Social Engineering Attacks and the Risks of Weaponized Psychology

Christina Lekati

Social Engineering Security Trainer & Consultant

Cyber Risk GmbH

About Me

Christina Lekati

- Psychologist & Social Engineer
- Trainer & Consultant for Cyber Risk GmbH on the Human Element of Security
- Social Engineering & Security Awareness Trainings to All Levels of Employees / Security Teams
- Corporate & High-Value Target Vulnerabilities Assessments
- Board Member of the OSINT Curious project

#OSINTCURIOUS
OSINTCURIO.US

Evolution of Cyber Security

Computer Security

Securing a machine/ group of machines by hardening the Software and Hardware

Network Security

Securing the integrity of networks against unauthorized access

Cyber Security

Securing the integrity of devices, networks, information from unauthorized access or damage

Evolution of Cyber Security

Cyber Security

Securing the integrity of devices, networks, information from unauthorized access or damage

⇄

Information Security

Protection of sensitive data and information from unauthorized access.
(in any form: print, verbal electronic etc.)

“*A cost-effective way to steal secrets*”

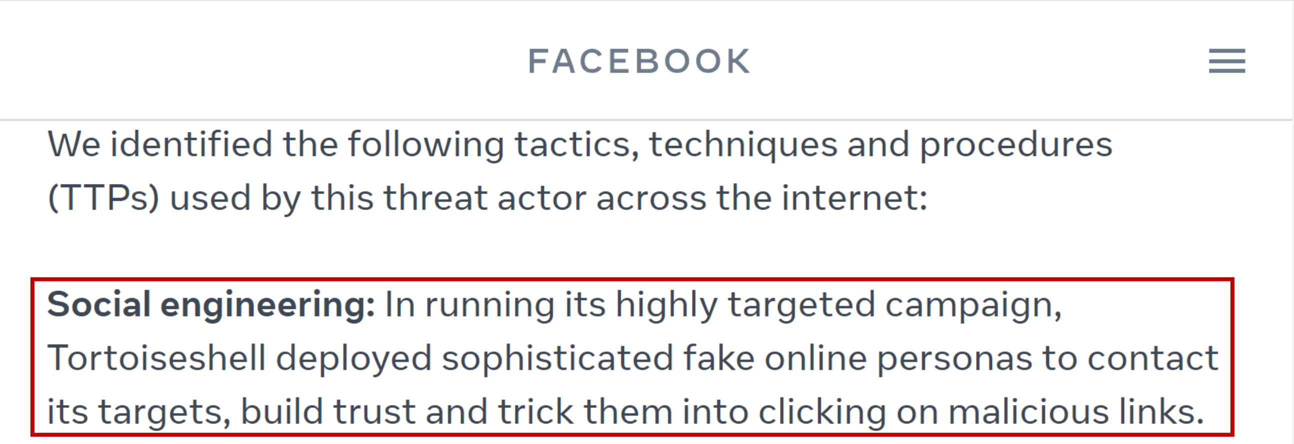
“The ends did not always justify the means we chose to employ.

<u>But, as long as there is espionage, there will be Romeos seducing unsuspecting Juliets with access to secrets</u>.

After all, I was running an intelligence service, not a lonely-hearts club."

This was a classic example of weaponized psychology.

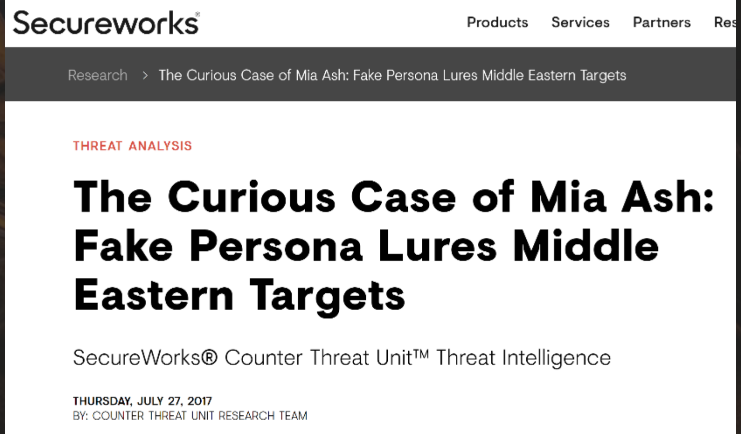
Do These Operations STILL Happen Today?!



FACEBOOK

We identified the following tactics, techniques and procedures (TTPs) used by this threat actor across the internet:

Social engineering: In running its highly targeted campaign, Tortoiseshell deployed sophisticated fake online personas to contact its targets, build trust and trick them into clicking on malicious links.



Secureworks — Products · Services · Partners · Res

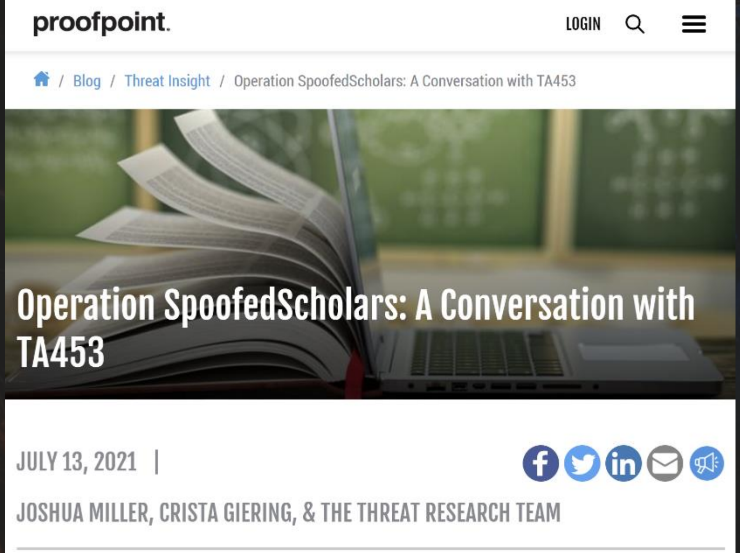
Research > The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets

THREAT ANALYSIS

The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets

SecureWorks® Counter Threat Unit™ Threat Intelligence

THURSDAY, JULY 27, 2017
BY: COUNTER THREAT UNIT RESEARCH TEAM



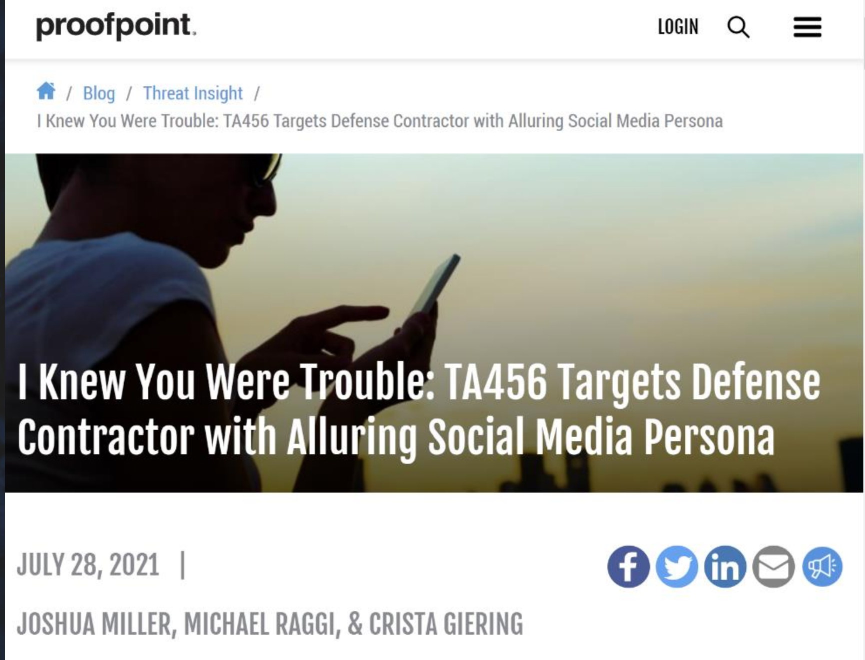
proofpoint. — LOGIN

Blog / Threat Insight / Operation SpoofedScholars: A Conversation with TA453

Operation SpoofedScholars: A Conversation with TA453

JULY 13, 2021 |

JOSHUA MILLER, CRISTA GIERING, & THE THREAT RESEARCH TEAM



proofpoint. — LOGIN

Blog / Threat Insight /
I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona

I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona

JULY 28, 2021 |

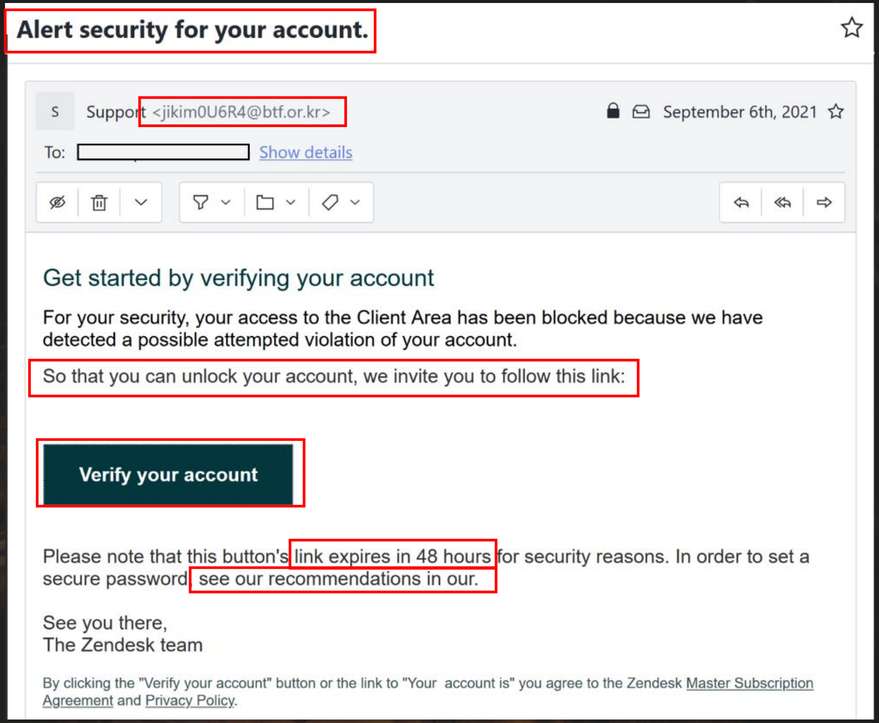
JOSHUA MILLER, MICHAEL RAGGI, & CRISTA GIERING

Sources:

- https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/
- https://www.secureworks.com/research/the-curious-case-of-mia-ash
- https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media
- https://www.proofpoint.com/us/blog/threat-insight/operation-spoofedscholars-conversation-ta453?utm_source=social_organic&utm_social_network=twitter&utm_campaign=21_July_Corporate_blog+&utm_post_id=ccf4c45f-a244-4163-8b61-f55737f869ff

Social Engineering Attacks Have Evolved

“Hit-and-Run”



Alert security for your account.

S Support <jikim0U6R4@btf.or.kr> September 6th, 2021

To: Show details

Get started by verifying your account

For your security, your access to the Client Area has been blocked because we have detected a possible attempted violation of your account.

So that you can unlock your account, we invite you to follow this link:

Verify your account

Please note that this button's link expires in 48 hours for security reasons. In order to set a secure password see our recommendations in our.

See you there,
The Zendesk team

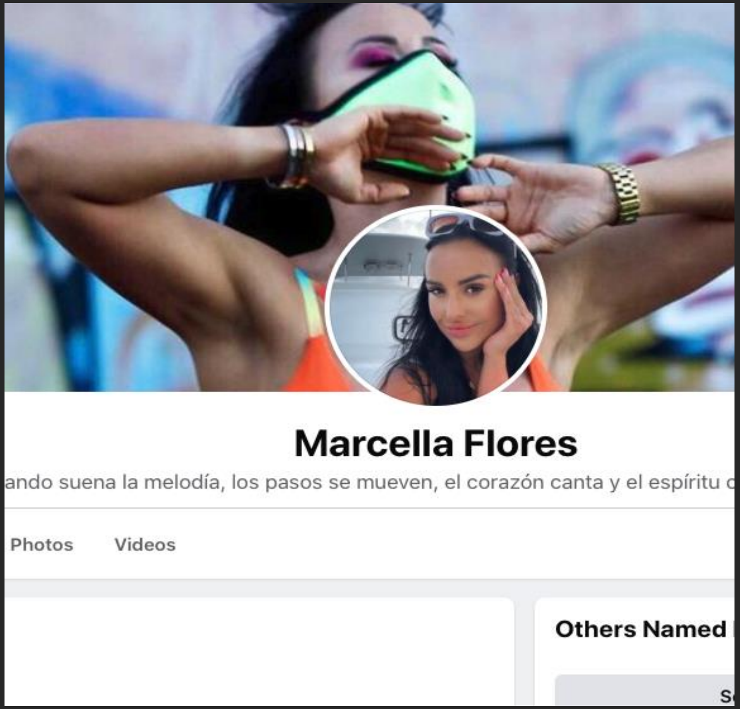
By clicking the "Verify your account" button or the link to "Your account is" you agree to the Zendesk Master Subscription Agreement and Privacy Policy.

VS

More elaborate campaigns:

- Longer reconnaissance
- Tailored/ Personalized approach
- More elaborate mind-games
- Deep-fakes
- Ongoing, state-sponsored social engineering campaigns

Case Study: Marcella (Marcy) Flores



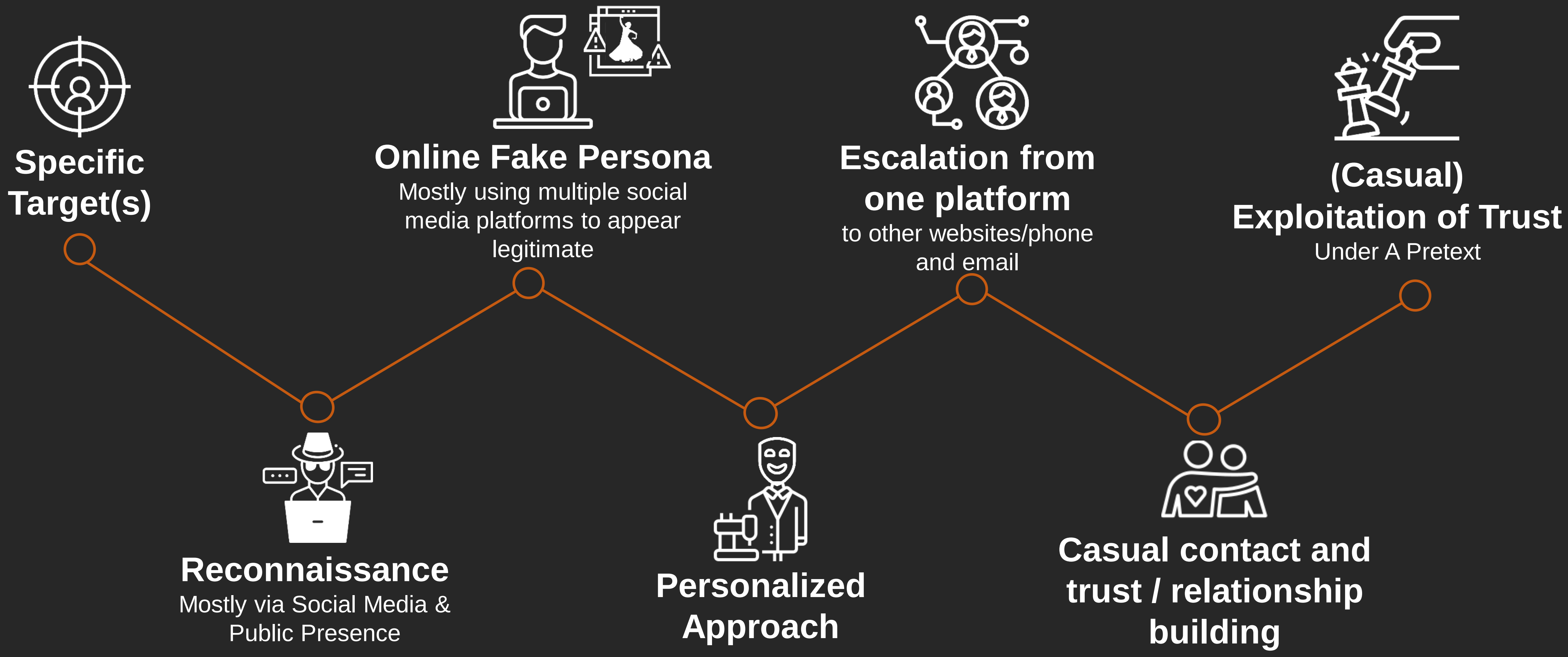
Marcella Flores

ando suena la melodía, los pasos se mueven, el corazón canta y el espíritu c

Source: https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media

- Years-long Social Engineering operation targeting an employee of an aerospace defence contractor
- “Marcella Flores” befriends the employee — 2019
- First evidence of communication — Nov. 2020
- “She” builds a relationship with him across corporate and personal communication platforms
- The threat actor sends the target malware via an ongoing email communication chain — June 2021
- The “LEMPO” malware is designed to “establish persistence, perform reconnaissance, and exfiltrate sensitive information. ”

