Who will be the next Mossack Fonseca?

> The Insider Security Threat

Dr. Mary Haigh
Head of Threat Analytics
BAE Systems

BAE SYSTEMS PROPRIETARY

BAE SYSTEMS
INSPIRED WORK

Business Defence for Insurers

COUNTER FRAUD

- POINT OF QUOTE, SALE & CLAIM
- DATA PARTNERSHIPS
- ADVANCED SIU ANALYTICS

COMPLIANCE

- SANCTIONS & PEPS
- AML
- CUSTOMER DUE DILIGENCE

CYBER SECURITY

- CYBER RISK ASSESSMENT
- MANAGED SECURITY SERVICES
- INCIDENT RESPONSE

WE PROTECT LEADING INSURERS AGAINST COMPLEX EMERGING THREATS

BAE SYSTEMS PROPRIETARY

BAE SYSTEMS
INSPIRED WORK

The Unusual Suspects

Cyber threats, methods and motivations

BAE SYSTEMS
INSPIRED WORK

The Mule

The Mule is motivated by greed or desperation. They are the final link in the chain – and most vulnerable to arrest.

The Professional

They work a 9-to-5 day job that looks legitimate – but the reality couldn't be further from the truth.

The Nation State Actor

The Nation State Actor has a 'Licence to Hack' – and they use it to target their adversaries.

The Activist

Whatever their cause, it's a burning one. The Activist's tactics cross the line from legitimate protest into criminality.

The Getaway

The Getaway is too young to go to jail: even if they're caught, they're unlikely to get more than a slap on the wrist.

The Insider

They're fed up, blackmailed, or just being really helpful. Your business' defences are wide open to the Insider.

BAEsystems.com/unusualsuspects

It's not just security. It's defence.

Insider Threats

> Is a big problem

Losing data – external attacks **AND** insider attackers.

Employee negligence or maliciousness is the root cause of many data breaches.

78% of respondents say negligent or malicious employees or other insiders have been responsible for at least one data breach within their organizations over the past two years.

Around **1 in 1,000** employees are thought to be malicious insiders.

BAE SYSTEMS PROPRIETARY

BAE SYSTEMS
INSPIRED WORK

The Insider

A disillusioned employee, a blackmail target or just greedy – they've got the keys to the castle, and they're much more effective than malware, OR, they're well intentioned but unaware of the damage they might cause if used by criminals

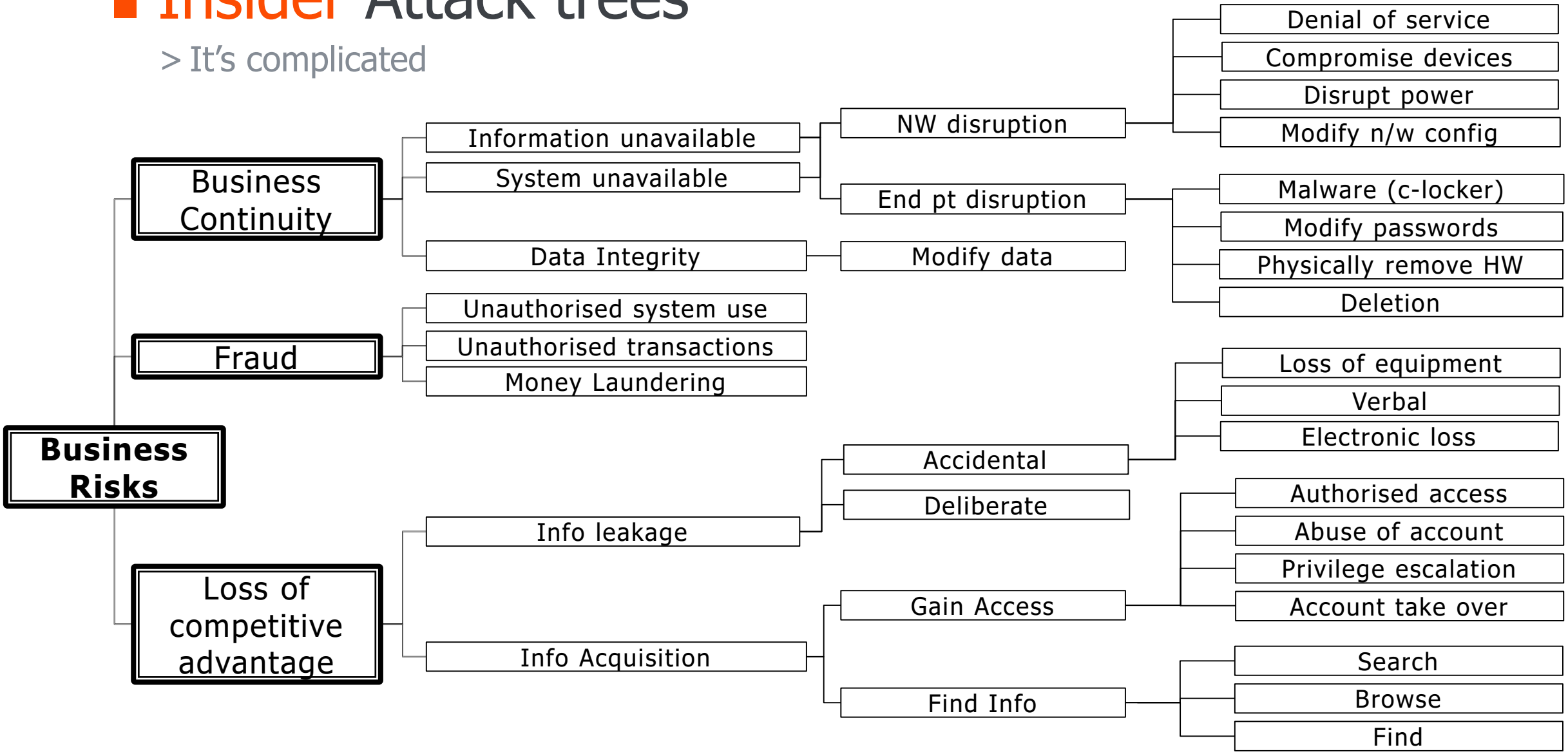
The Insider is one of the hardest suspects to identify and defend against. The Insider's position within the organisation can mean they can do just as much damage as the most sophisticated piece of malware.

