Providing Digital Assurance and Cyber Hygiene

Bamboo Technology delivering digital assurance and resilience through end to end security management services.

Organisational Resilience; ability of an organisation to anticipate, prepare for, respond and adapt to any incremental change and sudden disruptions in order to survive and prosper. (ISO 65000:14. P.2)

January 2021

Cybersecurity Insurance Has a Big Problem

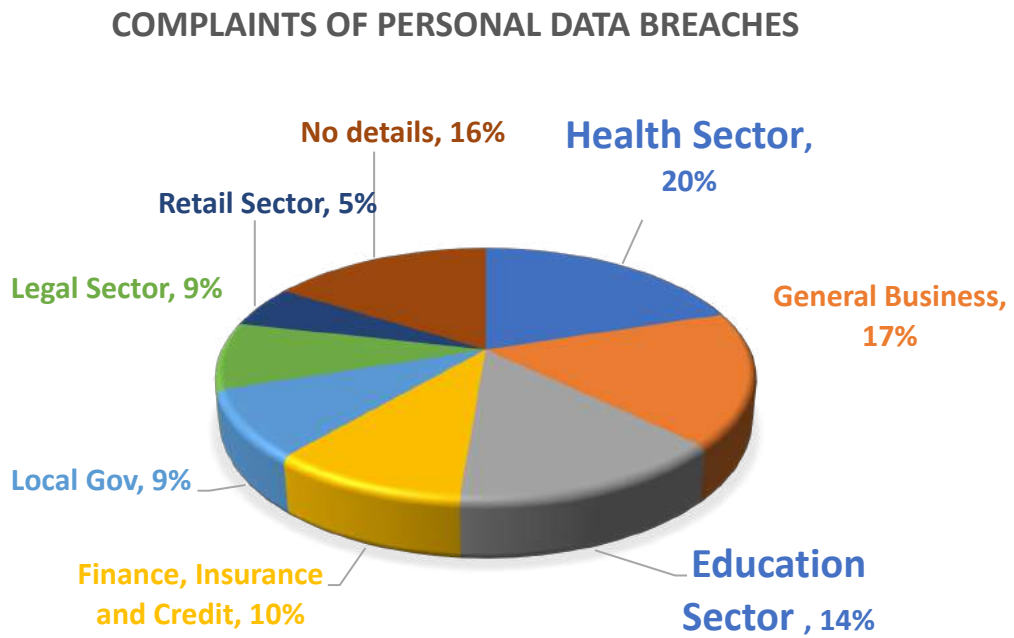
by Tom Johansmeyer

January 11, 2021

Harvard Business Review

https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem

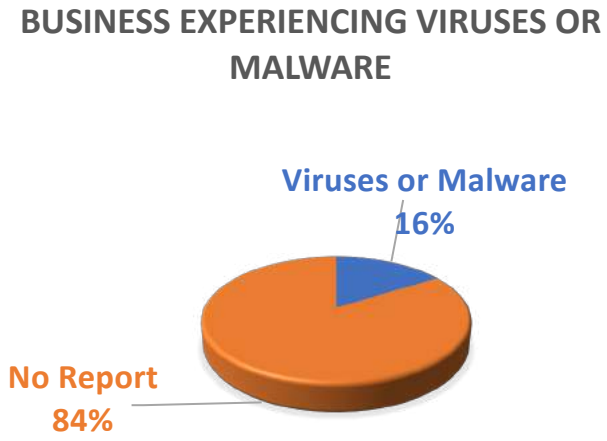
- The Threat -Data Breaches & Cyber Attacks 2019-2020

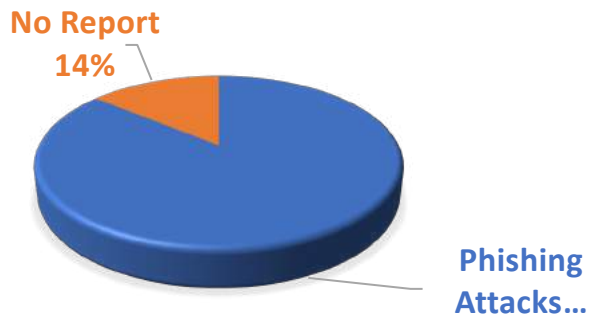


Cyber Attack Trends
Almost half of all business (46%) and a quarter of charities (26%) reported having cyber security breaches or attacks in 2020.

