



Cyber security is NOT a product - it is a shared responsibility

Vijay Velu

Technical Director, Head of Offensive Security Services

WHOAMI\$

Drwxr----- 0 Head of Offensive Security/DFIR - BDO LLP

Drwxr----- 1 Break and Fix from past decade and half

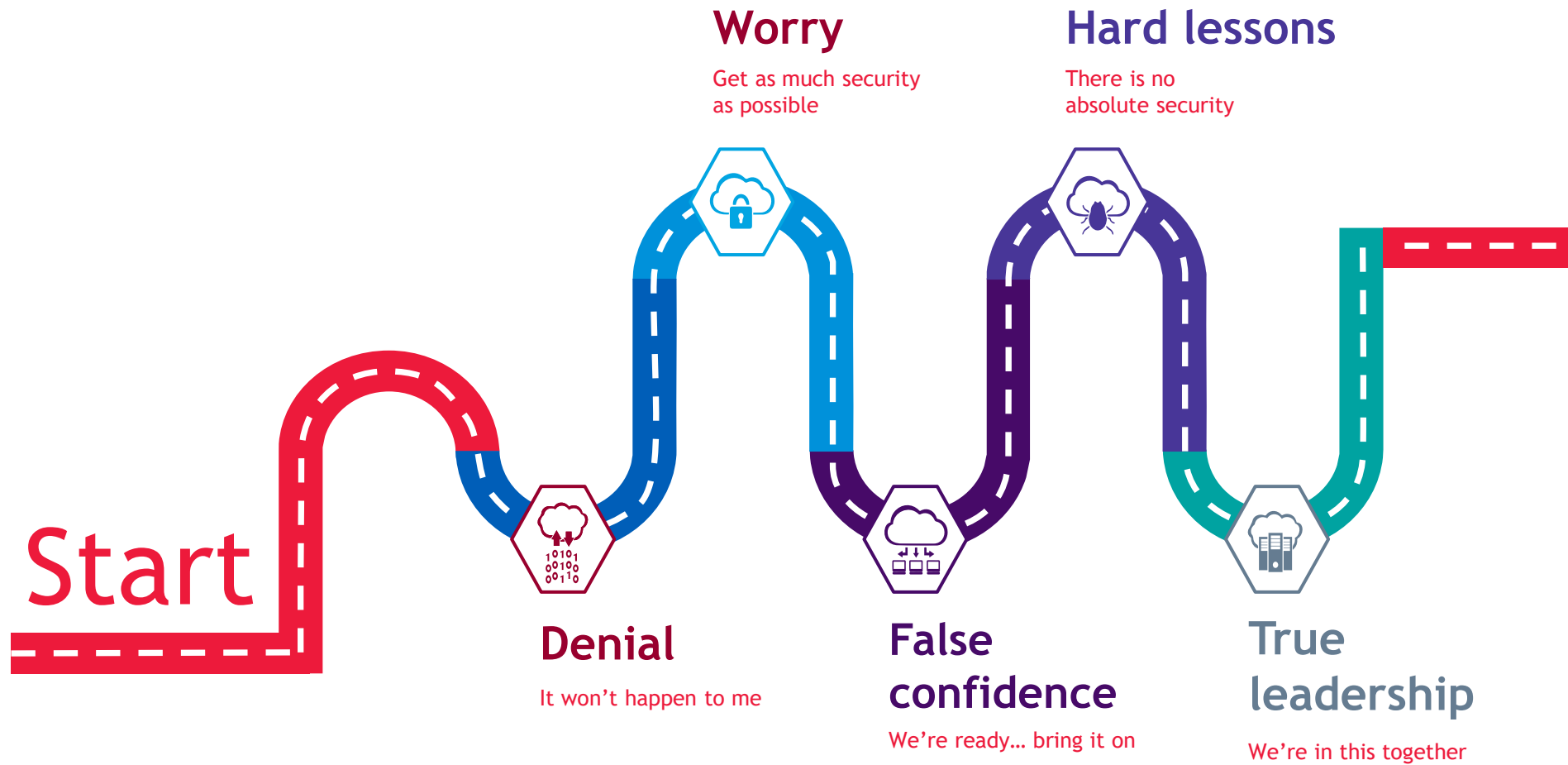
Drwxr----- 0 Tester by Passion

-rwxr ----- 1 Forensics Investigator by Choice

-rwxr ----- 0 Speaker

THE JOURNEY

Today's cyber world



2022 BREACHES AT A GLANCE



April 2022: Block Confirms Cash App Data Breach

March 2022: Microsoft Breached by Lapsus\$ Hacker Group

March 2022: Lapsus\$ Group Breaches Authentication Company Okta

February 2022: Ottawa Freedom Convoy Donors Leaked via Christian Fundraising Platform

