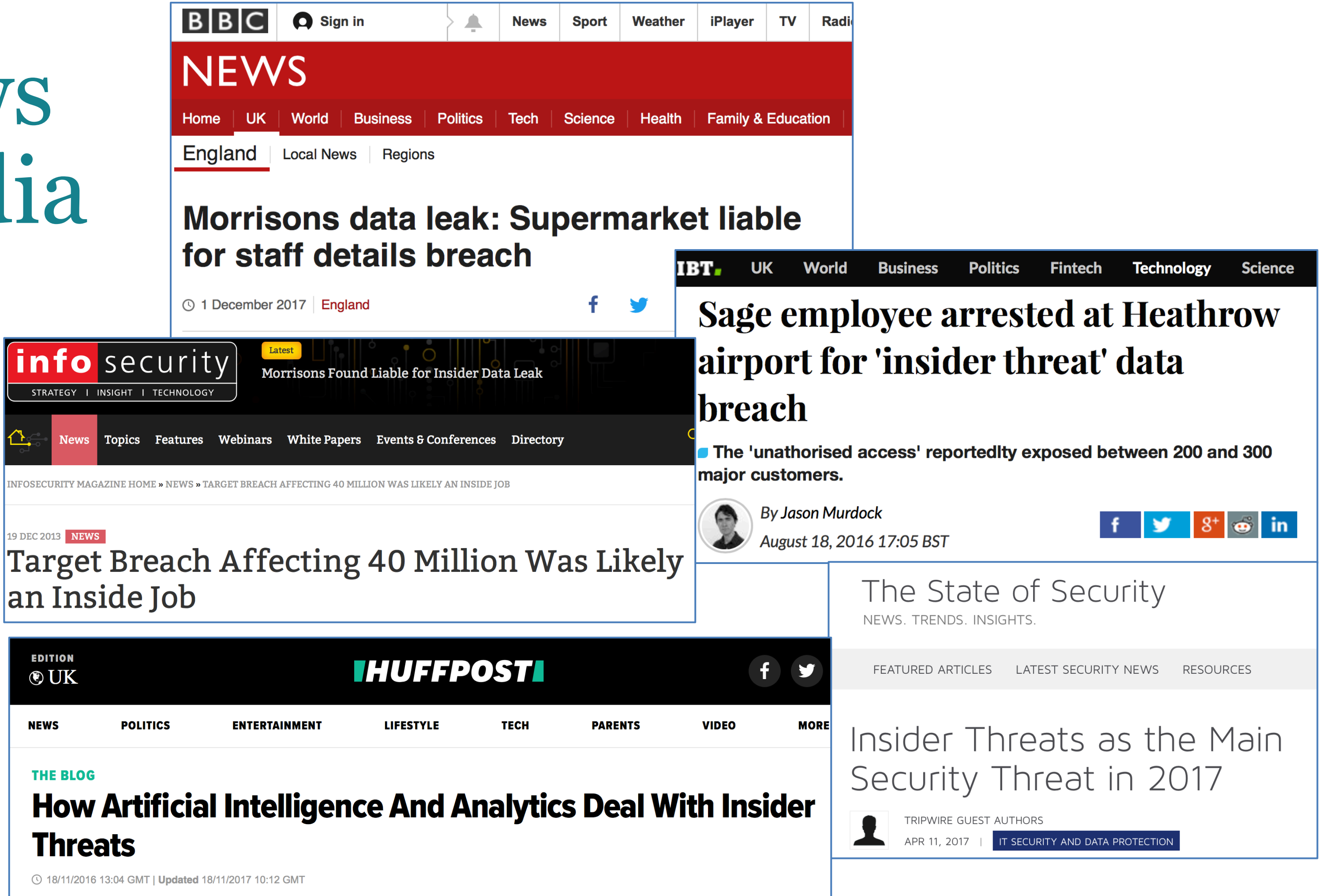
45% of respondents did not know the potential for financial losses associated with an insider incident, while another **33%** were unable to place a value on the losses

18% have a formal incident response plan with provisions for insider attacks, while **49%** are developing such programs

62% believe they've never experienced an insider attack, but **38%** admit their detection and prevention capabilities are ineffective

40% rate malicious insiders as the most damaging threat vector they face, and 36% rate the accidental or negligent insider as most damaging

News Media



BBC Sign in News Sport Weather iPlayer TV Radi

NEWS

Home UK World Business Politics Tech Science Health Family & Education

England Local News Regions

Morrisons data leak: Supermarket liable for staff details breach

1 December 2017 | England

IBT UK World Business Politics Fintech Technology Science

Sage employee arrested at Heathrow airport for 'insider threat' data breach

The 'unathorised access' reportedlty exposed between 200 and 300 major customers.