NCSC Annual Review

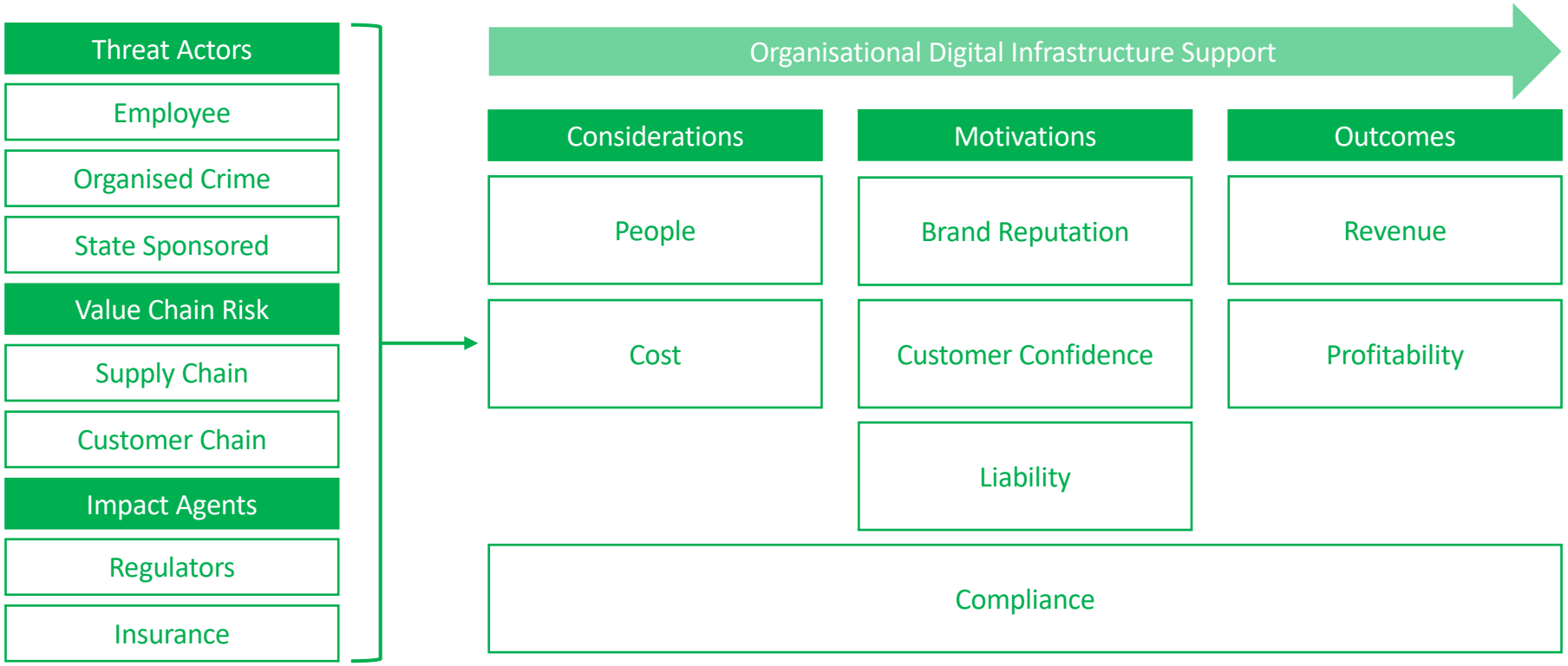
THE ICO reported 12,000 reports of personal data breaches, and took regulatory action in 236 instances including 15 fines.



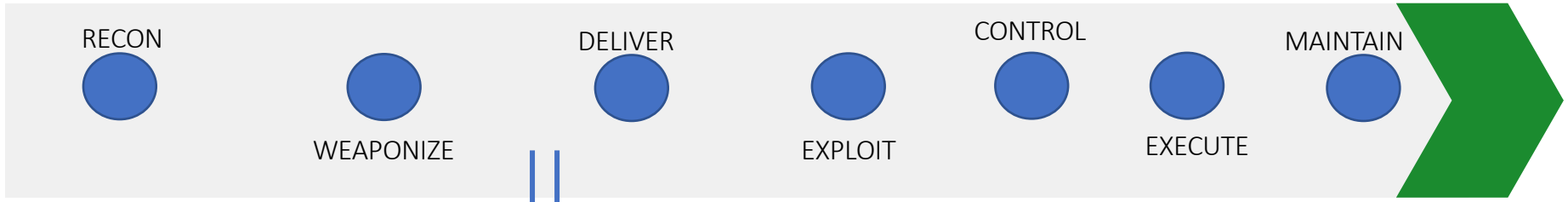


Protecting Organisational Objectives

By focusing digital assurance on your organisations real world, we can co-create and customise a proactive and reactive security system that aligns with the threats, risks and agents that can impact on your organisations digital infrastructure. This approach to digital security as the output being digital assurance and resilience, and the input being an aligned organisational consideration, motivations and desired outcomes or objectives.



Criminals are organised



PRE-ATT&CK

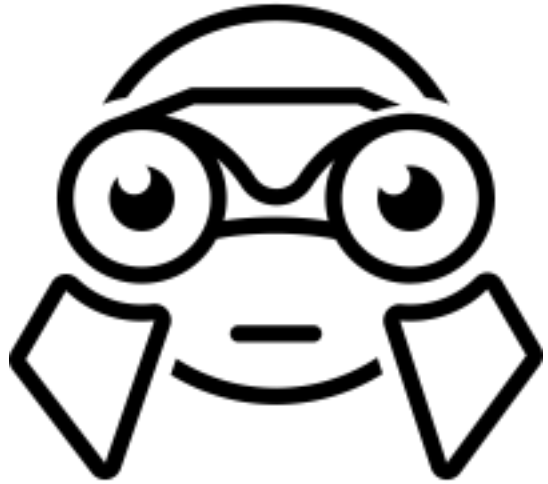
- Priority Definition
  - Planning, Direction
- Target Selection
- Information Gathering
  - Technical, People, Organisational
- Weakness Identification
  - Technical, People, Organisational
- Adversary OpSec
- Establish and Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