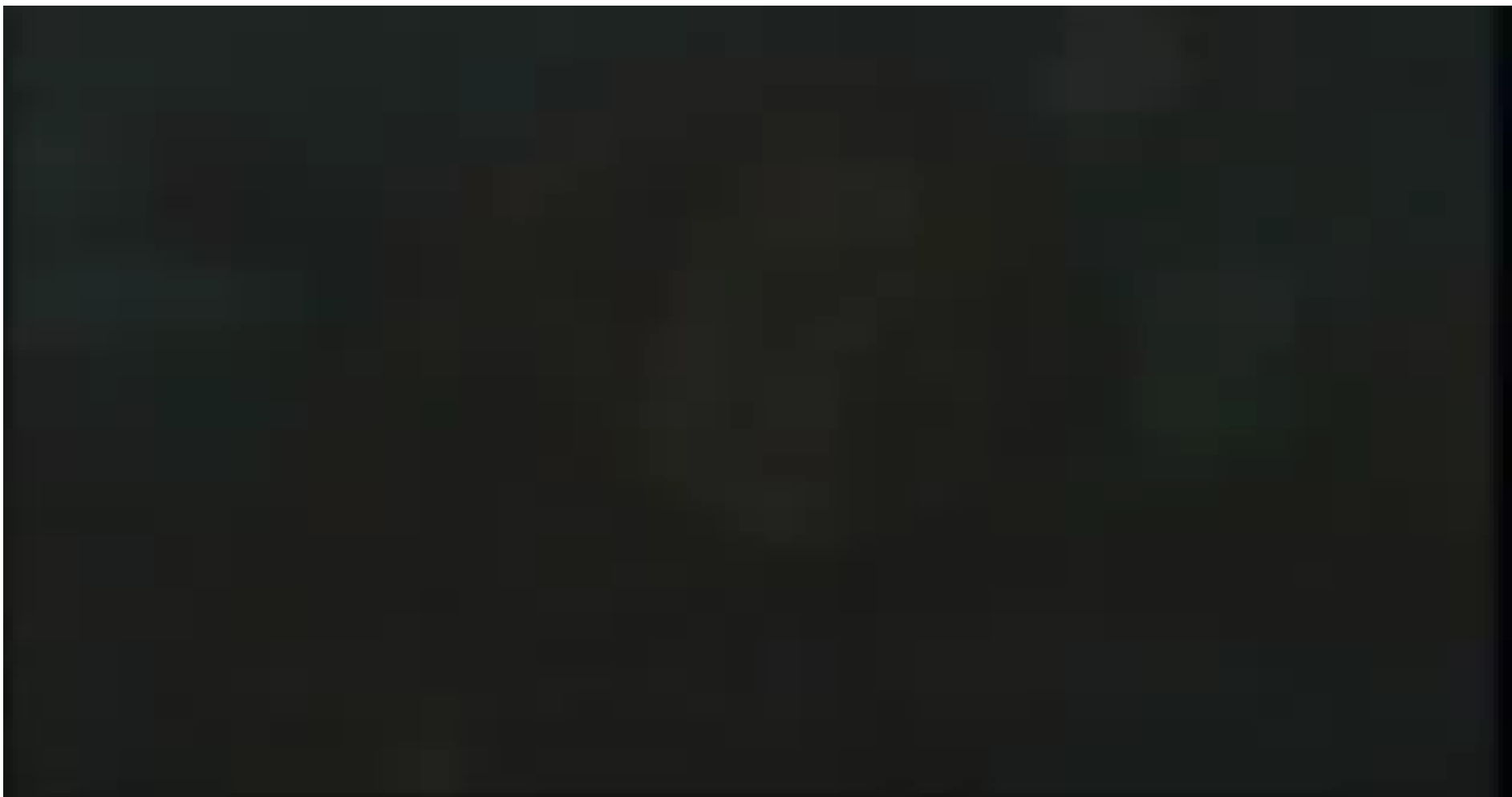
January 2022: Over \$30 Million Looted in Crypto.com Breach

January 2021: 2.28 Million MeetMindful User Records Exposed by Hacker

January 2021: Microsoft Exchange Server Flaw Leads to 60,000+ Hack

April 2021: 530 Million Facebook Users' Data Leaked on Online Hacker Forum

April 2021: 500 Million LinkedIn Users' Data Scraped and Sold



Understanding your adversary's available courses of action



Photo: Roger Nilsson

is fundamental to determining your own viable courses of action.