Kill-Chain Backbone



Specific Target(s)

Reconnaissance
Mostly via Social Media & Public Presence

Online Fake Persona
Mostly using multiple social media platforms to appear legitimate

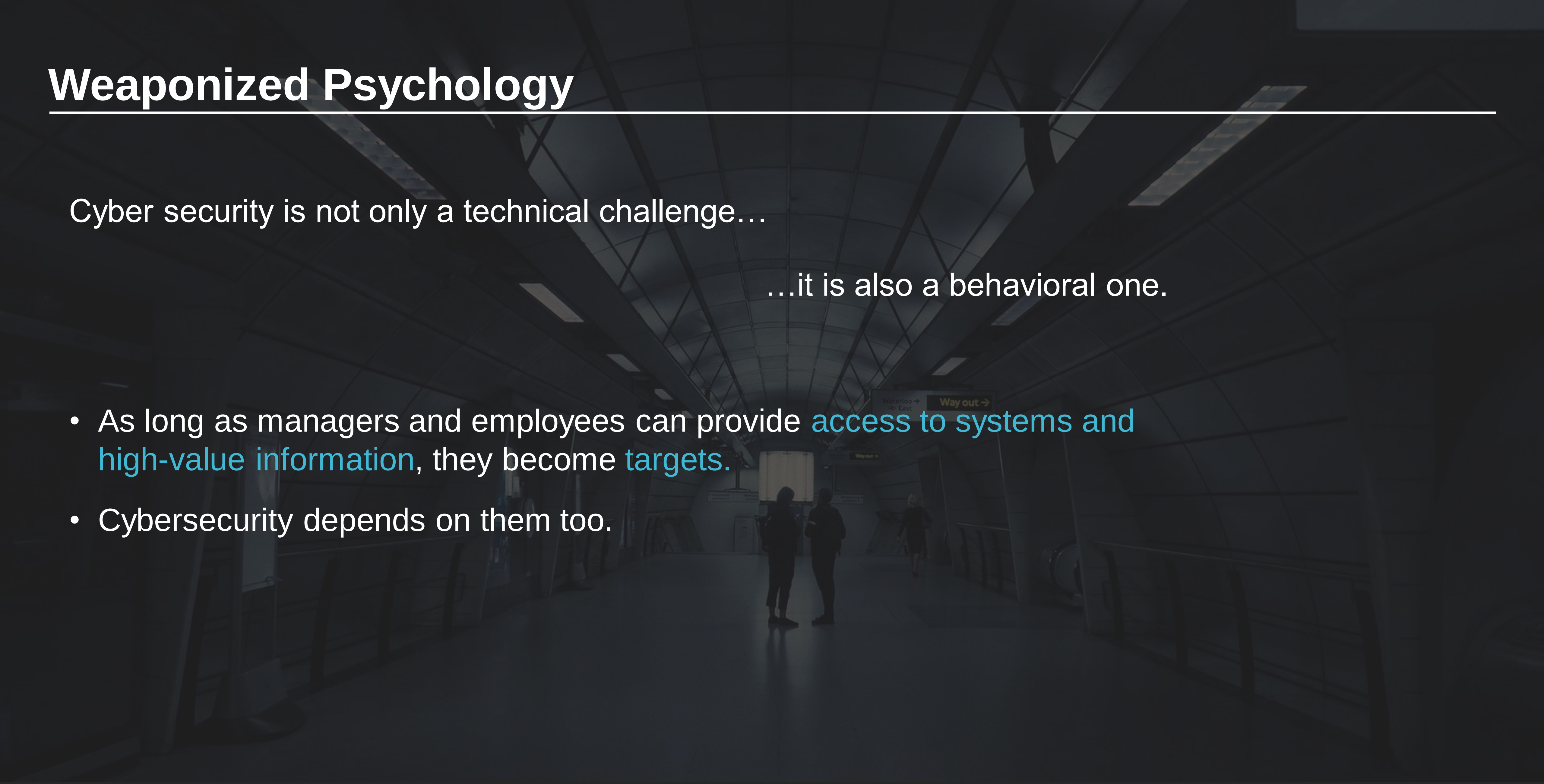
Personalized Approach

Escalation from one platform
to other websites/phone and email

Casual contact and trust / relationship building

(Casual) Exploitation of Trust
Under A Pretext

Weaponized Psychology

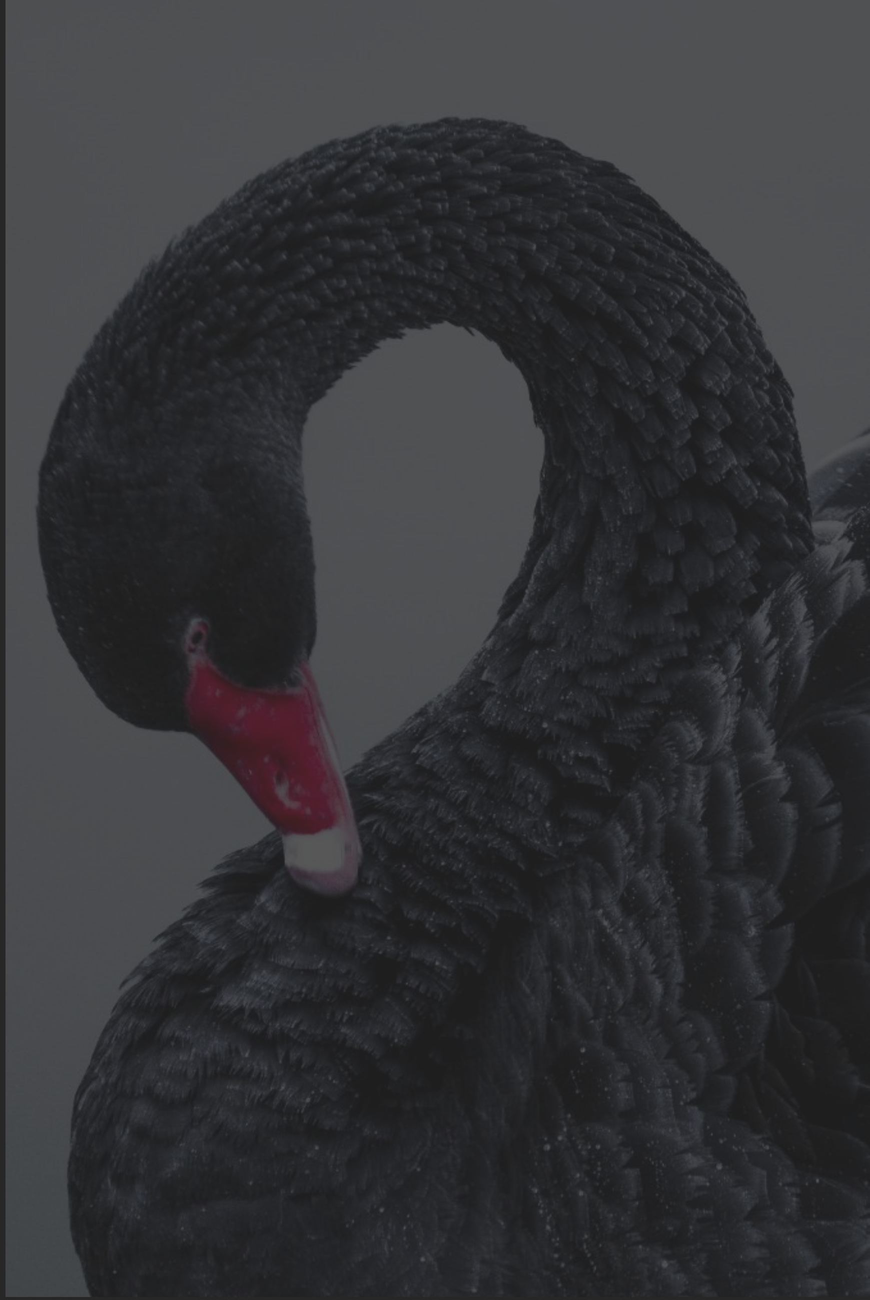


Cyber security is not only a technical challenge…

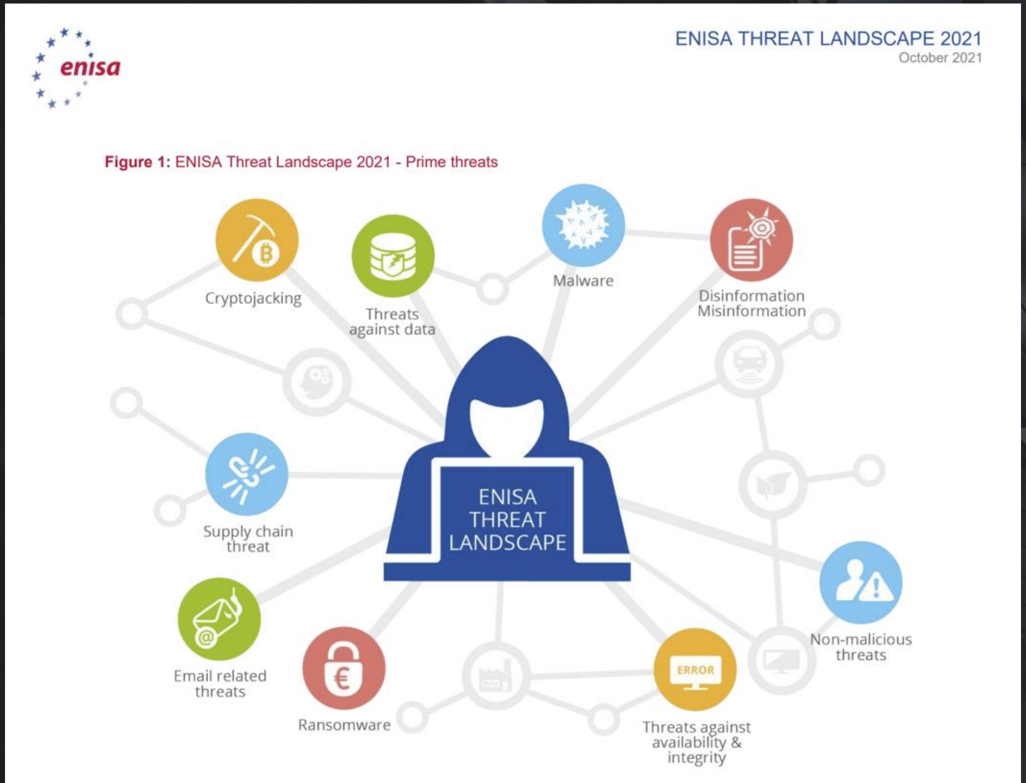
…it is also a behavioral one.

- As long as managers and employees can provide access to systems and high-value information, they become targets.
- Cybersecurity depends on them too.

Is this a black swan type of risk?