ATT&CK FOR ENTERPRISE

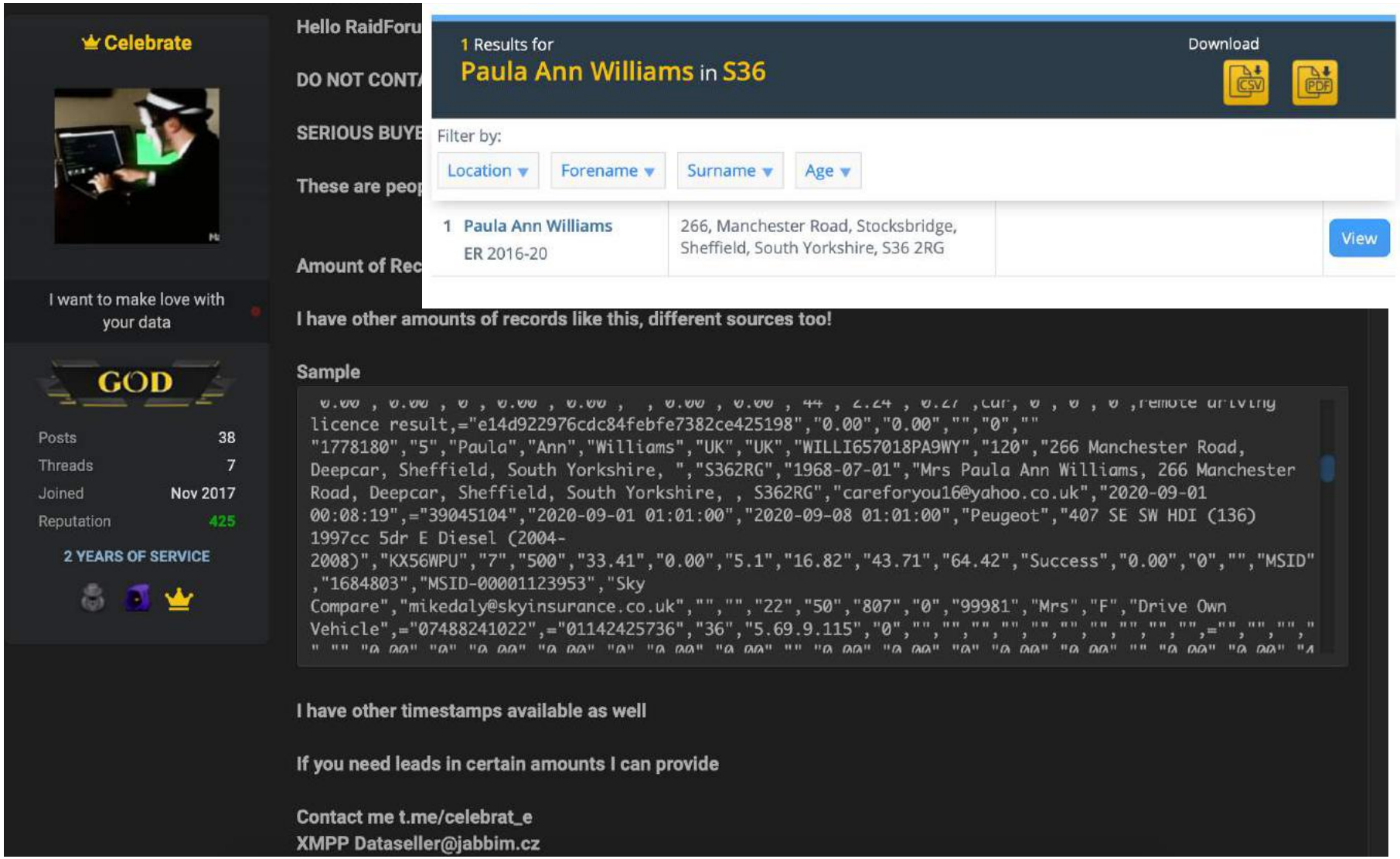
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control
- Impact

The observations 2020/21 – Real World View

- Cloud transition has been fast and has only quickened due to COVID
- Cyber crime ‘entry’ lower due powerful free tools and ‘you tube generation’
- Shift in cyber tactics – data exfiltration now standard practice (Regulatory and share price pressures)
- Human element is more important than ever
- Key is ‘validation’ not always more security – make complex simple and obtainable to the mass market (PROJECT HELIX)
- Ransomware – Touch on at the end happy to discuss in Q&A



What is the hacker’s motivation ?

