

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

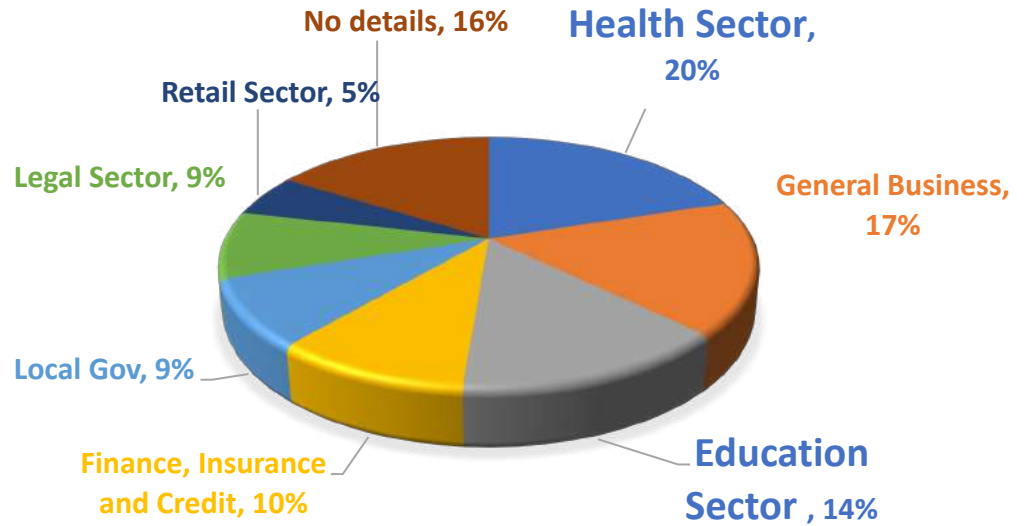


**Harvard
Business
Review**

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

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

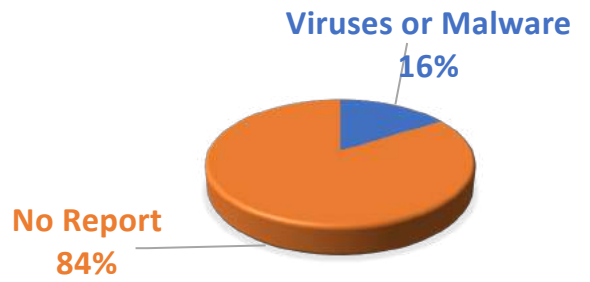
COMPLAINTS OF PERSONAL DATA BREACHES



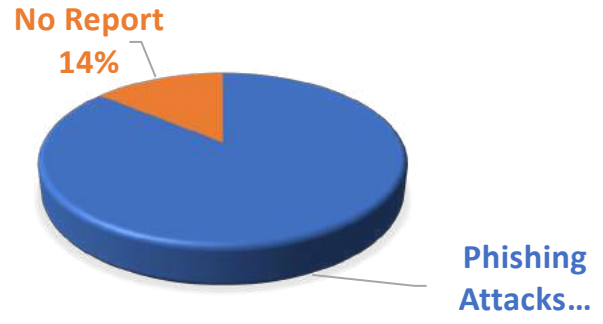
Cyber Attack Trends
 Almost half of all business (46%) and a quarter of charities (26%) reported having cyber security breaches or attacks in 2020.
[NCSC Annual Review](#)