By Jason Murdock
August 18, 2016 17:05 BST

info security
STRATEGY | INSIGHT | TECHNOLOGY

Latest
Morrisons Found Liable for Insider Data Leak

News Topics Features Webinars White Papers Events & Conferences Directory

INFOSECURITY MAGAZINE HOME » NEWS » TARGET BREACH AFFECTING 40 MILLION WAS LIKELY AN INSIDE JOB

19 DEC 2013 NEWS

Target Breach Affecting 40 Million Was Likely an Inside Job

The State of Security
NEWS. TRENDS. INSIGHTS.

FEATURED ARTICLES LATEST SECURITY NEWS RESOURCES

Insider Threats as the Main Security Threat in 2017

TRIPWIRE GUEST AUTHORS
APR 11, 2017 | IT SECURITY AND DATA PROTECTION

EDITION
UK

HUFFPOST

NEWS POLITICS ENTERTAINMENT LIFESTYLE TECH PARENTS VIDEO MORE

THE BLOG

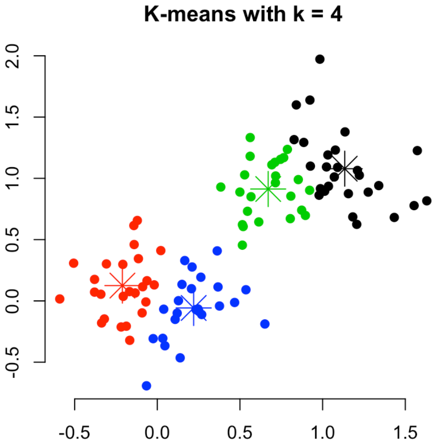
How Artificial Intelligence And Analytics Deal With Insider Threats

18/11/2016 13:04 GMT | Updated 18/11/2017 10:12 GMT

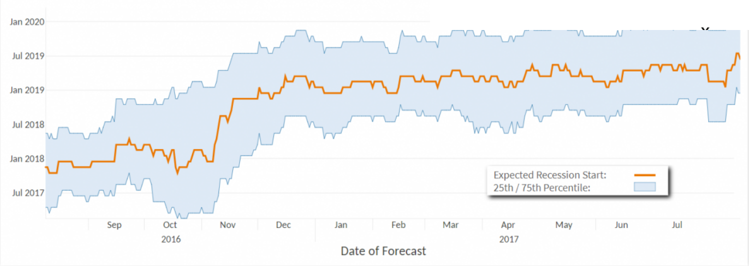
UWE Bristol University of the West of England

Artificial Intelligence

- AI works well for
  - classifying (cats v dogs)
  - clustering (similar users),
  - recognising patterns (time-series change)



- Works best when success can be quantified and when historical data is available



Behavioral Analytics

- AI has the potential to learn about ‘normal’ behaviour of users
  - If we can determine normal behaviour, can we then determine abnormal behaviour?

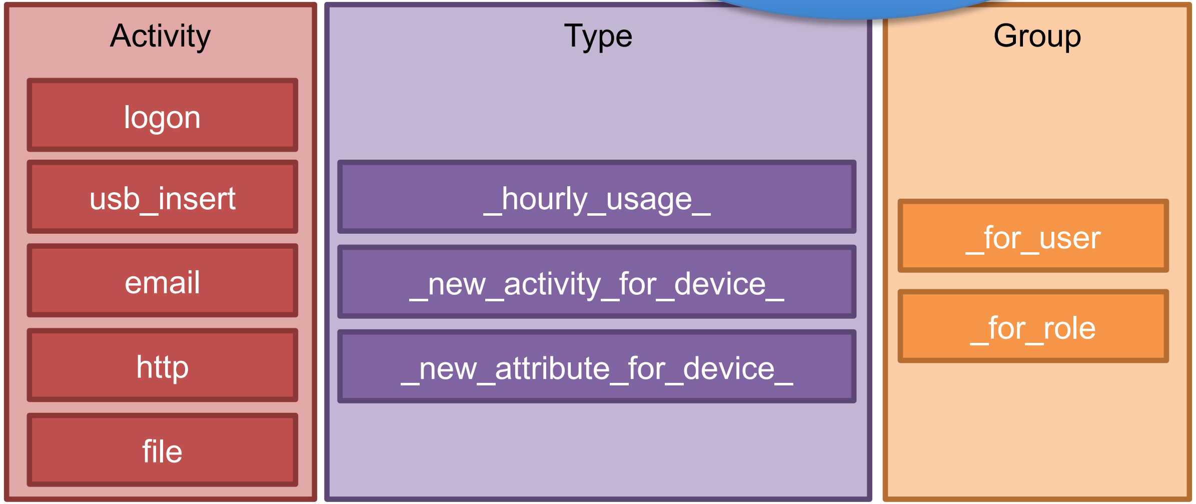
- How does an AI system achieve this?
  - Features! Typically numerical values that characterise behaviour of a user or a machine
    - Machine: CPU usage, #network connections, #processes executed
    - User: login time, #files accessed, #emails sent, #web pages browsed
      - Can assess #new events (so we know what is typical for a user)