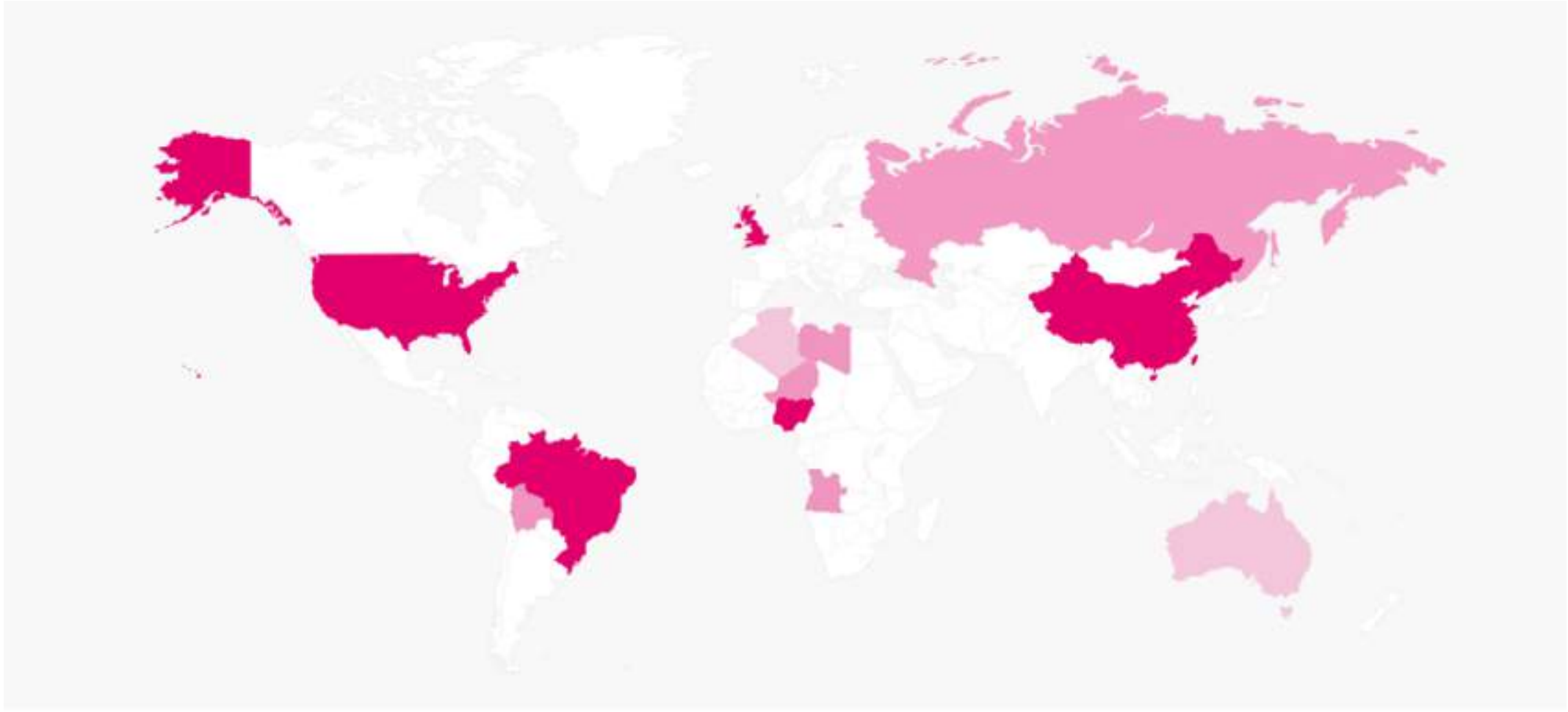


Microsoft Office 365 we are all joining

```
; OPT PSEUDOSECTION:
 EDNS: version: 0, flags:; udp: 4096
; QUESTION SECTION:
renishaw.com.                  IN      MX

; ANSWER SECTION:
renishaw.com.           21600   IN      MX      0 renishaw-com.mail.protection.o
utlook.com.

; Query time: 63 msec
; SERVER: 192.168.0.1#53(192.168.0.1)
; WHEN: Mon Jan 18 21:48:05 GMT 2021
; MSG SIZE  rcvd: 94
```

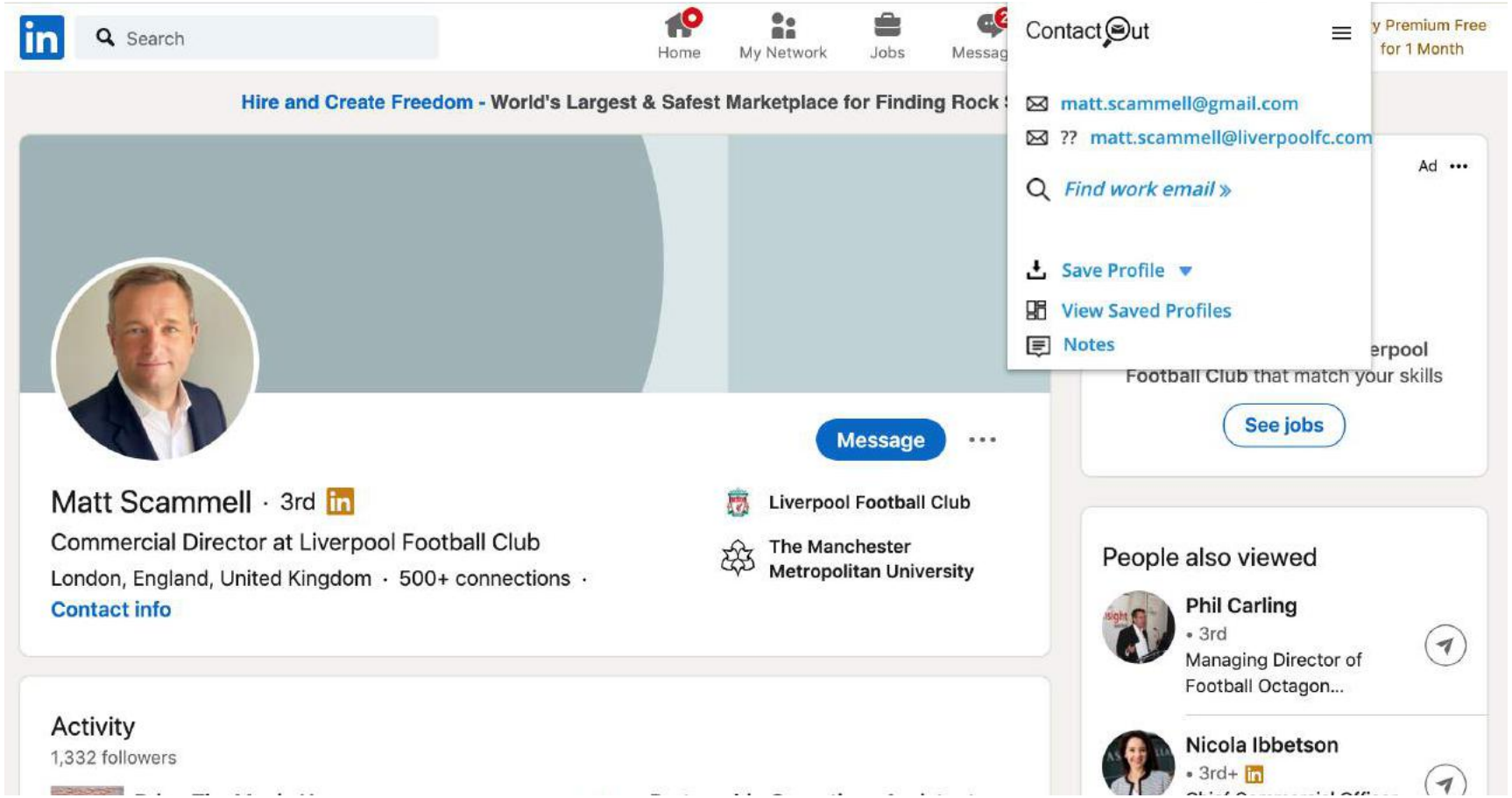
```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;mearsgroup.co.uk.              IN      MX

;; ANSWER SECTION:
mearsgroup.co.uk.       3600    IN      MX      10 mearsgroup-co-uk.mail.protect
ion.outlook.com.

;; Query time: 30 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Mon Jan 18 21:46:01 GMT 2021
;; MSG SIZE  rcvd: 105
```