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

BUSINESS EXPERIENCING VIRUSES OR MALWARE

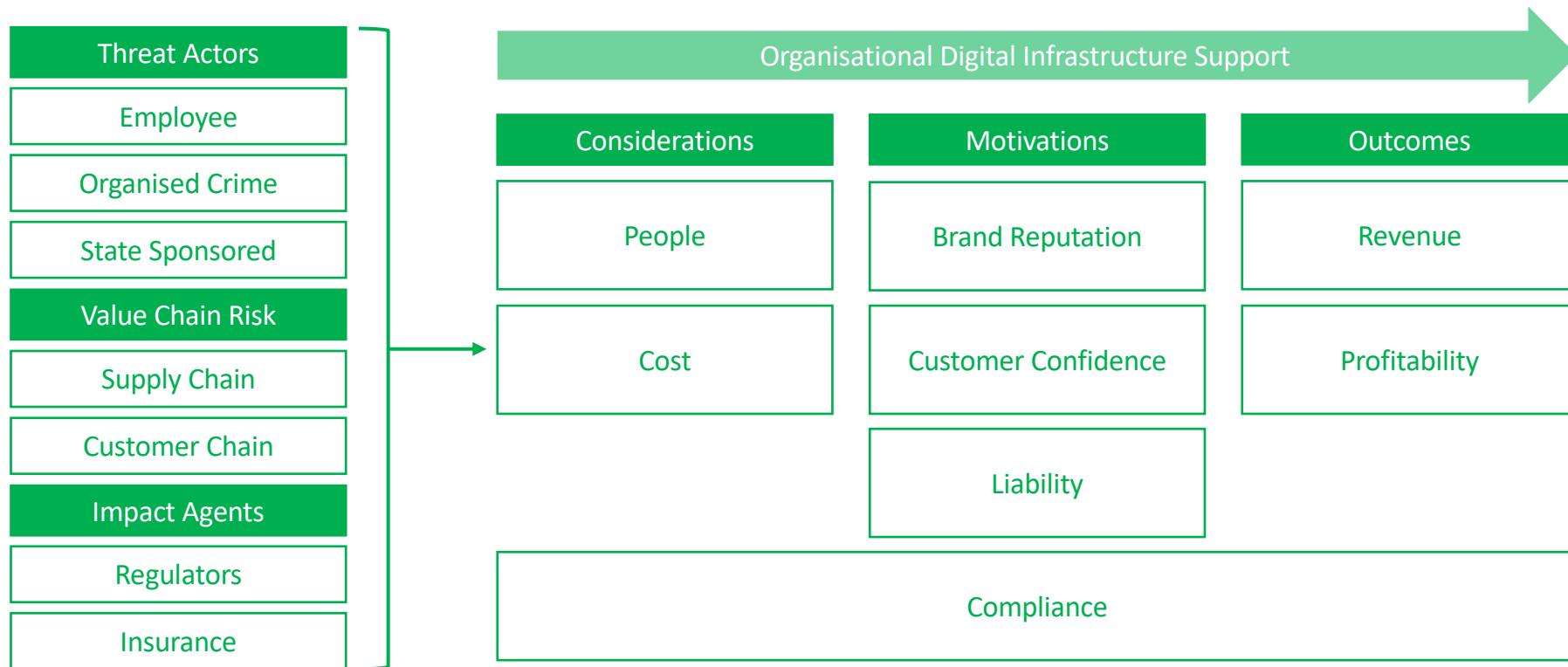


BUSINESS EXPERIENCING PHISHING ATTACKS

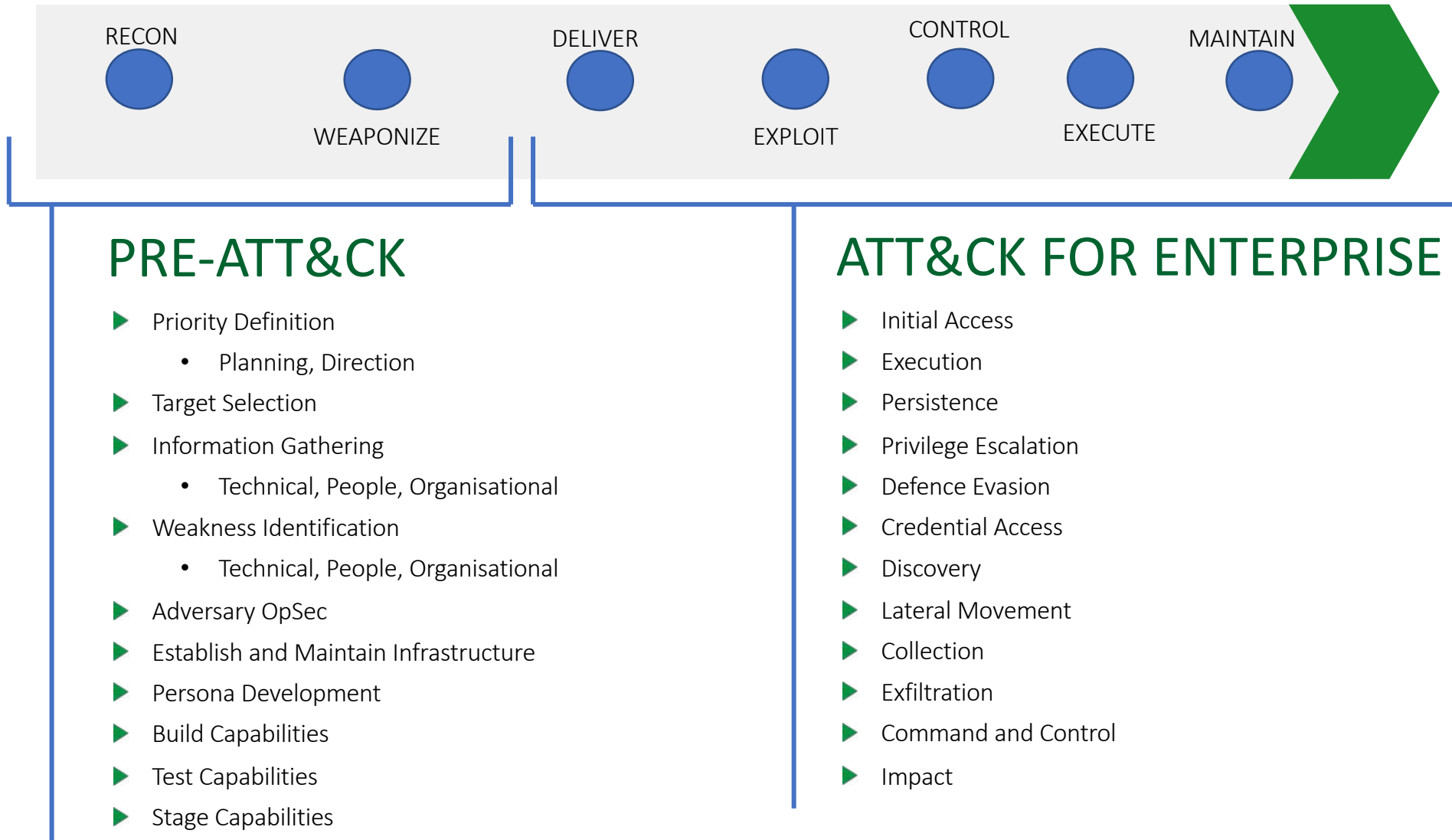


Protecting Organisational Objectives

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.

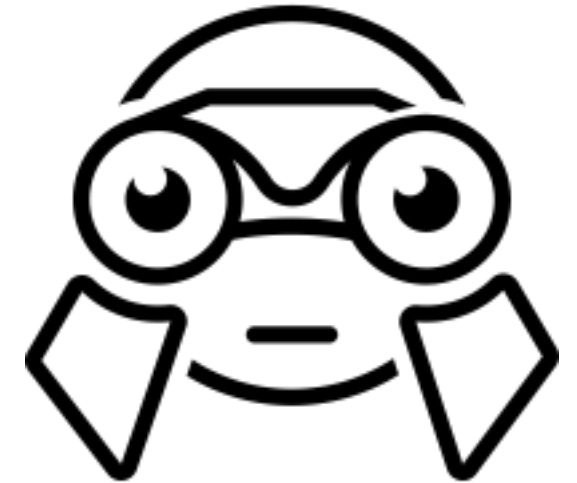


Criminals are organised



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



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.