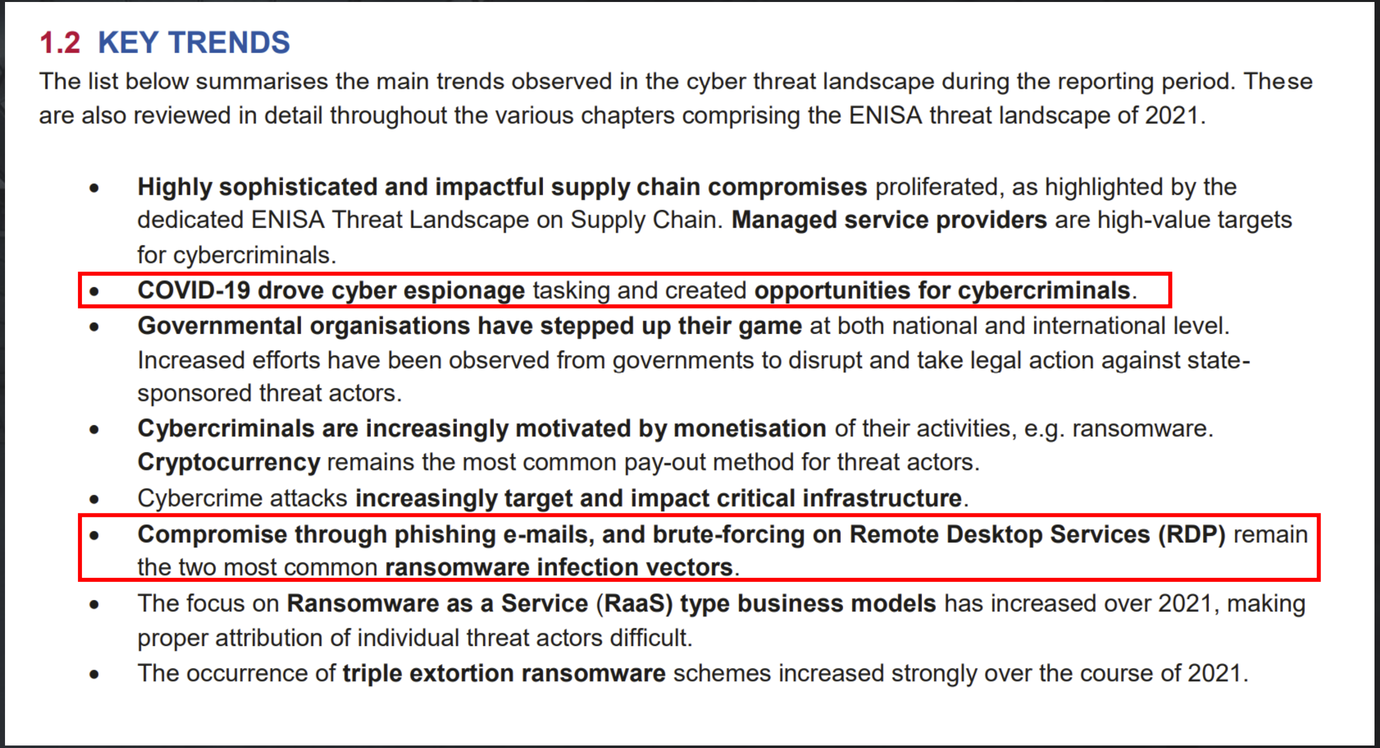


ENISA Threat Landscape Report 2021



ENISA THREAT LANDSCAPE 2021
October 2021

Figure 1: ENISA Threat Landscape 2021 - Prime threats



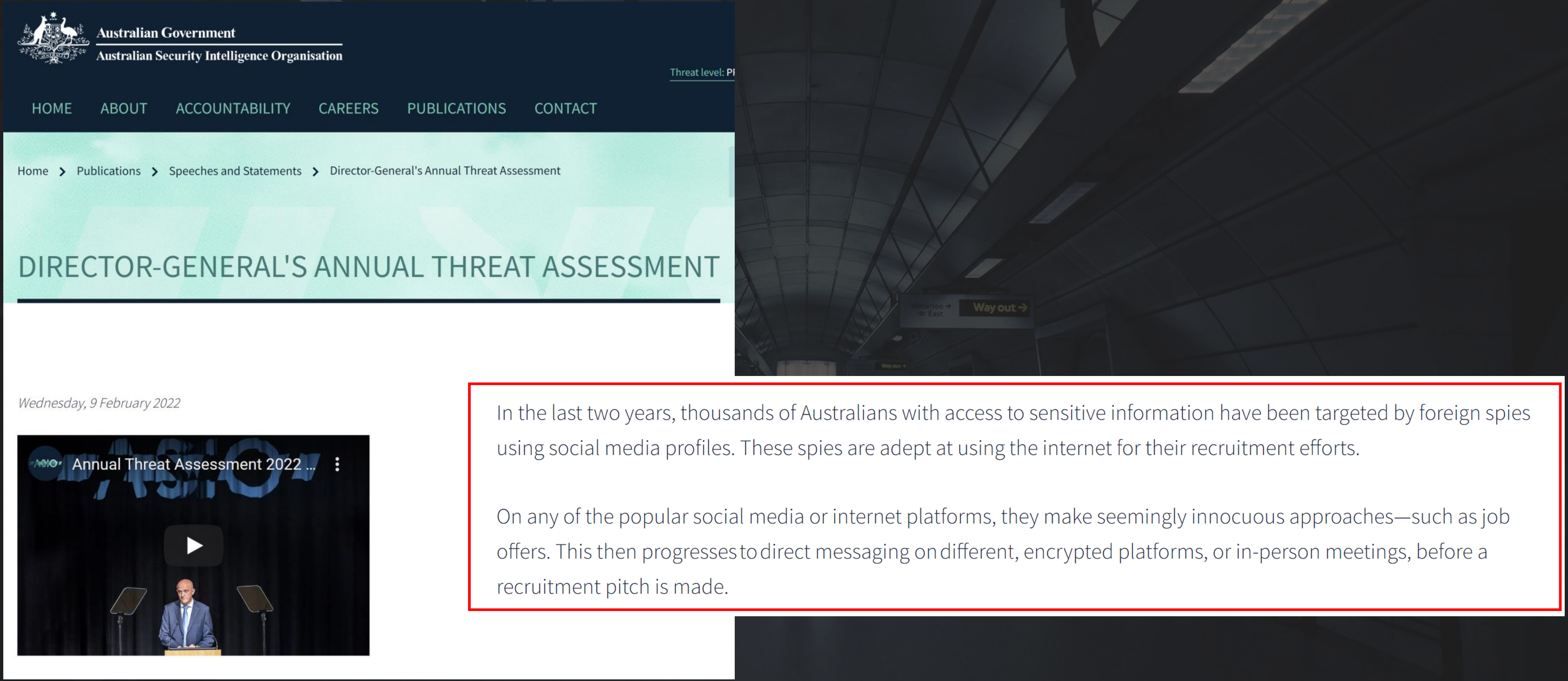
1.2 KEY TRENDS

The list below summarises the main trends observed in the cyber threat landscape during the reporting period. These are also reviewed in detail throughout the various chapters comprising the ENISA threat landscape of 2021.

- **Highly sophisticated and impactful supply chain compromises** proliferated, as highlighted by the dedicated ENISA Threat Landscape on Supply Chain. **Managed service providers** are high-value targets for cybercriminals.
- **COVID-19 drove cyber espionage** tasking and created **opportunities for cybercriminals**.
- **Governmental organisations have stepped up their game** at both national and international level. Increased efforts have been observed from governments to disrupt and take legal action against state-sponsored threat actors.
- **Cybercriminals are increasingly motivated by monetisation** of their activities, e.g. ransomware. **Cryptocurrency** remains the most common pay-out method for threat actors.
- Cybercrime attacks **increasingly target and impact critical infrastructure**.
- **Compromise through phishing e-mails, and brute-forcing on Remote Desktop Services (RDP)** remain the two most common **ransomware infection vectors**.
- The focus on **Ransomware as a Service** (**RaaS**) **type business models** has increased over 2021, making proper attribution of individual threat actors difficult.
- The occurrence of **triple extortion ransomware** schemes increased strongly over the course of 2021.

Source: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Australian Security Intelligence Organisation



Australian Government
