Handout Notes: Cybercrime, Psychology, and the M&S Attack

VRA — 22 January 2026

Slide 1 – Three Card Monte and Social Engineering

In the mid-1980s, I was walking down Park Lane with school friends when we came across a street scammer running the classic "Three Card Monte" outside a hotel. Many people know it's a scam and assume they're too clever to fall for it. Yet the trick has very little to do with card manipulation. It's an intricately staged performance involving multiple accomplices ("shills"), all working together to lure observers into believing the game is beatable.

This story illustrates the essence of social engineering. It isn't just a metaphor for cyberattacks—many modern attacks operate on the same psychological principles. Social engineering is simply con artistry at scale.

Slide 2 – Historical Roots of the Con

The techniques behind these scams are far from new. In William Powell Frith's 1858 painting *The Derby Day*, we see a "thimble rigger" running a similar deception. The dynamic is instantly recognisable: A distracted victim, an opportunistic con artist, and the social pressure that encourages people to take risks they shouldn't.

Slide 3 – Even Older Deceptions

Earlier still, Hieronymus Bosch's *The Conjurer* (c.1502) shows another variation of the scam. A performer distracts the crowd with a cup-and-ball routine while an accomplice steals from the wealthy onlooker. The lesson here is that we often look for complex explanations when the con is actually very simple. The psychological principles have not changed in centuries.

This talk focuses on those psychological aspects of cybercrime, and uses the Marks & Spencer ransomware attack as a case study. All details discussed are in the public domain.

Although much of cybersecurity discourse feels grim, it is important to note that defensive capabilities are improving. The industry is fighting back.

Slide 4 – Psychological Factors Exploited by Attackers

Cybercriminals and con artists both exploit a set of predictable human tendencies:

- **Truth bias** – We assume most things are legitimate unless proven otherwise.
- **Illusion of personal immunity** – We believe that *other* people are vulnerable to scams, but we are not.
- **Proportionality bias** – We expect large outcomes to have large, sophisticated causes.
- **Confirmation bias** – We interpret new information as supporting what we already believe.
- **Social proof** – If others appear to be doing something safely, we assume it must be safe.

This is consistent with Robert Cialdini's 7 psychological principles of persuasion: Reciprocity, Commitment, Social Proof, Respect, Authority, Scarcity - often manipulated as urgency & greed - and Unity. Hacker Conversations: Rachel Tobac and the Art of Social Engineering - SecurityWeek

These tendencies evolved to help us make fast decisions. They are features of human cognition—but in cybersecurity, they become liabilities.

Slide 5 – Causes of Cyber Incidents

Data shows that 56% of cyber incidents originate from employee negligence, yet management tends to believe the primary cause is credential theft.
This mismatch highlights a fundamental misunderstanding: Many breaches do not rely on advanced technical exploits. Instead, they hinge on human error, manipulation, or coercion. The “hack” often begins long before any technology is involved.

Slide 6 – Key Lessons About Human Vulnerabilities

From these observations, several overarching lessons emerge:

1. Human mental shortcuts are adaptive features, refined over billions of years.
2. Con artists have exploited these traits for millennia.
3. Humans evaluate risk effectively, but only within certain contexts.
4. Victim-blaming is misguided; our behaviours are shaped by innate cognitive patterns.

5. We overestimate the complexity of sophisticated outcomes.
6. Organisations frequently misunderstand where they are vulnerable.

History provides countless examples of cities that fell because a traitor opened the gates: Troy, Sardis, Tyre, Antioch, Constantinople, Granada, and more. Breaches rarely begin outside the walls—the failure typically comes from the inside.

Slide 7 – Cybercrime as a Global Economic Force

Cybercrime is now a major global industry. Its impact is significant enough that events such as the JLR outage were cited by government officials as contributors to reduced economic productivity. The scale of the threat is now widely recognised.