BAE SYSTEMS PROPRIETARY

BAE SYSTEMS
INSPIRED WORK

Insider Attack trees

> It's complicated



BAE SYSTEMS PROPRIETARY

BAE SYSTEMS
INSPIRED WORK

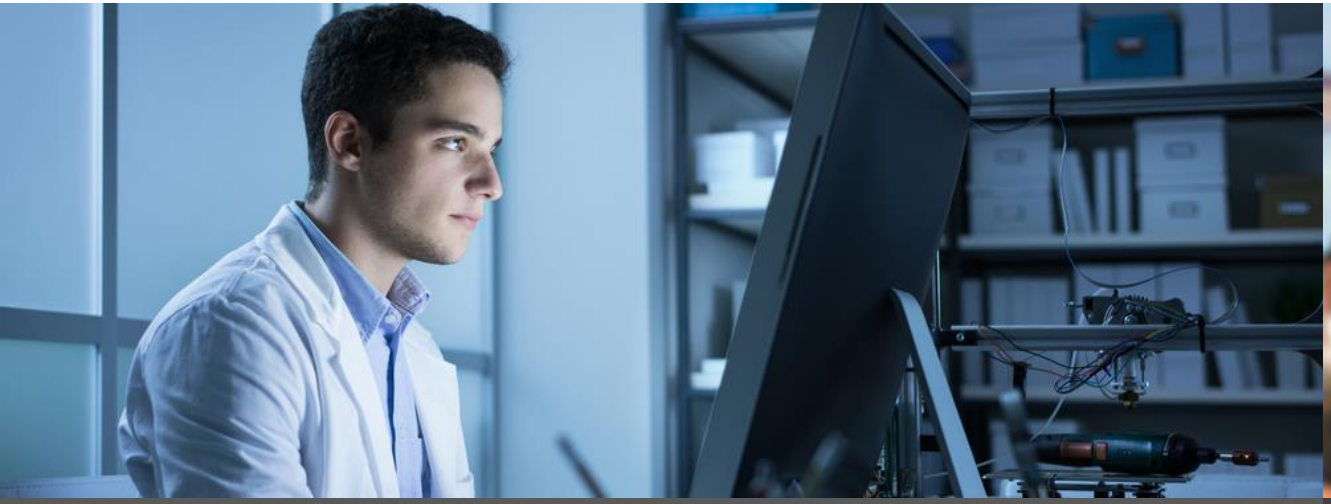
Insider Threats

> The different faces of the insider

MALICIOUS/ACCIDENTAL		
THEFT	SABOTAGE	FRAUD
Stealing intellectual property & information to gain competitive advantage or for money	Impacting the ability of the organisation to do business.	Abusing the capabilities of the organisation usually for money.