UNDERSTANDING THE CYBER THREAT

Who will attack me and what is their objective?



Activists targeting online services in line with their inclinations e.g. Anonymous and Lulzsec



Groups backed by states, targeting for political or commercial interests



Sophisticated and organised groups targeting systems for financial gain



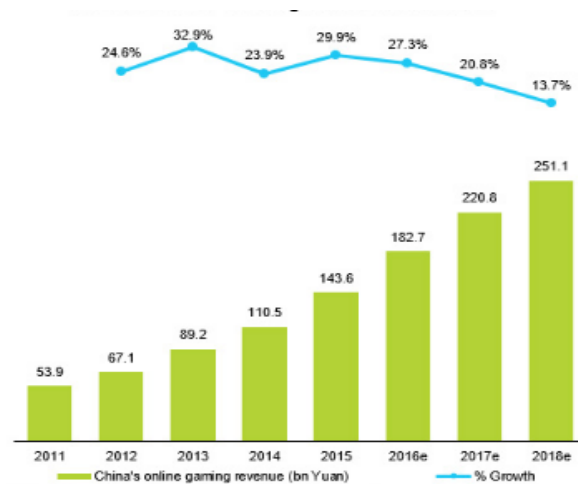
Employees having access to critical systems and resources by virtue of their roles

UNDERSTANDING THE CYBER THREAT

Why is the financial mutual sector an attractive target?

HIGH VALUE INDUSTRY

Technology driven environment, high turnover, sensitive users and highly regulated make it the perfect target



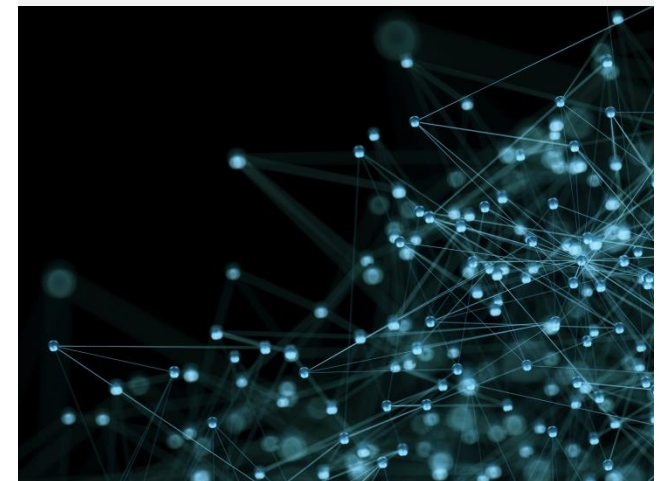
LOW COST OF ENTRY

Attacks can be launched from anywhere, successfully and with limited resources



COMMON PLATFORMS

Common platforms create common vulnerabilities



THREAT LANDSCAPE

- ▶ Distractive attacks (SWIFT/ payment switch attacks)
- ▶ Targeted ransomware attacks
- ▶ Supply chain attacks
- ▶ Cryptojacking
- ▶ Trickle-down effect

Russia vs. Ukraine
North Korea vs. South Korea

- ▶ Data theft
 - ▶ Data integrity and sabotage
 - ▶ Direct financial theft
-

IMPACTS OF A BREACH

Broad and Deep - Create a business risk (no longer just an IT risk)



- Complaints
- Identity fraud



- General staff
- Loss of jobs
- Increases work loads



- Loss of share price



- Supply chain



- Information Commissioner (GDPR)
- Industry Regulators (e.g. FCA and PCI)



- Drop in share price
- Loss of income
- Direct loss (fraud)



- Bad press
- Social media
- Customers and suppliers perceptions/ confidence



- Mental wellbeing
- Operational systems stop working



- Increased load on Call Centre
- Time to recover and investigate

ROLE OF NEDS IN FINANCIAL MUTUALS



TECH/IT RISKS ARE NOT ALWAYS THE PROBLEM



Create a fake identity



Go to the bank, ask for a loan



Disappear with the money

EFFECTIVE INCIDENT RESPONSE?