Australian Security Intelligence Organisation

Threat level: PI

HOME ABOUT ACCOUNTABILITY CAREERS PUBLICATIONS CONTACT

Home > Publications > Speeches and Statements > Director-General's Annual Threat Assessment

DIRECTOR-GENERAL'S ANNUAL THREAT ASSESSMENT

Wednesday, 9 February 2022

In the last two years, thousands of Australians with access to sensitive information have been targeted by foreign spies using social media profiles. These spies are adept at using the internet for their recruitment efforts.

On any of the popular social media or internet platforms, they make seemingly innocuous approaches—such as job offers. This then progresses to direct messaging on different, encrypted platforms, or in-person meetings, before a recruitment pitch is made.

Source: https://www.asio.gov.au/publications/speeches-and-statements/director-generals-annual-threat-assessment-2022.html

Weaponized Psychology

- Identifying and exploiting human vulnerabilities

…or simply human needs.

- The basic human psychological wiring is universal

…and it is universally exploitable.

- It is also practical: low-cost, low risk, high-reward.

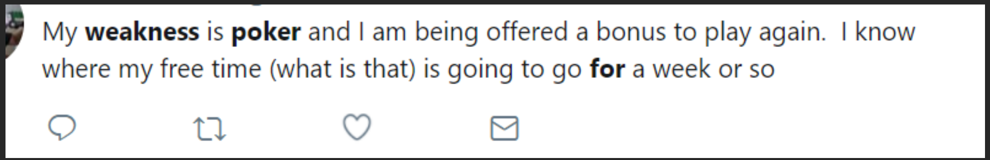
The stimulus-response effect in human triggers is consistent, and exploiting these vulnerabilities is consistently successful.

Weaponized Psychology

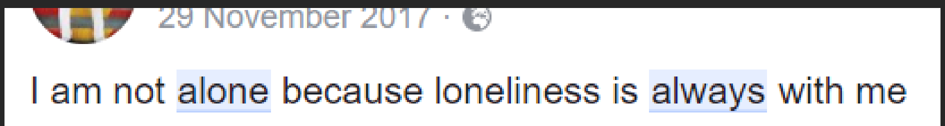
Example:

Unmet Needs.

Difficult to identify?

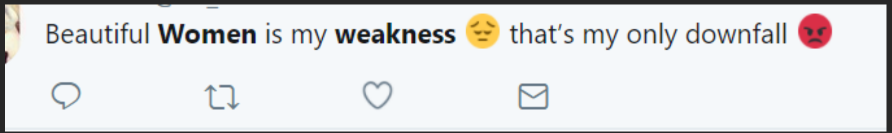


My **weakness** is **poker** and I am being offered a bonus to play again. I know where my free time (what is that) is going to go **for** a week or so

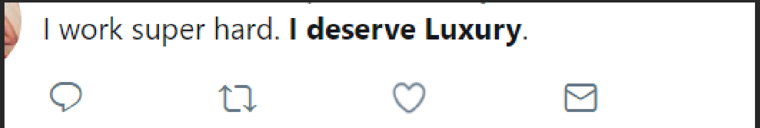


29 November 2017 ·

I am not alone because loneliness is always with me



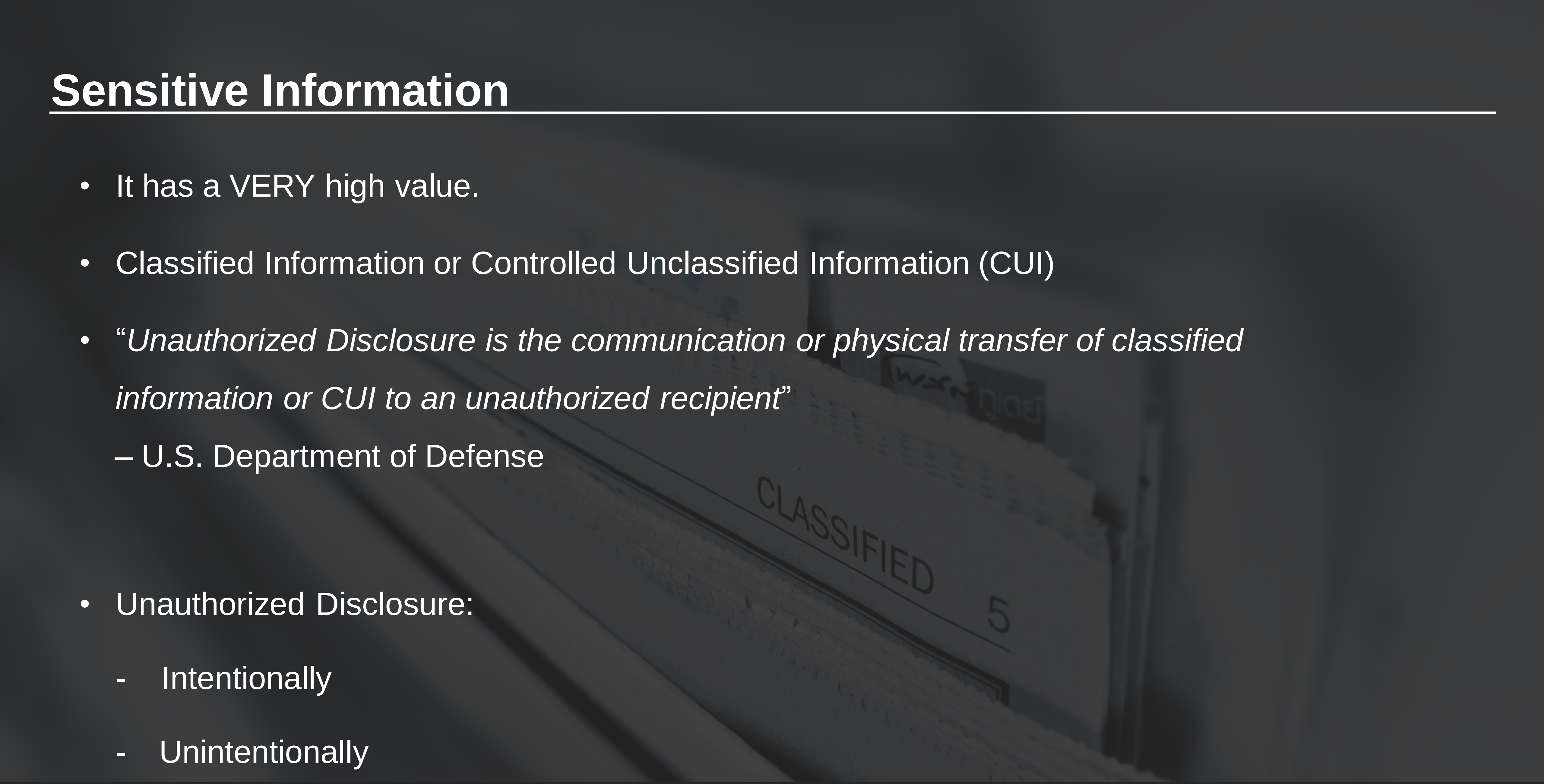
Beautiful **Women** is my **weakness** 😔 that's my only downfall 😡