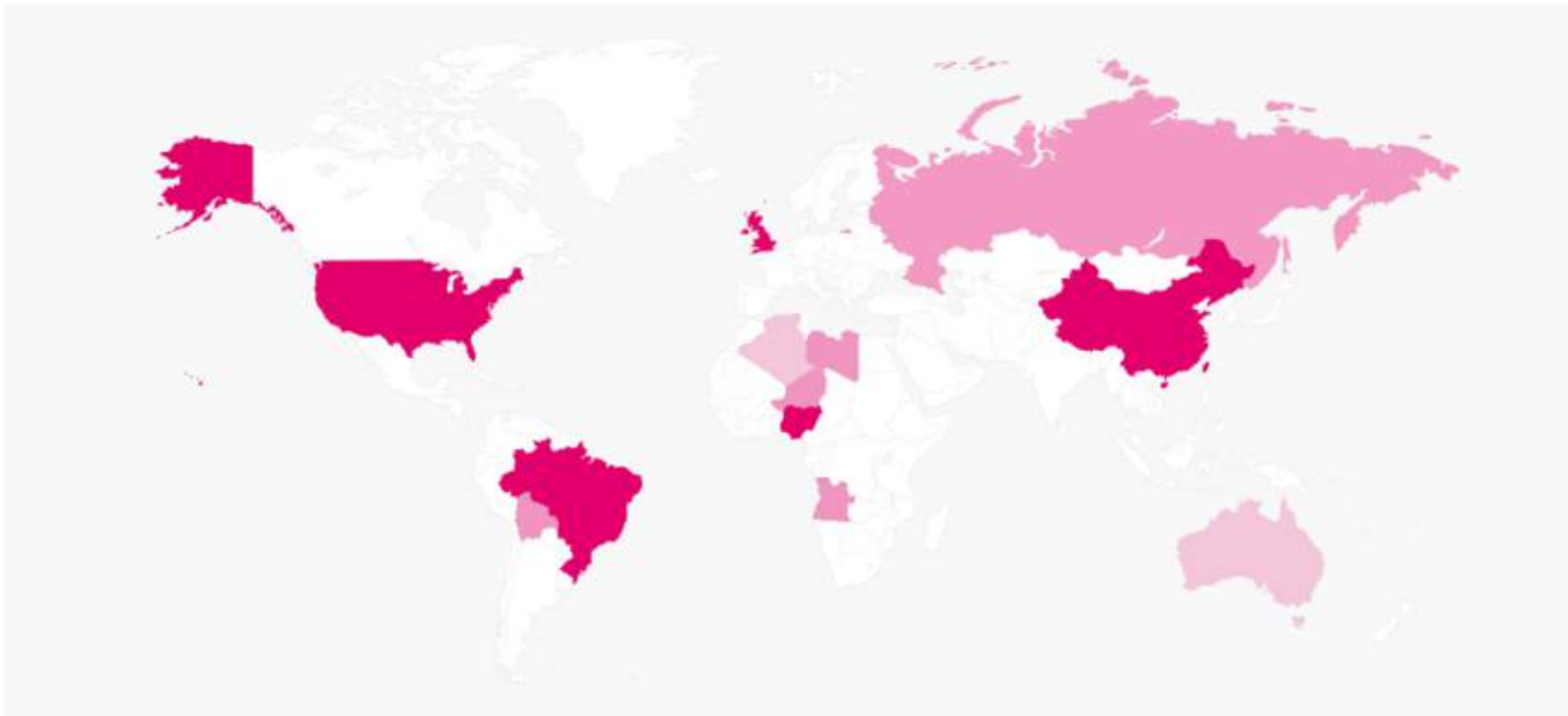
; Query time: 63 msec
; SERVER: 192.168.0.1#53(192.168.0.1)
; WHEN: Mon Jan 18 21:48:05 GMT 2021
; MSG SIZE rcvd: 94
```

```
;; 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'

The image shows a LinkedIn profile for Matt Scammell. The profile includes a circular profile picture, a blue 'Message' button, and text identifying him as a Commercial Director at Liverpool Football Club. A dropdown menu titled 'Contact Out' is open, showing email addresses and options like 'Find work email', 'Save Profile', and 'View Saved Profiles'. The right sidebar features a 'See jobs' button and a 'People also viewed' section with profiles for Phil Carling and Nicola Ibbetson.