Slide 8 – The Automotive Sector Under Threat

The automotive sector has been a high-value target for cybercriminals for many years. Increasing digitisation and interconnected systems have expanded the attack surface, making it especially vulnerable. Speaking with Eddie Hawthorne from Arnold Clark it emerged that the cybercriminals were tough, well informed, and very good at their "job". But you don't need to outrun the bear, only your companions.

Slide 9 – Nation-State Cybercrime Ecosystems

Several major nation states are deeply involved in cybercrime:

- **Russia:** State-approved actors are responsible for roughly 80% of global ransomware revenue.
- **China:** Accusations of commercial cyber espionage tied to national industrial strategy (*Made in China 2025*).
- **North Korea (Lazarus Group):** Cyber operations used to generate foreign currency in defiance of sanctions.
- **Iran:** A mixture of espionage, criminal activity, and disruptive attacks as a tool of asymmetric warfare.

These examples show that cybercriminals are not just isolated individuals, but part of sophisticated ecosystems.

Ironically, the M&S attack was not carried out by nation-state professionals but by a group of young English-speaking hackers.

Slide 10 – The M&S Attack: Impact and Context

The Marks & Spencer ransomware attack caused an estimated **£300 million** reduction in operating profit, with around half recoverable through insurance. The market capitalisation fell by approximately **£1 billion**, and the brand suffered significant reputational damage.
The attack was carried out by the group **Scattered Spider**. Co-op and Harrods were also targeted.
The attackers used the "Dragon Force" ransomware platform, possibly through a ransomware-as-a-service model.
The initial breach appears to have started within the TCS-operated helpdesk.

Slide 11 – How the Attack Worked

The attack followed the typical social-engineering-driven ransomware pattern:

1. **Social engineering:** phishing emails and fraudulent calls.
2. **Impersonation:** attackers posed as trusted colleagues to extract credentials.
3. **Unauthorised access:** login details allowed entry into the network.
4. **Data exfiltration:** sensitive data and intellectual property were stolen.
5. **Ransomware deployment:** data was encrypted, and ransom demanded.

Notably, the first genuinely technical step occurs only at step 4. The preceding stages are psychological, not technical—directly comparable to classic confidence tricks.

Slide 12 – Who Are Scattered Spider?

Scattered Spider is a loosely organised collective of young English-speaking men, primarily in the US and UK. They operate more like a decentralised cult than a formal criminal organisation. While financially motivated, the group also focuses on indoctrinating new recruits.
The individuals arrested for the M&S attack were reportedly among their newest members.
Scattered Spider is linked to a broader network called **The Com**, which engages in:

- Sextortion and child exploitation
- Cybercrime across multiple sectors
- Physical threats and violence
- Fraud and financial schemes

The Com operates across platforms such as Discord and Telegram, making it difficult to detect or disrupt. Many recruits are vulnerable young people drawn into these toxic online communities. These crimes are not victimless—they have real and serious consequences.

Slide 13 – What Organisations Must Keep Doing

Cybersecurity isn't solved by any single action. It requires sustained discipline across several areas:

1. **Perimeter security is necessary but not sufficient.**
   Traditional defences matter, but attackers now routinely bypass them through social engineering and insider manipulation.
2. **Manage access rights.**
   Because attackers often gain entry through compromised employees, controlling internal permissions is critical. The bad actors are frequently "already inside the building."
3. **Eliminate Shadow IT.**
   Unapproved tools and systems create blind spots and vulnerabilities. Security must be prioritised above convenience.
4. **Understand the implications of Artificial Intelligence.**
   AI expands both defensive capability and attacker capability. Organisations must grasp its risks and opportunities—not ignore them.
5. **Manage supply chain risk.**
   Third parties are now one of the most common sources of breaches. Security must extend beyond organisational boundaries.
6. **Have an incident response plan; practise it; follow it.**
   A plan is only useful if it is rehearsed and adhered to under pressure.
7. **Follow Government guidance, especially from the NCSC.**
   Practical, well-tested frameworks already exist. Organisations should use them.

8. **Build a security-aware culture.**
   Leadership must model good cyber hygiene. Culture—not technology—is the most enduring defence.