Theft

> The entitled independent vs the plant



- They’ve created that brilliant design or idea
- They are now moving onto a new job
- That idea belongs to them in their mind

- Target whole product / business line
- A plant or out to set up in competition
- Recruit Helpers

BAE SYSTEMS PROPRIETARY

Sabotage

> Insiders hit where it hurts

- Disillusioned employee turns nasty
- Network Admin Case study
  - Re-assigned after reprimanded for poor performance
  - Refused to hand over passwords
  - Re-configured network devices
  - Went to jail
  - After 12 day standoff mayor visited his prison cell

BAE SYSTEMS PROPRIETARY

Fraud

> Everything has a price

- Its tempting.
  - Get £250 to check someone's licence.
- Poor role based access control:
  - Could generate drivers licences
  - Arrested after issuing 195 illegal licences

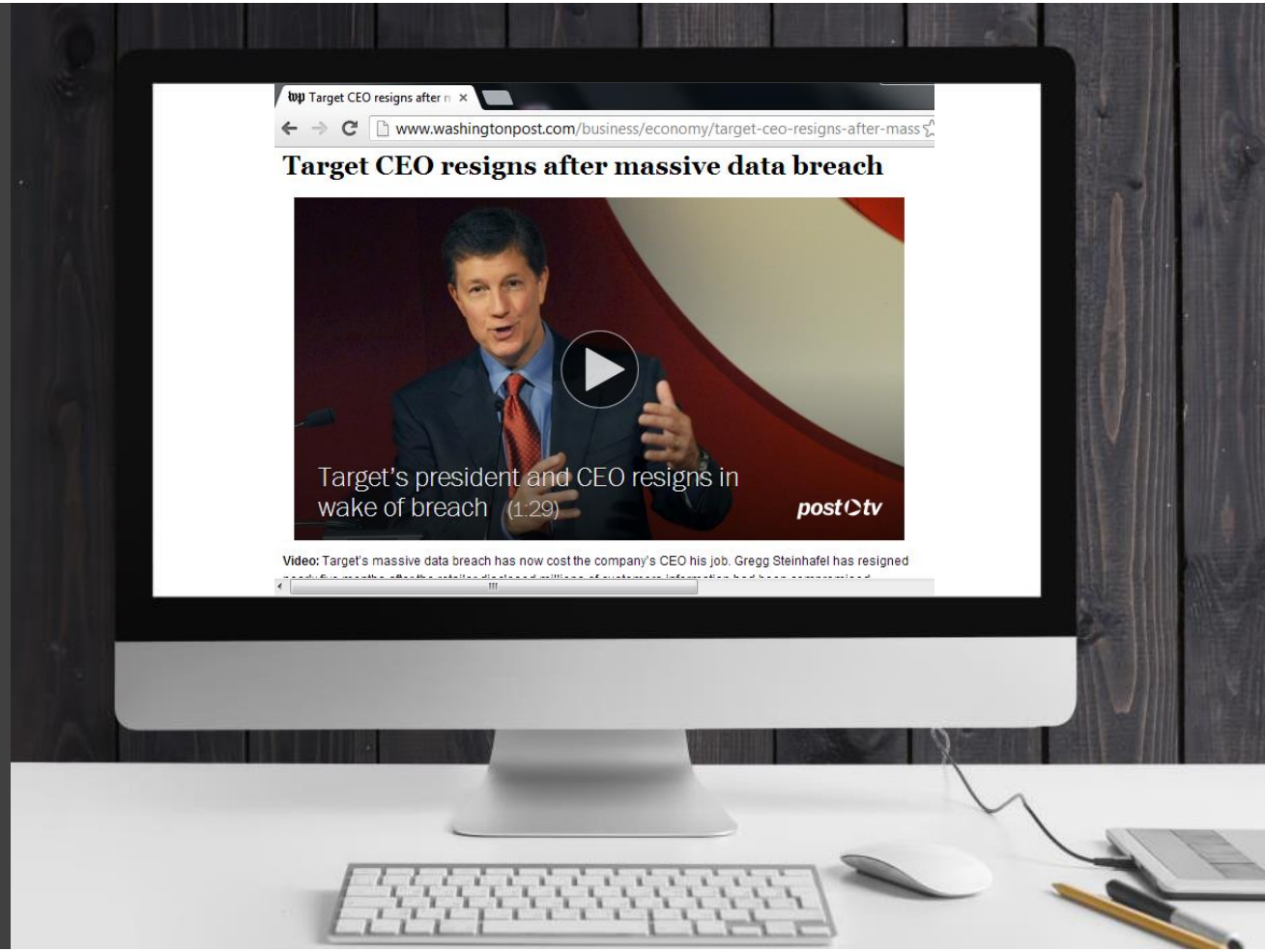
BAE SYSTEMS PROPRIETARY

BAE SYSTEMS
INSPIRED WORK

Insider

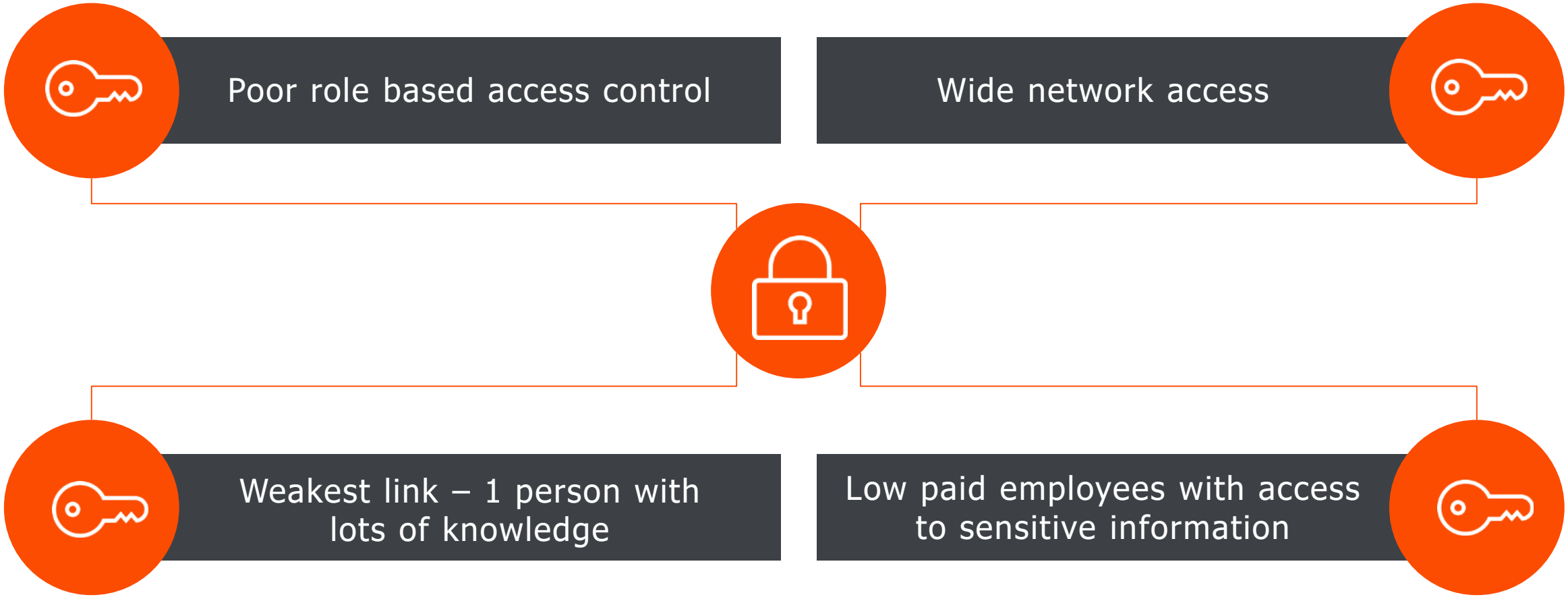
> Don’t forget your supply chain

- Increasingly attackers are using supply chain as a way in – they are often the weak link
  - Target
  - Home Depot
- Also true for insiders