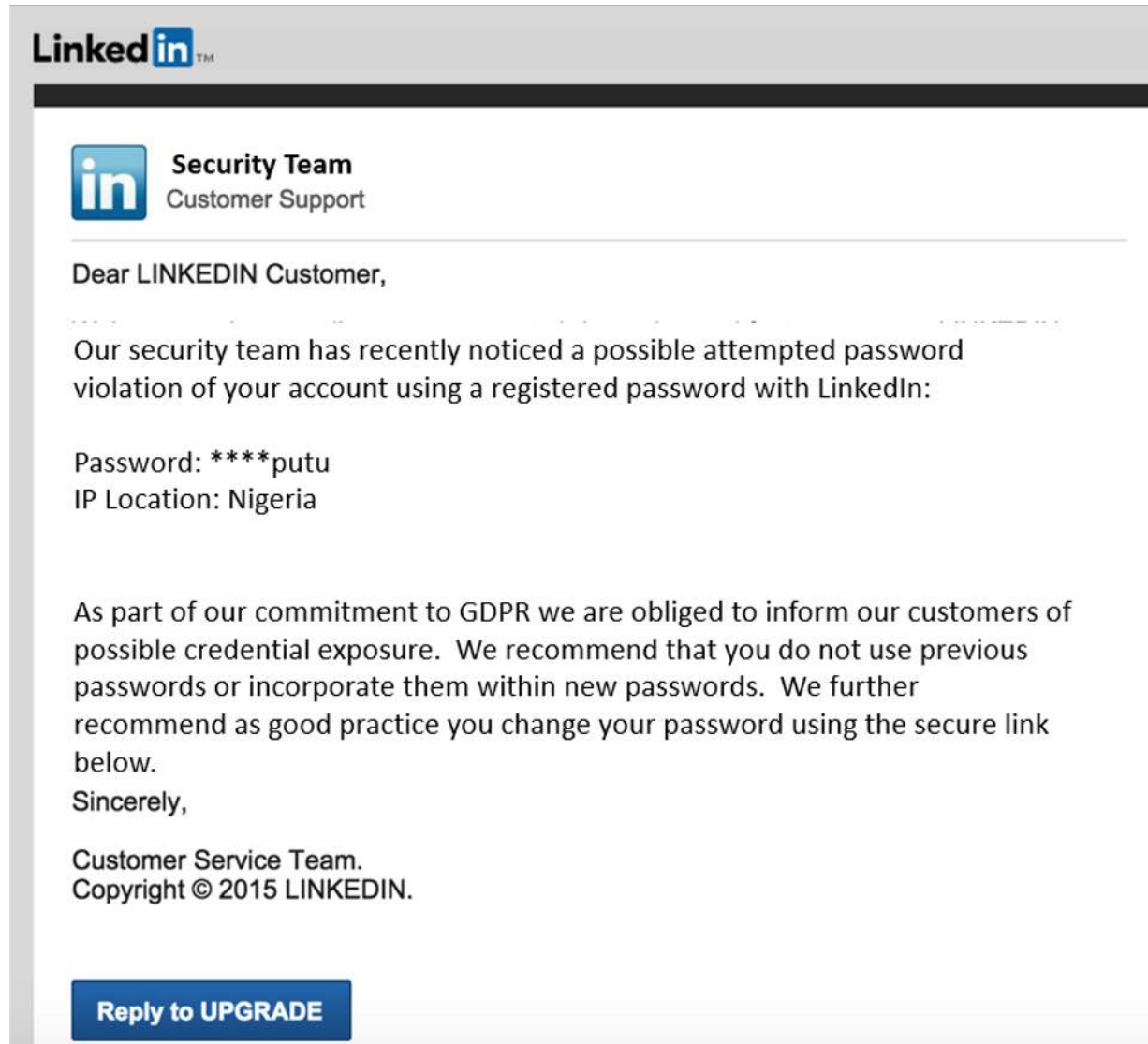
Profile Information:
Name: Matt Scammell · 3rd
Title: Commercial Director at Liverpool Football Club
Location: London, England, United Kingdom · 500+ connections · [Contact info](#)