Cyber Security Strategy without
leadership is like a broken pencil.

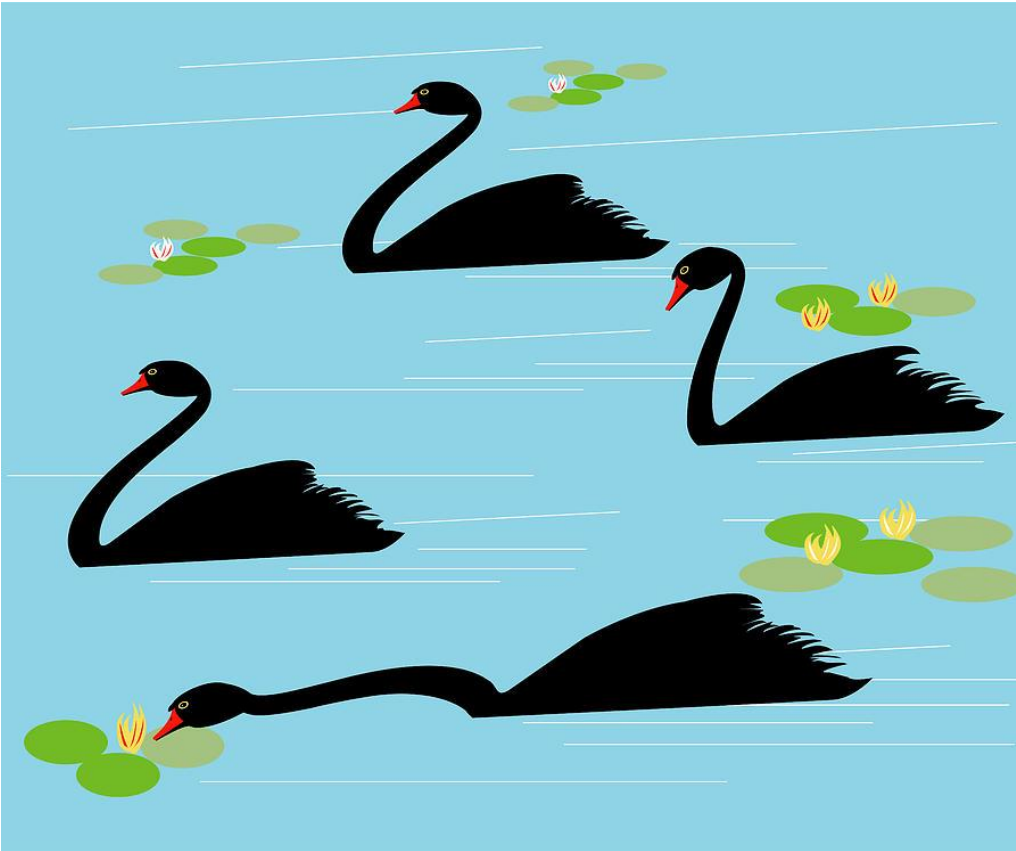
Pointless!



THOUGHTS

- ▶ NEDs with clear situational awareness
 - Chief Threat Officer, Chief Privacy Officer, Chief Information Security Officer, Chief Risk Officer and the C-Suite.
- ▶ Clear Decision making
 - Re-active vs Pro-active
- ▶ Digital Fraud Crisis Management
 - Prevent and Transfer of risk

SHAPING THE DEFENCE



- ▶ Engage before Another Black Swan
- ▶ Consistent Response to Incidents
- ▶ Reduce Risk by Early Threats
- ▶ Keep It Simple and Secure



FOR MORE INFORMATION:

VIJAY VELU

+44 (0)207 893 3014
vijay.velu@bdo.co.uk

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO LLP to discuss these matters in the context of your particular circumstances. BDO LLP, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO LLP or any of its partners, employees or agents.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO member firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

Copyright © June 2022 BDO LLP. All rights reserved. Published in the UK.

www.bdo.co.uk