The Anatomy of the Attack

> Common Themes



BAE SYSTEMS PROPRIETARY

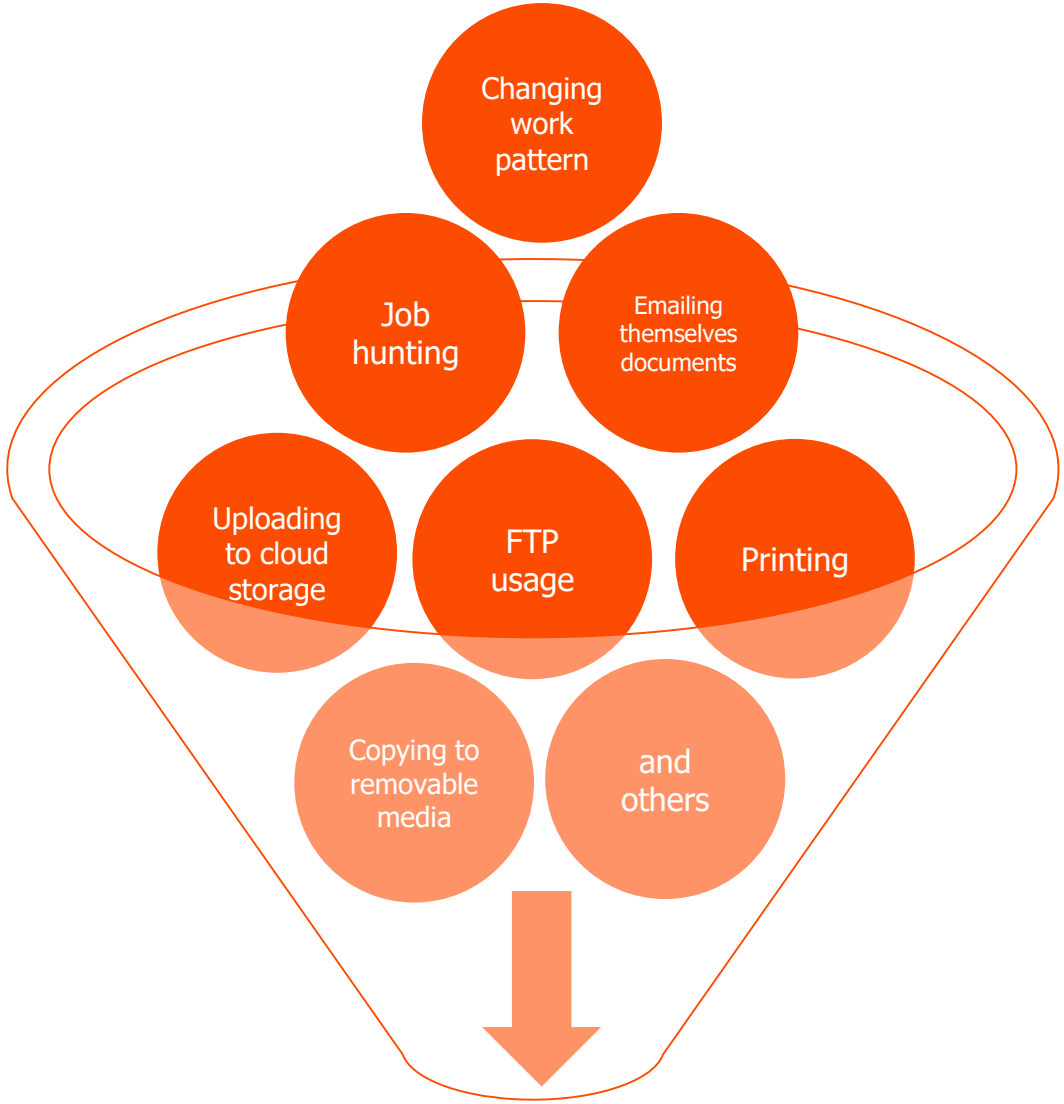
Their Undoing…

> How to catch them

PEOPLE, PROCESS & TECHNOLOGY

TECHNOLOGY: ADVANCED ANALYTICS

- Big Data - collect information across your network through time
- Analyse the data and look for multiple behaviours indicative of insiders
- Risk each behaviour and bring together into a single risk score