Employers:
 Liverpool Football Club
 The Manchester Metropolitan University

Contact Out Menu:
Contact Out
✉ matt.scammell@gmail.com
✉ ?? matt.scammell@liverpoolfc.com
🔍 Find work email »
📄 Save Profile ▼
📄 View Saved Profiles
📄 Notes

Right Sidebar:
Liverpool Football Club that match your skills
[See jobs](#)
People also viewed
Phil Carling · 3rd
Managing Director of Football Octagon...
Nicola Ibbetson · 3rd+

Human led attacks



The image shows a screenshot of an email from LinkedIn's Security Team. The email header includes the LinkedIn logo and the text "Security Team Customer Support". The body of the email addresses the recipient as a "LINKEDIN Customer" and informs them of a possible password violation. It provides specific details: the password was "****putu" and the IP location was "Nigeria". The email also includes a warning about GDPR and a recommendation to change the password using a secure link. The email concludes with a signature from the Customer Service Team and a copyright notice for 2015. At the bottom, there is a blue button labeled "Reply to UPGRADE".

LinkedInTM

in 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

Home - Security & Compliance

protection.office.com/homepage

Office 365 Security & Compliance

Records management

Information governance

Supervision

Threat management

Mail flow

Data privacy

Search

Content search

Audit log search

Productivity app discovery

eDiscovery

Microsoft 365

Check out the new homes for Microsoft 365 security and compliance

Check out the new homes for Microsoft 365 security and compliance. Designed with accessibility and usability in mind, Microsoft 365 security center specialized workspaces for managing security and compliance across Microsoft 365 services. [Learn more](#)

Office 365 [Customize](#)

✓ We're committed to helping on your GDPR journey

GDPR is all about protecting and enabling individuals' privacy rights inside the European Union (EU). Our tools can help you detect, classify, and secure this sensitive info across locations (like Exchange, OneDrive, and more) and can also help you quickly find and export content in response to data subject requests.

[Go to the GDPR dashboard](#)