The average company

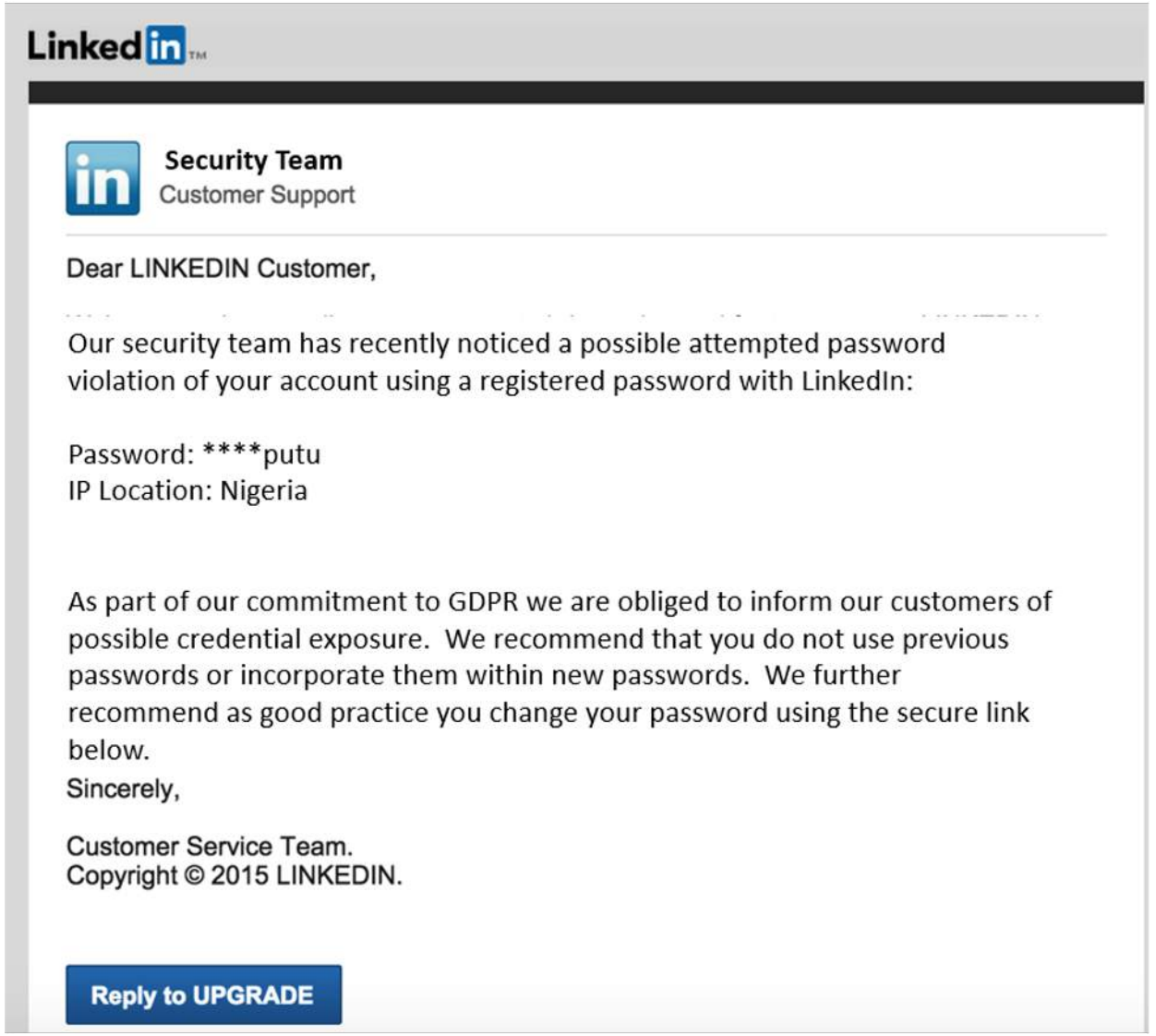


Project Helix: UK SME (1 Week Period)

Be aware of ‘features’



Human led attacks



LinkedIn™

Security Team
Customer Support

Dear LINKEDIN Customer,

Our security team has recently noticed a possible attempted password violation of your account using a registered password with LinkedIn:

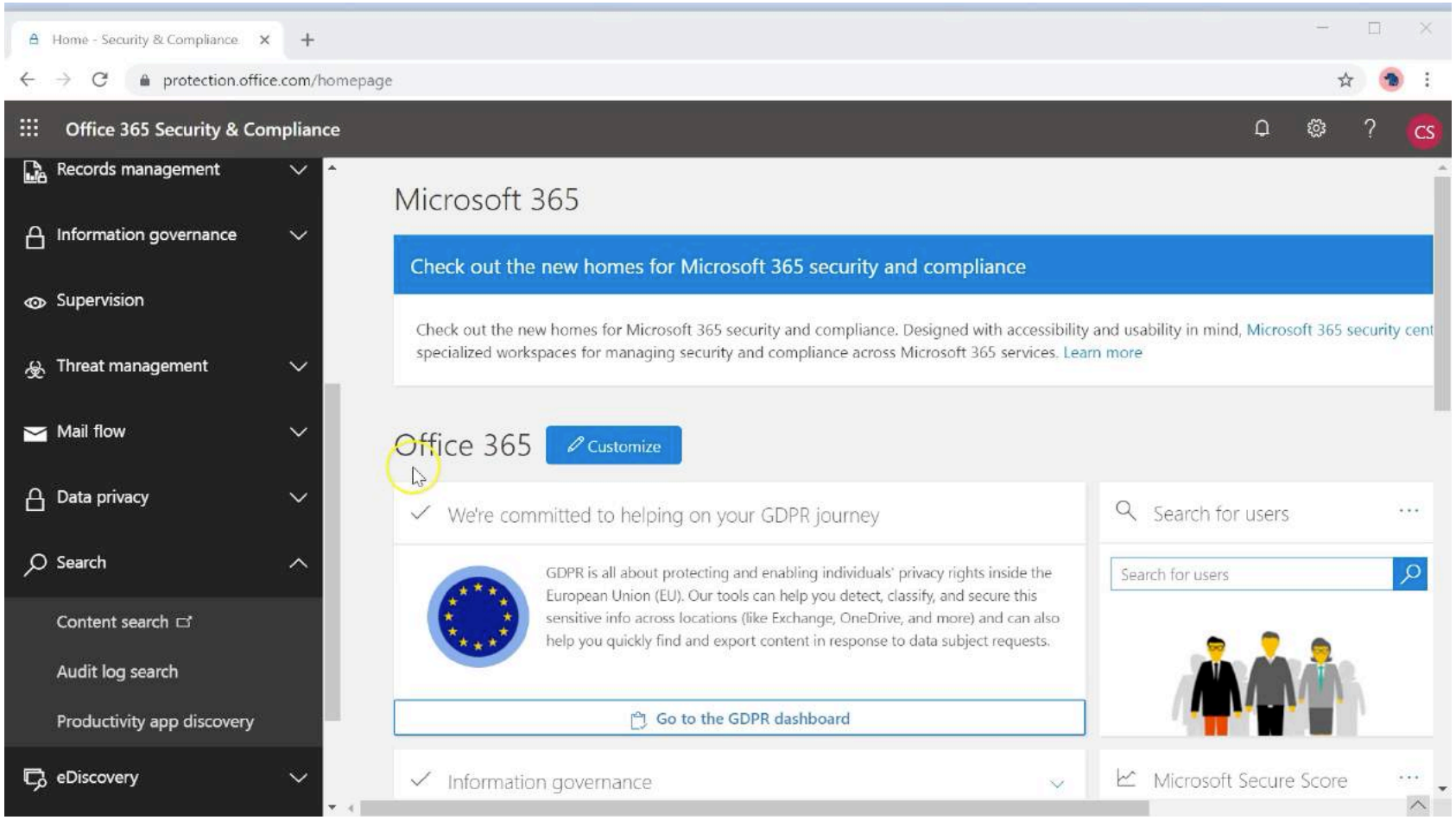
Password: ****putu
IP Location: Nigeria

As part of our commitment to GDPR we are obliged to inform our customers of possible credential exposure. We recommend that you do not use previous passwords or incorporate them within new passwords. We further recommend as good practice you change your password using the secure link below.
Sincerely,

Customer Service Team.
Copyright © 2015 LINKEDIN.