Potential Malicious Insider

BAE SYSTEMS
INSPIRED WORK

Their Undoing…

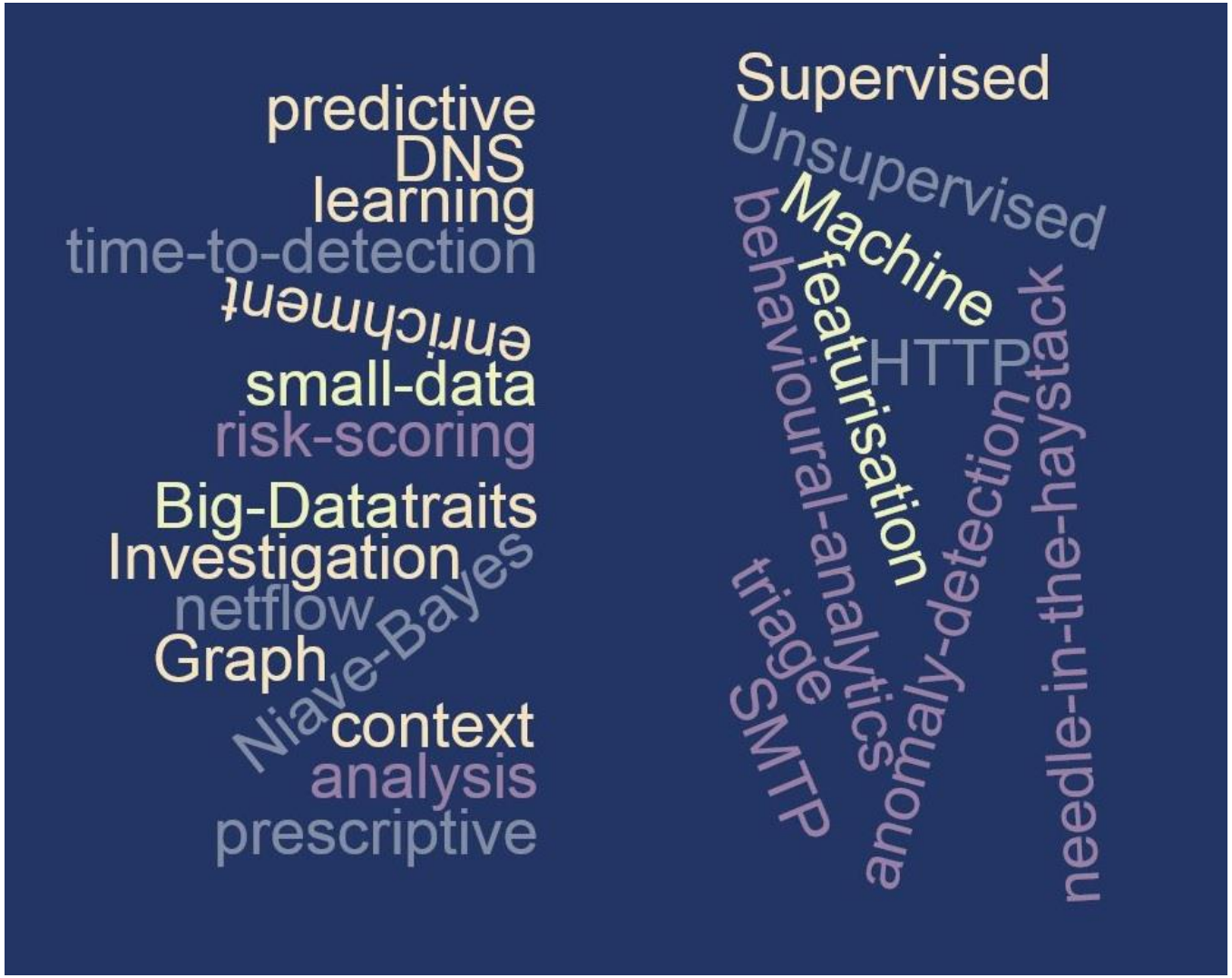
> The key to detection

Know your enemy

Cyber domain knowledge, threat intelligence

Know how to find your enemy

Data science



BAE SYSTEMS PROPRIETARY

Thank You

BAE SYSTEMS PROPRIETARY

BAE SYSTEMS
INSPIRED WORK

FREEDOM OF INFORMATION ACT

This document (<projectreference><documentnumber>) contains confidential and commercially sensitive material which is provided for the Authority's internal use only and is not intended for general dissemination.

The information contained herein pertains to bodies dealing with security, national security and/or defence matters that would be exempt under Sections 23, 24 and 26 of the Freedom of Information Act 2000 (FOIA). It also consists of information which describes our methodologies, processes and commercial arrangements all of which would be exempt from disclosure under Sections 41 and 43 of the Act.

Should the Authority receive any request for disclosure of the information provided in this document, the Authority is requested to notify BAE Systems Applied Intelligence. BAE Systems Applied Intelligence shall provide every assistance to the Authority in complying with its obligations under the Act.

BAE Systems Applied Intelligence's point of contact for FOIA requests is:

Chief Counsel
Legal Department
BAE Systems Applied Intelligence
Surrey Research Park
Guildford Gu2 7YP
Telephone 01483 816082

BAE SYSTEMS
Surrey Research Park
Guildford
Surrey
GU2 7YP
United Kingdom

T: +44 (0)1483 816000
F: +44 (0)1483 816144