I work super hard. **I deserve Luxury**.

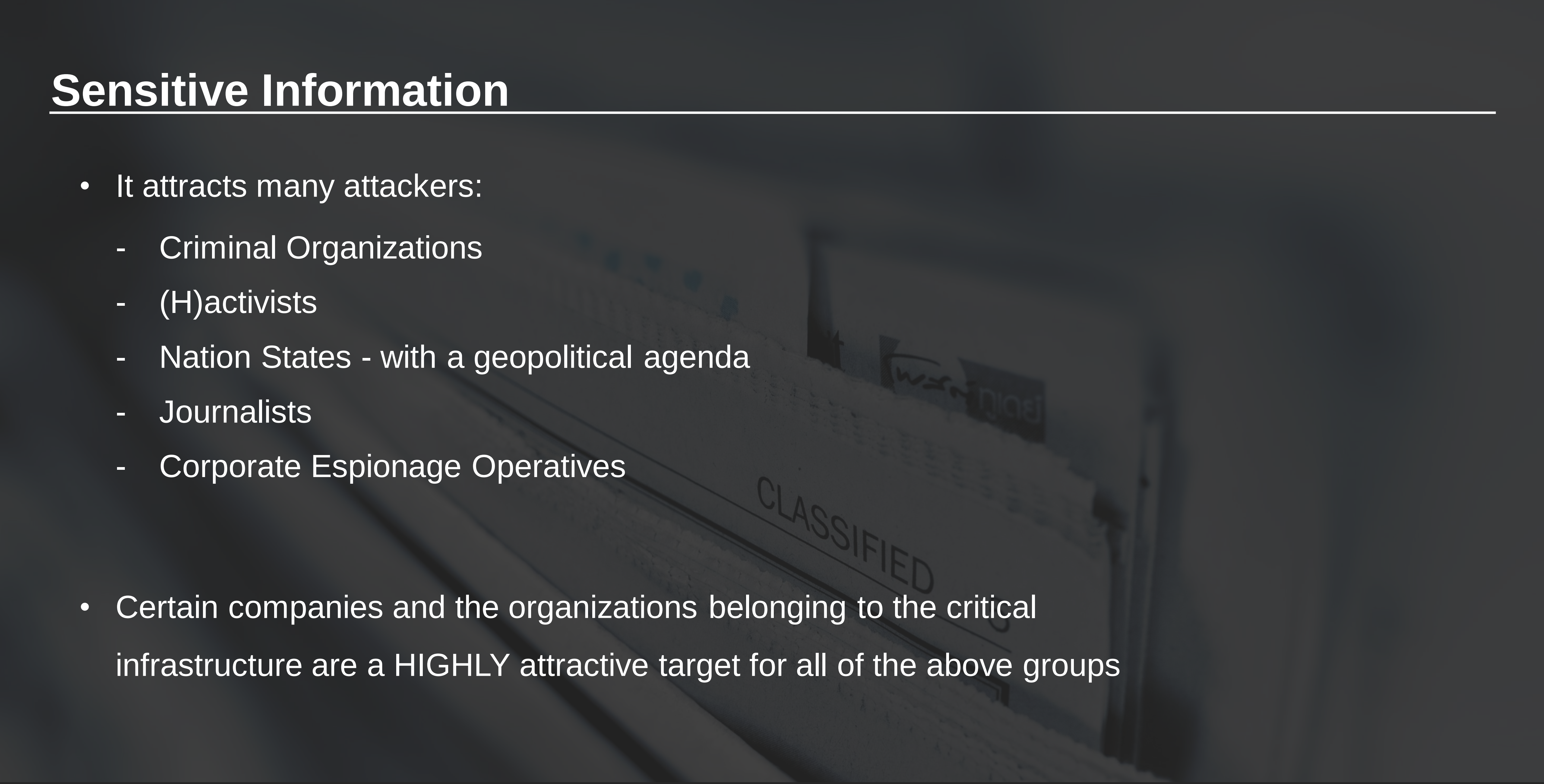
Sensitive Information

Sensitive Information



- It has a VERY high value.
- Classified Information or Controlled Unclassified Information (CUI)
- “*Unauthorized Disclosure is the communication or physical transfer of classified information or CUI to an unauthorized recipient*”
  – U.S. Department of Defense
- Unauthorized Disclosure:
  - Intentionally
  - Unintentionally

Sensitive Information



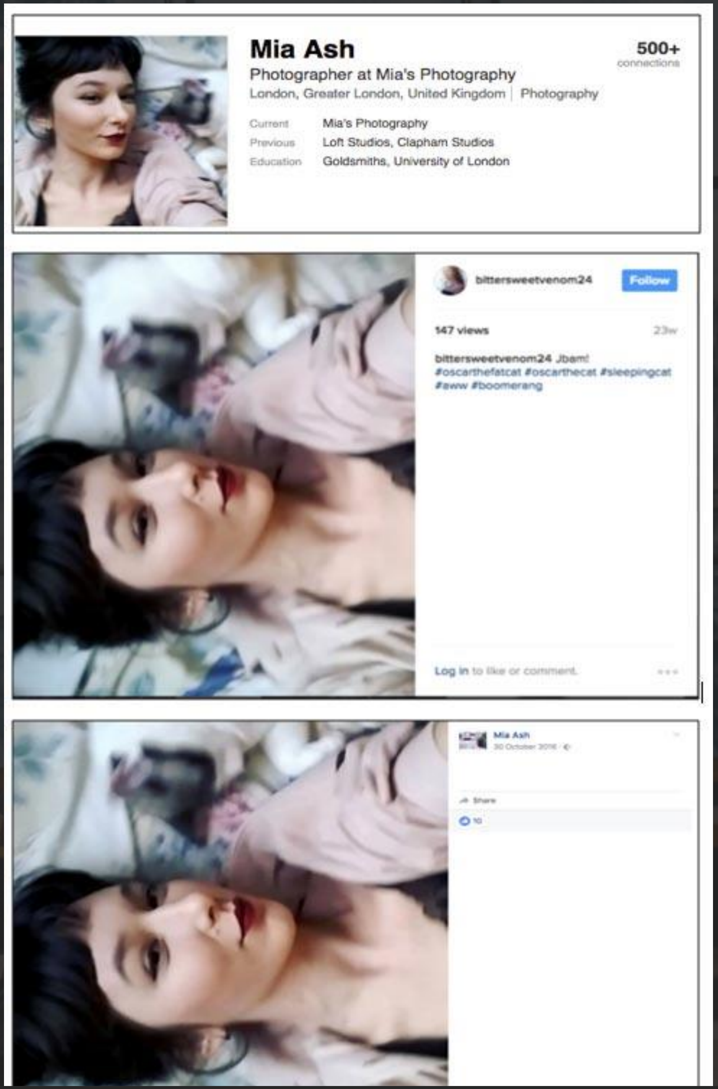
- It attracts many attackers:
  - Criminal Organizations
  - (H)activists
  - Nation States - with a geopolitical agenda
  - Journalists
  - Corporate Espionage Operatives