How may we attempt to detect insider threat?

- What data can we gather about users?
  - Log-on, E-mail, USB, File access, Web access?
  - Job role (any other HR related data)?

- What kind of 'features' can we calculate based on users?

This describes 30 numerical 'features' for each user per day to characterize the user behaviour

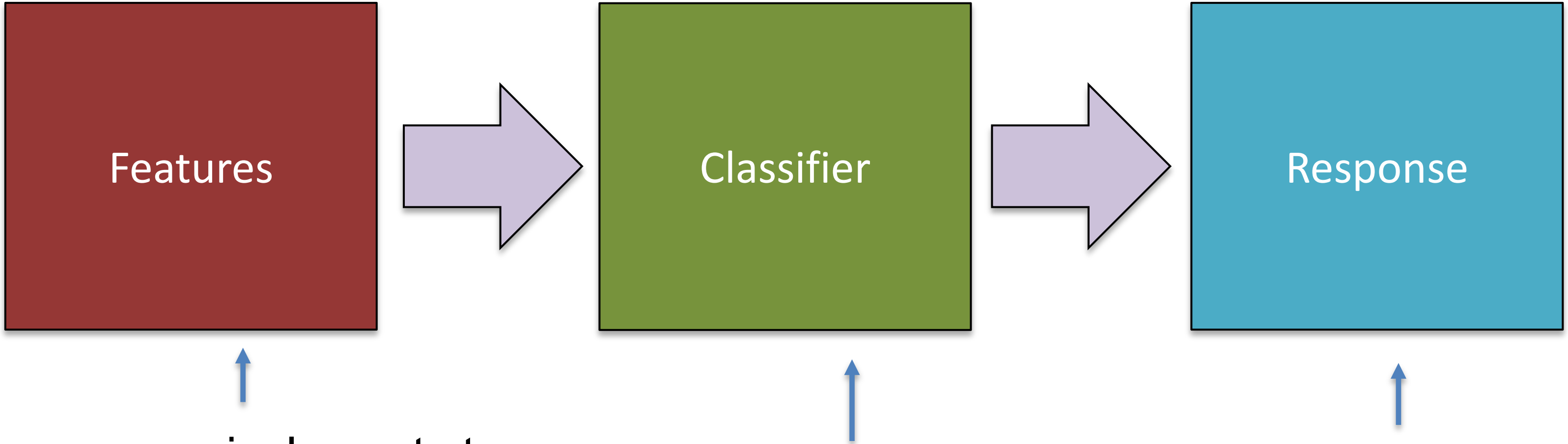


Activity
- logon
- usb_insert
- email
- http
- file

Type
- _hourly_usage_
- _new_activity_for_device_
- _new_attribute_for_device_

Group
- _for_user
- _for_role

AI to the rescue?