Search for users

Search for users

Information governance

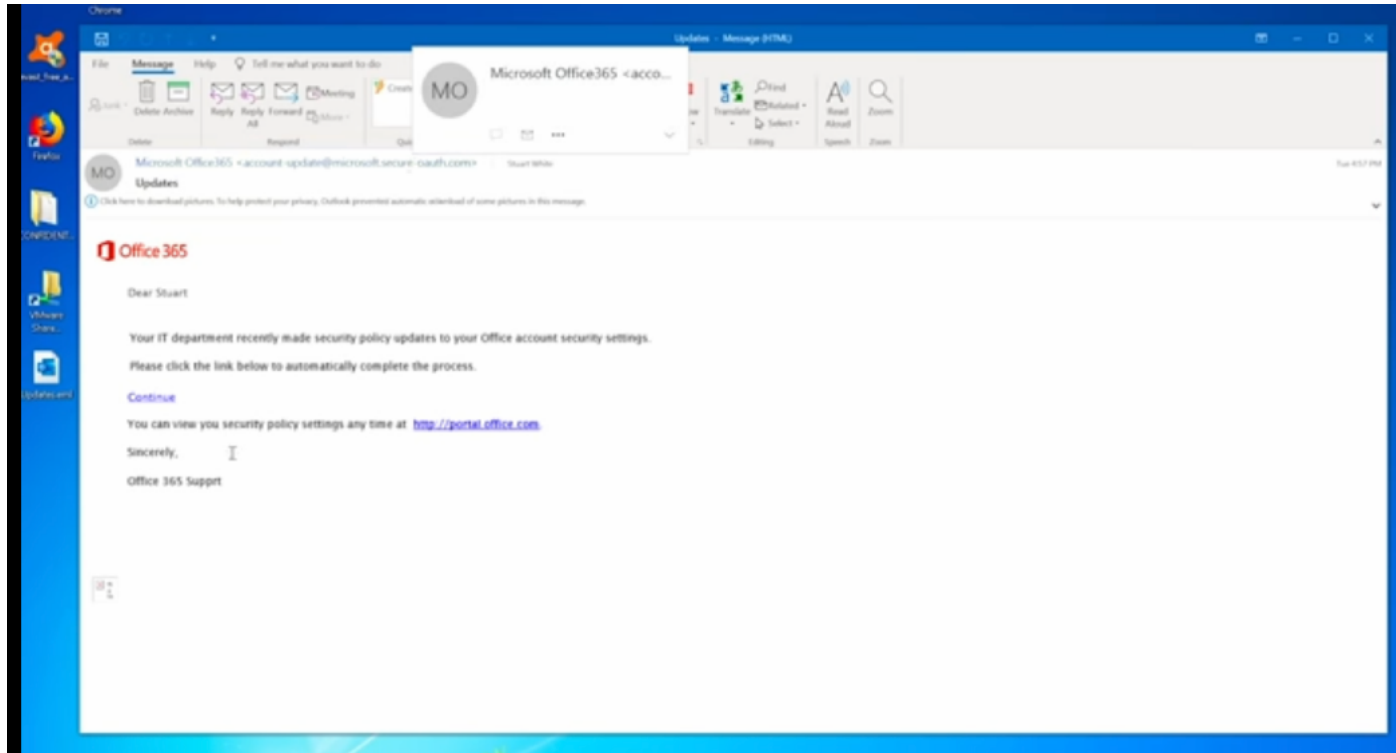
Microsoft Secure Score

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

```
bash-3.2$ bin/amass -src -ip -config amass_config.ini -d owasp.org
[Forward DNS]      owasp.org,104.130.219.202,2001:4801:7828:101:be76:4eff:fe10:4f89
[CertSpotter]     name-virt-host.owasp.org,159.203.183.216
[CertSpotter]     lists.owasp.org,162.209.12.188
[CertSpotter]     dsandbox.owasp.org,192.241.172.218
[Crtsh]           cheesemonkey.owasp.org,23.253.203.62
[Crtsh]           ocms.owasp.org,198.101.154.205
[HackerTarget]    new-wiki.owasp.org,104.130.219.202
[SiteDossier]     www.owasp.org,104.130.219.202,2001:4801:7828:101:be76:4eff:fe10:4f89
[HackerTarget]    kerala.owasp.org,151.101.1.195,151.101.65.195
[PassiveTotal]    origin-www.owasp.org,192.237.166.62
[HackerTarget]    update-wiki.owasp.org,23.253.174.254
[Crtsh]           haroldtest.owasp.org,107.170.101.169
[Brute Forcing]   contact.owasp.org,198.101.154.205
[ThreatCrowd]     owasp4.owasp.org,198.101.154.205
[Brute Forcing]   austin.owasp.org,159.203.183.216,2604:a880:400:d0::254f:3001
[Riddler]         mod.owasp.org,172.217.9.243,2607:f8b0:4000:803::2013
[SecurityTrails]  discourse.owasp.org,216.218.240.87,2001:470:1:669::87
[Brute Forcing]   mail.owasp.org,172.217.10.115,2a00:1450:4010:c0b::79
[Brute Forcing]   calendar.owasp.org,172.217.10.115,2a00:1450:4010:c0b::79
[Brute Forcing]   groups.owasp.org,172.217.10.115,2a00:1450:4010:c0b::79
```

1/6/2020
06:20 PM



Jai Vijayan
News

Connect Directly



4 COMMENTS

[COMMENT NOW](#)

[Login](#)



50% 50%



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

Related Content Sponsored by

RESOURCES

YOUTUBE

BLOG

VIDEOS



Service Account Security for Dummies eBook

See how to protect your service accounts before it's too late.



2019 State of Privileged Access Management (PAM) Maturity Report

PAM Maturity Assessment reveals four out of five not automating key privileged access capabilities.



Privileged Account Incident Response Template

The faster you respond to a cyber incident, the less damage it will cause.