- Certain companies and the organizations belonging to the critical infrastructure are a HIGHLY attractive target for all of the above groups

Case Study: Mia Ash

- Threat actor: likely COBALT GYPSY
- Target: telecommunications, government, defense, oil, and financial services organizations in Middle East and North Africa
- Plan A: Phishing attacks delivering PupyRAT
- Plan B: Mia Ash
- Fake identity used several social media accounts used to perform reconnaissance on and establish relationships with *specific targets*

Source: https://www.secureworks.com/research/the-curious-case-of-mia-ash



Mia Ash
Photographer at Mia's Photography
London, Greater London, United Kingdom | Photography
500+ connections

Current	Mia's Photography
Previous	Loft Studios, Clapham Studios
Education	Goldsmiths, University of London

bittersweetvenom24 Follow

147 views 23w

bittersweetvenom24 Jbam! #oscarthefatcat #oscarthecat #sleepingcat #aww #boomerang

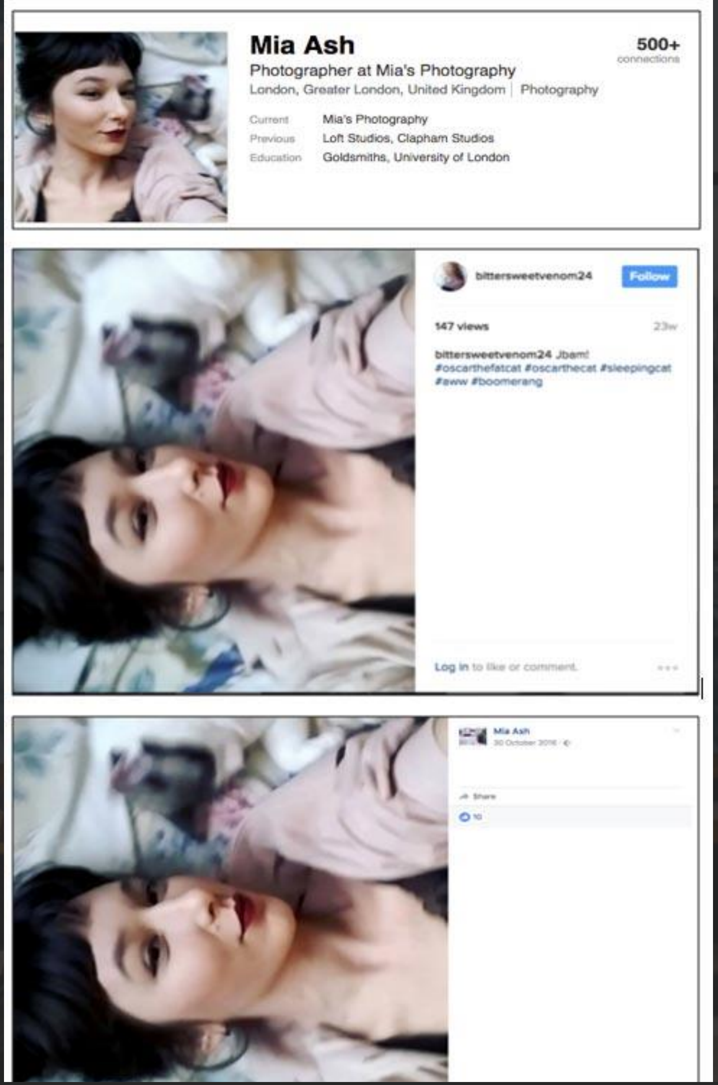
Log in to like or comment.

Mia Ash
30 October 2016

Case Study: Mia Ash

- Profiles that appear intended to **build trust and rapport** with potential victims.
- “She” initiated conversations based on “**common interests**” and moved on to profession-related, and personal discussions.
- **Escalated** target to other social media platforms & phone
- Once **work email** was provided – malicious Excel file was sent.
- The file would eventually deliver a PupyRAT

Source: https://www.secureworks.com/research/the-curious-case-of-mia-ash



Mia Ash

Photographer at Mia's Photography

London, Greater London, United Kingdom | Photography

500+ connections

Current: Mia's Photography

Previous: Loft Studios, Clapham Studios

Education: Goldsmiths, University of London

bittersweetvenom24 Follow

147 views 23w

bittersweetvenom24 Jbam! #oscarthefatcat #oscarthecat #sleepingcat #aww #boomerang

Log in to like or comment.

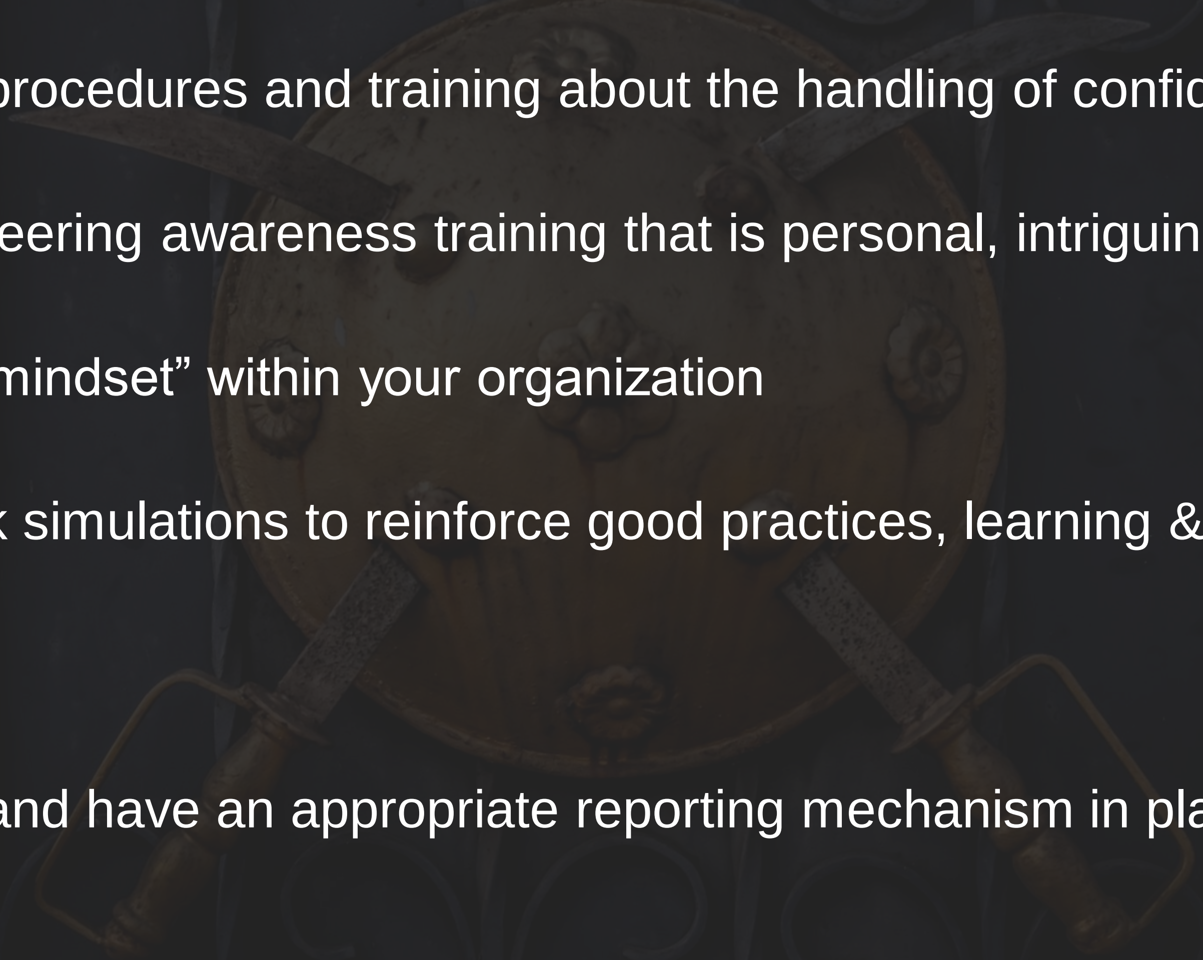
Mia Ash
30 October 2016

Share

10

How do we defend against weaponized psychology?