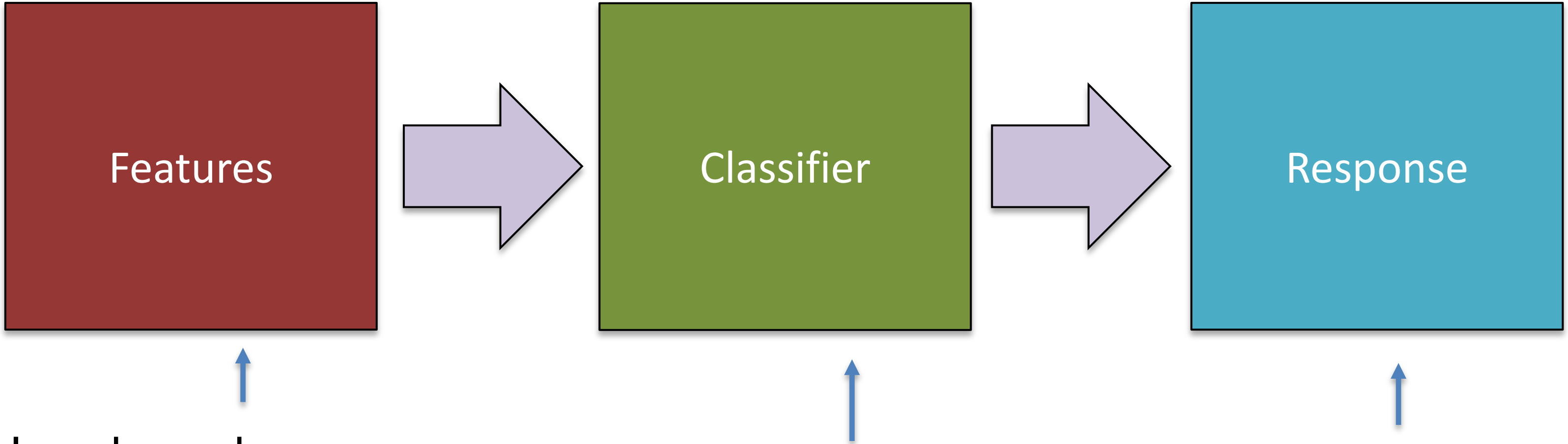
e.g., numerical counts to characterise activity

e.g., neural network, SVM,

e.g., threat / non-threat

e.g., some score of ‘normal’

AI to the rescue?



Features

Classifier

Response

How do we know we have suitable features?

How do we know this is learning well?

What does it really mean to be abnormal? Does abnormal mean malicious?

Takeaway

- Cybercrime and insider threat are dynamic challenges and constantly evolving!

- AI works well for classifying (cats v dogs), clustering (similar users), recognising patterns (time-series change) – works best when success can be quantified and when historical data is available

- Data 'features' are the biggest challenge – images rely on pixels to show the full picture, however other domains can be more challenging
    - Only have a partial view on employee activity – so we need to account for uncertainty. How do you measure more abstract features such as 'employee disgruntlement', or 'personal hardship'?

- Attackers will **always** aim to circumvent the 'features' of your detection tool over time – so the distribution of the trained model may be unreliable for predicting or detecting future events.

- AI Assistant / active learning / human-in-the-loop – use statistics and models to filter and analyse the available data, identify outlier cases. Time-series analysis and cluster analysis to identify behavioural changes. Interactive AI is required for complex decision-making tasks.

Thank you

Phil.Legg@uwe.ac.uk
@dr_plegg
2Q17, Frenchay, UWE

http://go.uwe.ac.uk/phil
http://www.plegg.me.uk

Related References:

- Legg, P. (2017) Human-machine decision support systems for insider threat detection . In: Palomares, Iván, Kalutarage, H. and Huang, Y., eds. (2017) Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications. Springer. ISBN 9783319594385 [In Press] Available from: http://eprints.uwe.ac.uk/31385
- Legg, P. A. (2015) Visualizing the insider threat: Challenges and tools for identifying malicious user activity . In: IEEE Symposium on Visualization for Cyber Security, Chicago, Illinois, USA, 26 October 2015. IEEE Symposium on Visualization for Cyber Security (VizSec) 2015: IEEE Available from: http://eprints.uwe.ac.uk/27441
- Legg, P. A., Buckley, O., Goldsmith, M. and Creese, S. (2015) Caught in the Act of an Insider Attack: Detection and Assessment of Insider Threat. In: *IEEE International Symposium on Technologies for Homeland Security*, Waltham, USA, 14th-16th April 2015. Available from: http://eprints.uwe.ac.uk/26244
- Legg, P., Buckley, O., Goldsmith, M. and Creese, S. (2015) Automated insider threat detection system using user and role-based profile assessment.*IEEE Systems Journal*, 11 (2). pp. 503-512. ISSN 1932-8184 Available from: http://eprints.uwe.ac.uk/25809

UWE Bristol University of the West of England