Black Hat 2019 Hacker Survey Report

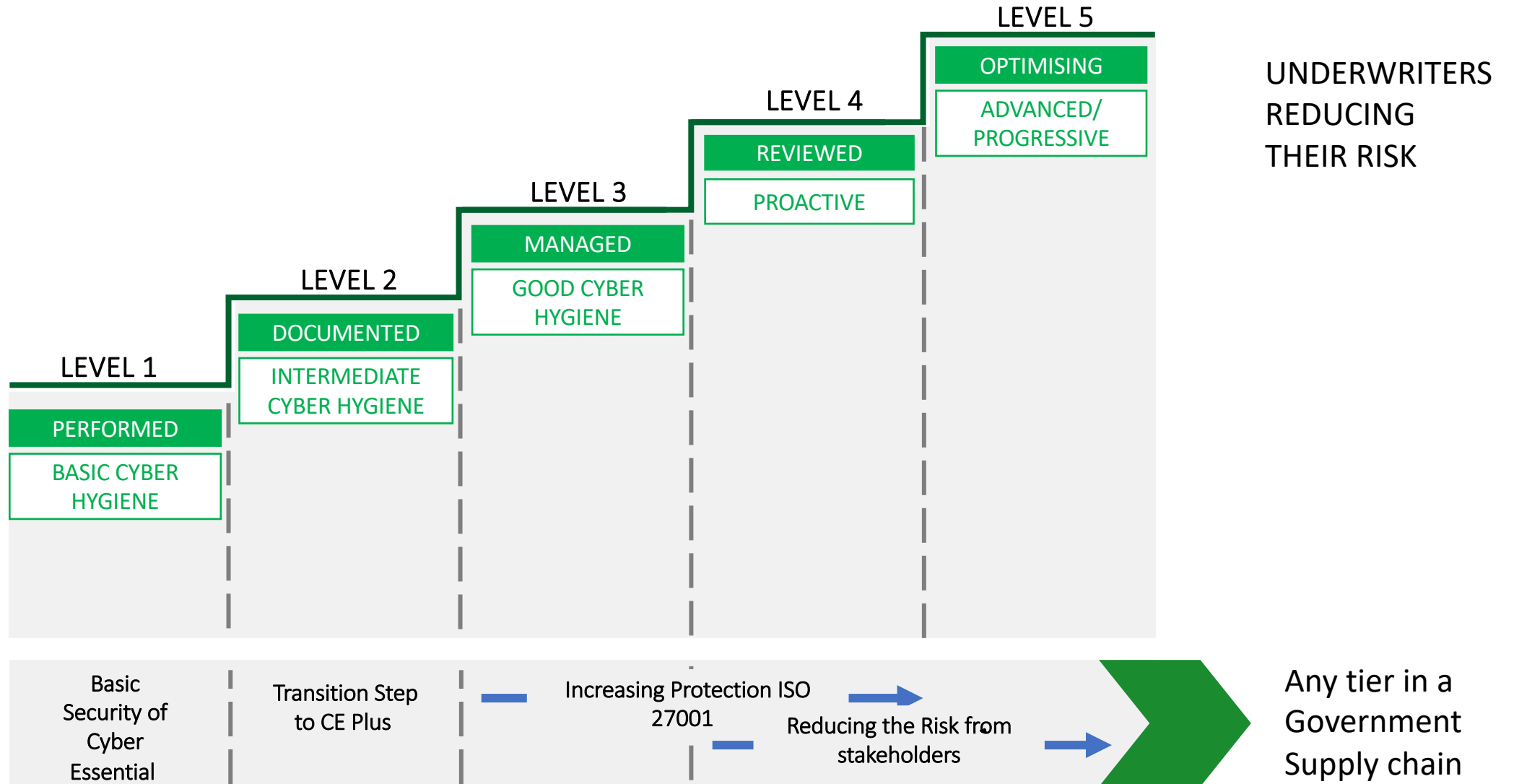
Key takeaways from the Black Hat 2019 Hacker Survey Report.



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



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