Organizational Recommendations



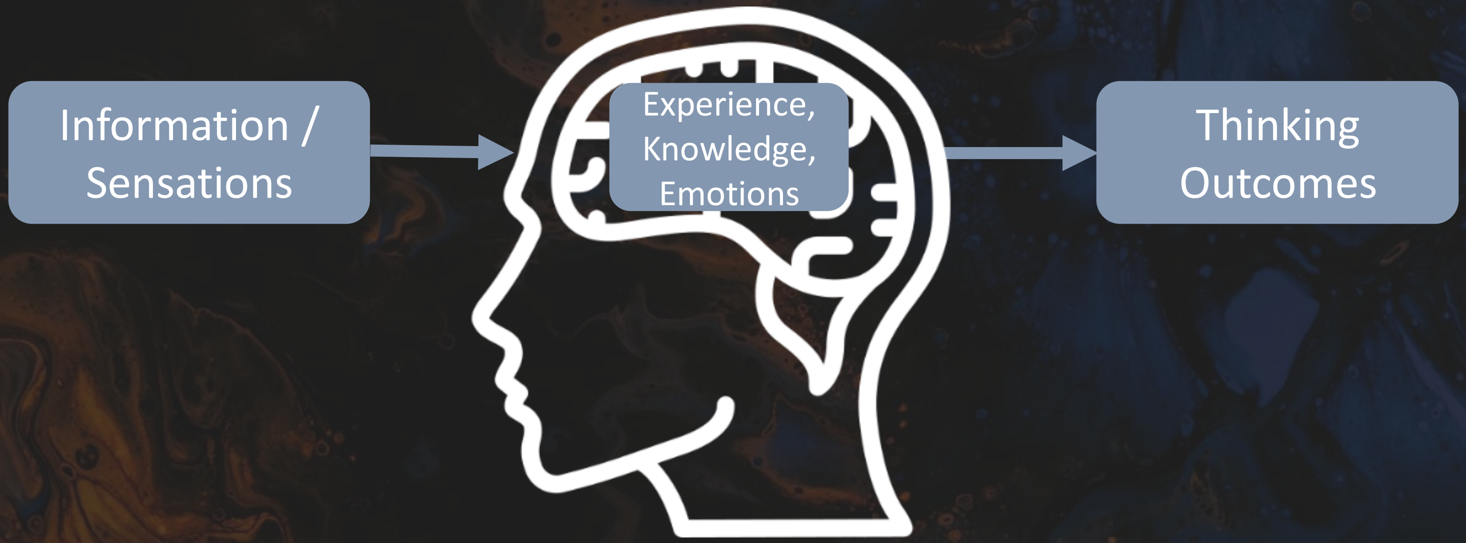
- Appropriate policies, procedures and training about the handling of confidential information
- Excellent social engineering awareness training that is personal, intriguing, and interesting
- Reinforce a “security mindset” within your organization
- Run exercises / attack simulations to reinforce good practices, learning & memory
- Knowledge → Skills
- Encourage reporting and have an appropriate reporting mechanism in place

The Good News: Neuroplasticity

All the above knowledge can be utilized in a defensive capacity.

Our brains ARE capable of creating new behavioral pathways that can become automatic.

Red flags act like cognitive triggers when employees have been trained well.

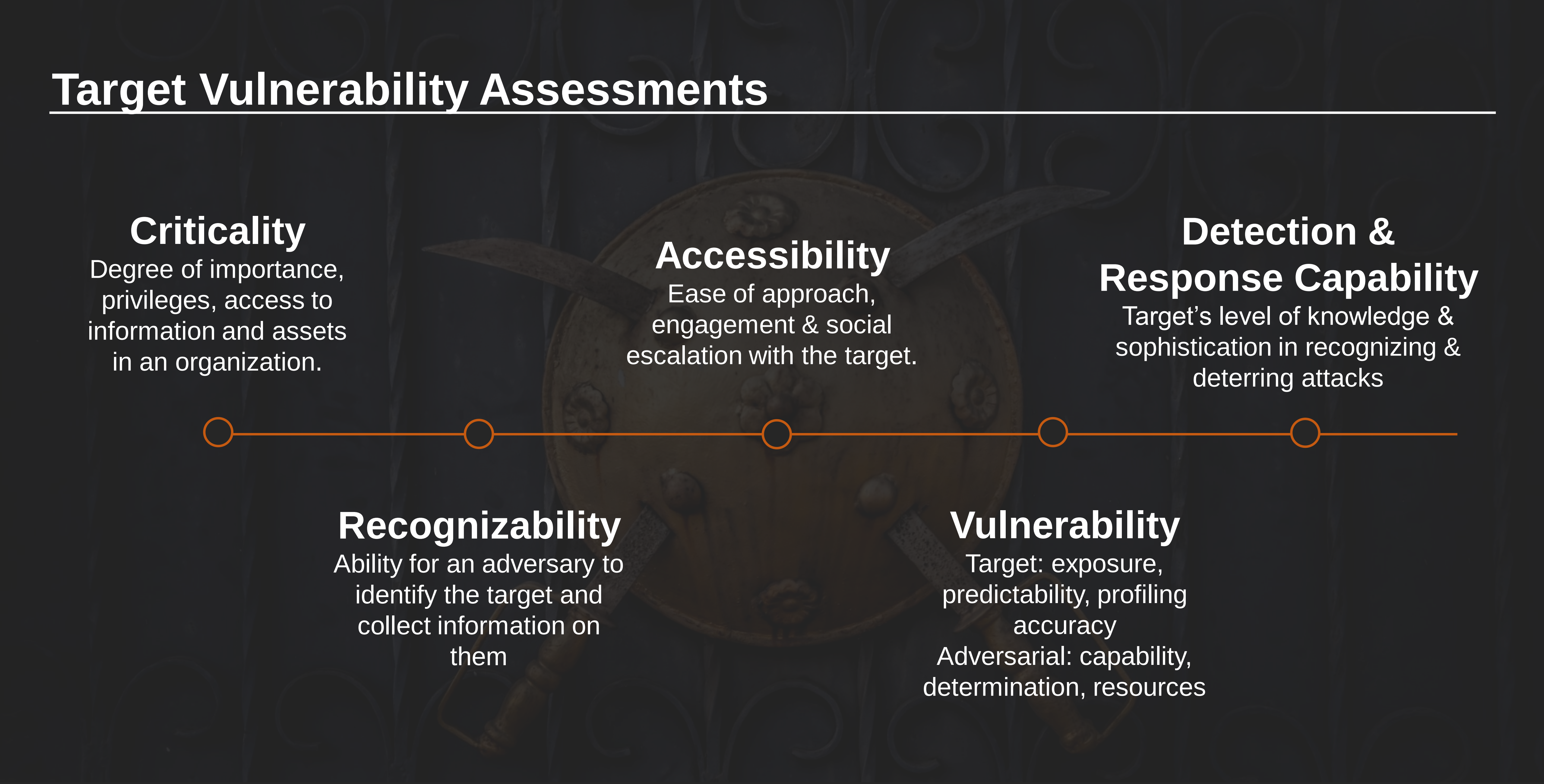


Information / Sensations

Experience, Knowledge, Emotions

Thinking Outcomes

Target Vulnerability Assessments



Criticality

Degree of importance, privileges, access to information and assets in an organization.

Recognizability

Ability for an adversary to identify the target and collect information on them

Accessibility

Ease of approach, engagement & social escalation with the target.

Vulnerability

Target: exposure, predictability, profiling accuracy
Adversarial: capability, determination, resources

Detection & Response Capability

Target’s level of knowledge & sophistication in recognizing & deterring attacks

> ***“Knowledge is a weapon.***
> ***I intend to be formidably armed.”***
>
> ***- Terry Goodkind***

Christina Lekati
Social Engineering Security
Trainer & Consultant
Cyber Risk GmbH

Contact Details:

Christina Lekati

@ChristinaLekati