Reply to UPGRADE

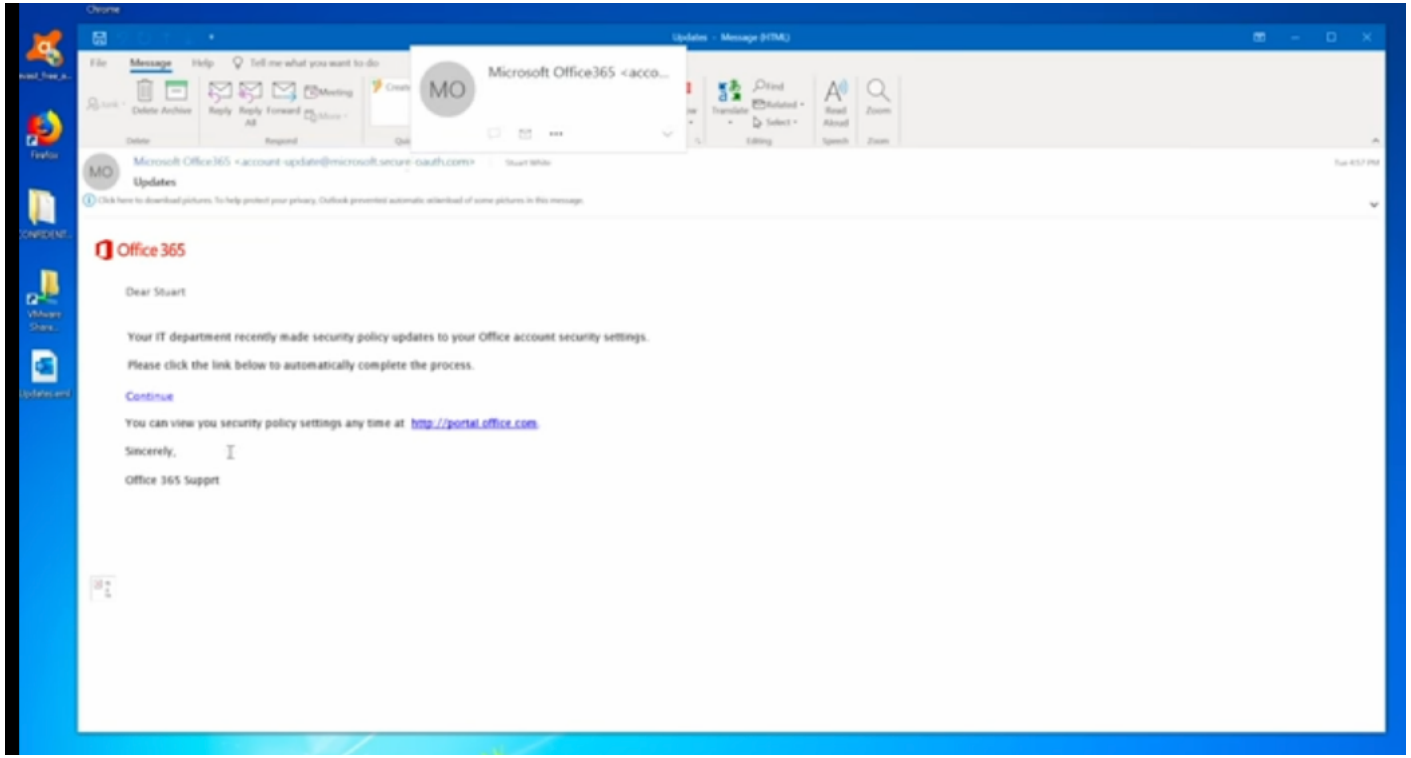
Thanks for the tools ! – Feature abuse



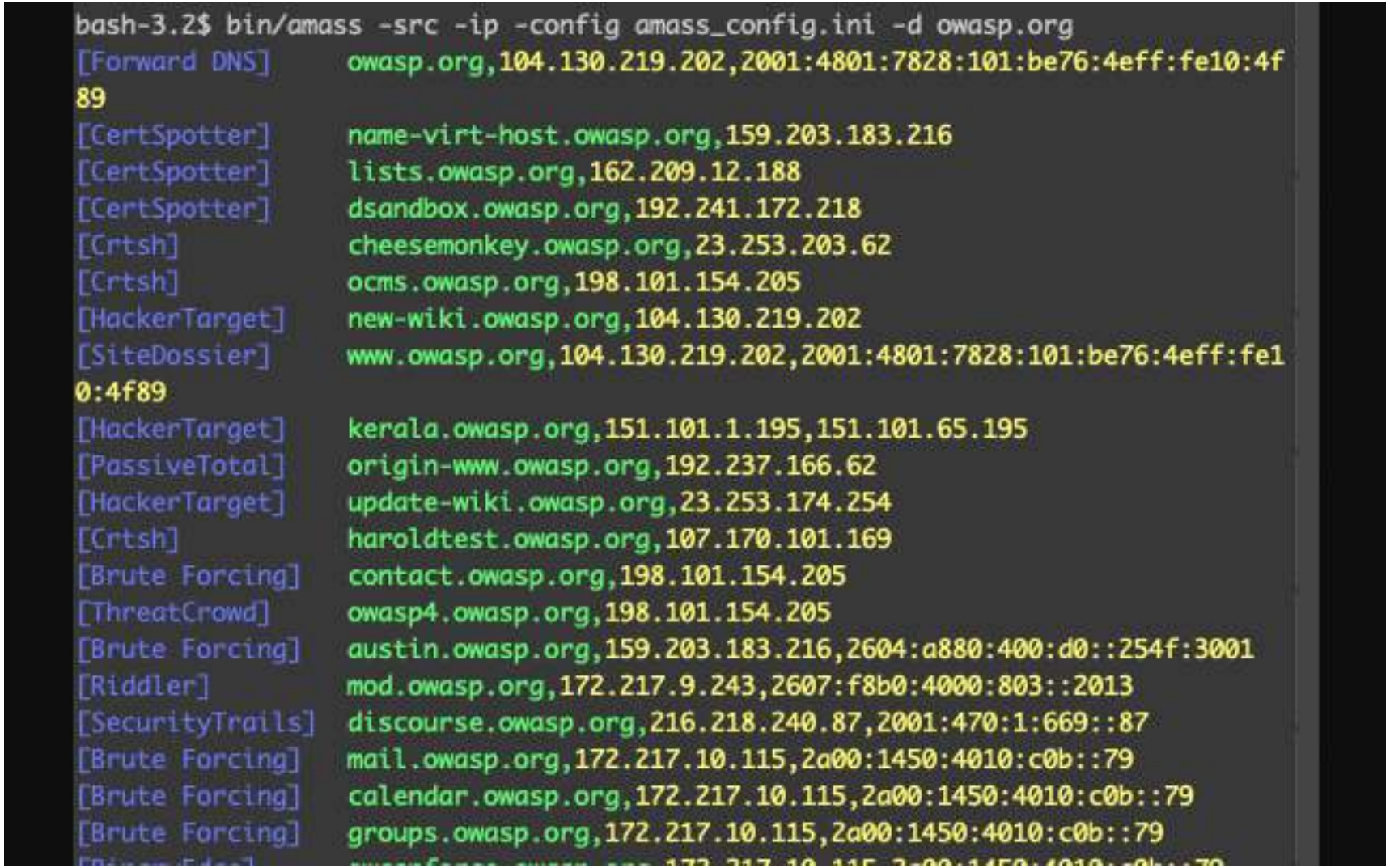
Let add a few file share access rules

Project Helix: Document Sharing and rule changes

But we have Multi Factor Authentication



Ransomware – Often we are not aware of our internet facing applications



1/6/2020
06:20 PM

Jai Vijayan
News

Widely Known Flaw in Pulse Secure VPN Being Used in Ransomware Attacks

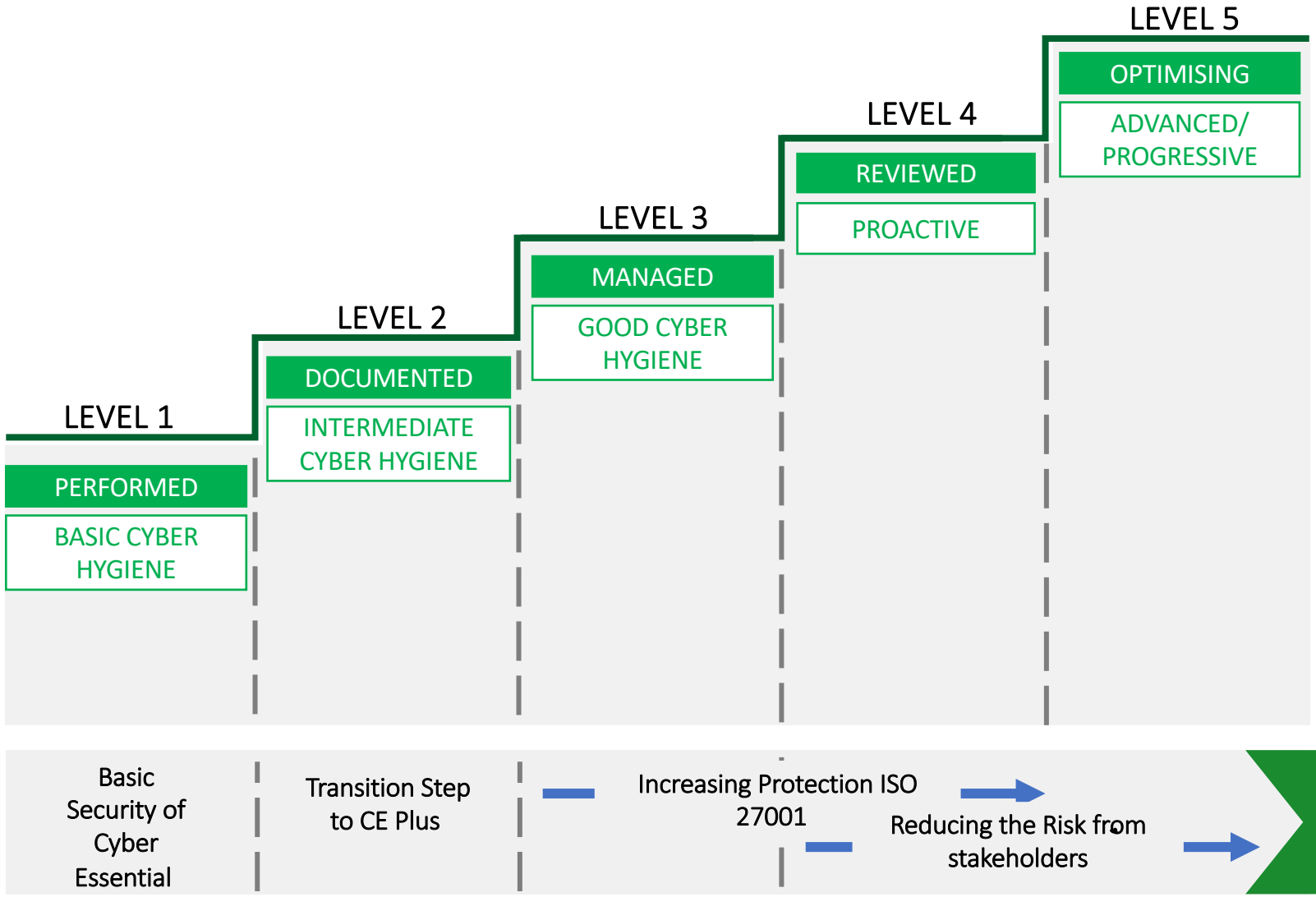
New Year's Eve attack on currency exchange service Travelex may have involved use of the flaw.

VPN provider Pulse Secure on Monday urged customers to immediately apply a security patch if they have not yet done so. The company issued the patch last April to

Key take away points

- Ensure auditing is enabled if using MS 365 and make sure your IT provider is!
- Conduct cloud ‘health check’ regardless of how secure you consider you are
- Conduct a digital scan of your sub domains
- Human is the fundamental weak point in many cases – real world training is important
- In many cases simply making our environment boring to the criminals works – time v reward
- Corporate engagement and understanding is key – Assurance is important

Building your Cyber Hygiene



UNDERWRITERS REDUCING THEIR RISK

Any tier in a Government Supply chain

Thank You

IF YOU THINK YOU NEED A HEALTH CHECK OR HAVE ANY QUESTIONS FEEL FREE TO CALL ME 07434812821 OR EMAIL ME AT LEE.H@BAMBOO.TECH

Bamboo Technology Group Ltd
2nd Floor, GC Campus,
Princess Elizabeth Way,
Cheltenham
Gloucestershire
GL51 7SJ