# Human Cyber Risk Management and Behaviour Change Platform

# Cyber Risk Aware

Creating your human firewall!!

**“Your staff are your greatest security asset, if helped in the right way .”**

**Stephen Burke**

Member of
Microsoft Intelligent Security Association

Microsoft

Gartner
Market Guide
Security Awareness Computer-Based Training

PDSC | bsi.
DIGITAL SECURITY PROVIDER

# Cyber Risk Aware

**Our Mission:** To protect people, institutions and cities from cybercrime through education and awareness that changes behaviour.

## *Market Disrupting Behaviour Change Technology*

Enabling positive human behaviour change in real-time, on any device, in any location.

*Our unique **real-time technology** is the future of protecting companies from the inside out.*

# Why help staff and not just focus on technical defences ?

## Cyber criminals are actively exploiting human behaviour vulnerabilities!

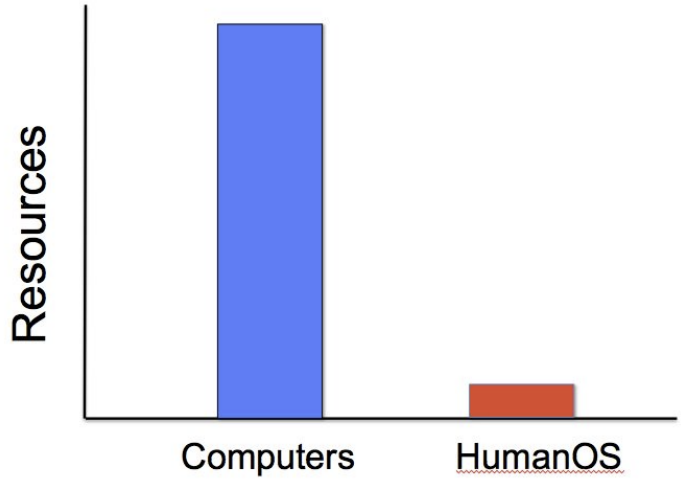
**Direct role in: -**

- **88% of total losses in the last 5 years**
- **66% of major data breaches**
  - **Lack of or ineffective security awareness**
  - **Social engineering**
  - **Unpatched systems**
  - **Weak configurations**
  - **Lack of appropriate defenses**

Source:- Verizon DBIR over the last 5 years

# What are security budgets being spent on ?

- **Operational infrastructure security (50 percent)**:
  - General Network Security
  - Identity and Access Management (IAM)
  - Privilege Access Management (PAM)
  - Endpoint and Data Security.




- **Vulnerability management and security monitoring (20 percent)**:
  - Vulnerability assessments, scanning and remediation
  - Security Operations Centre (SOC) and Security Information and Event Management (SIEM) costs.

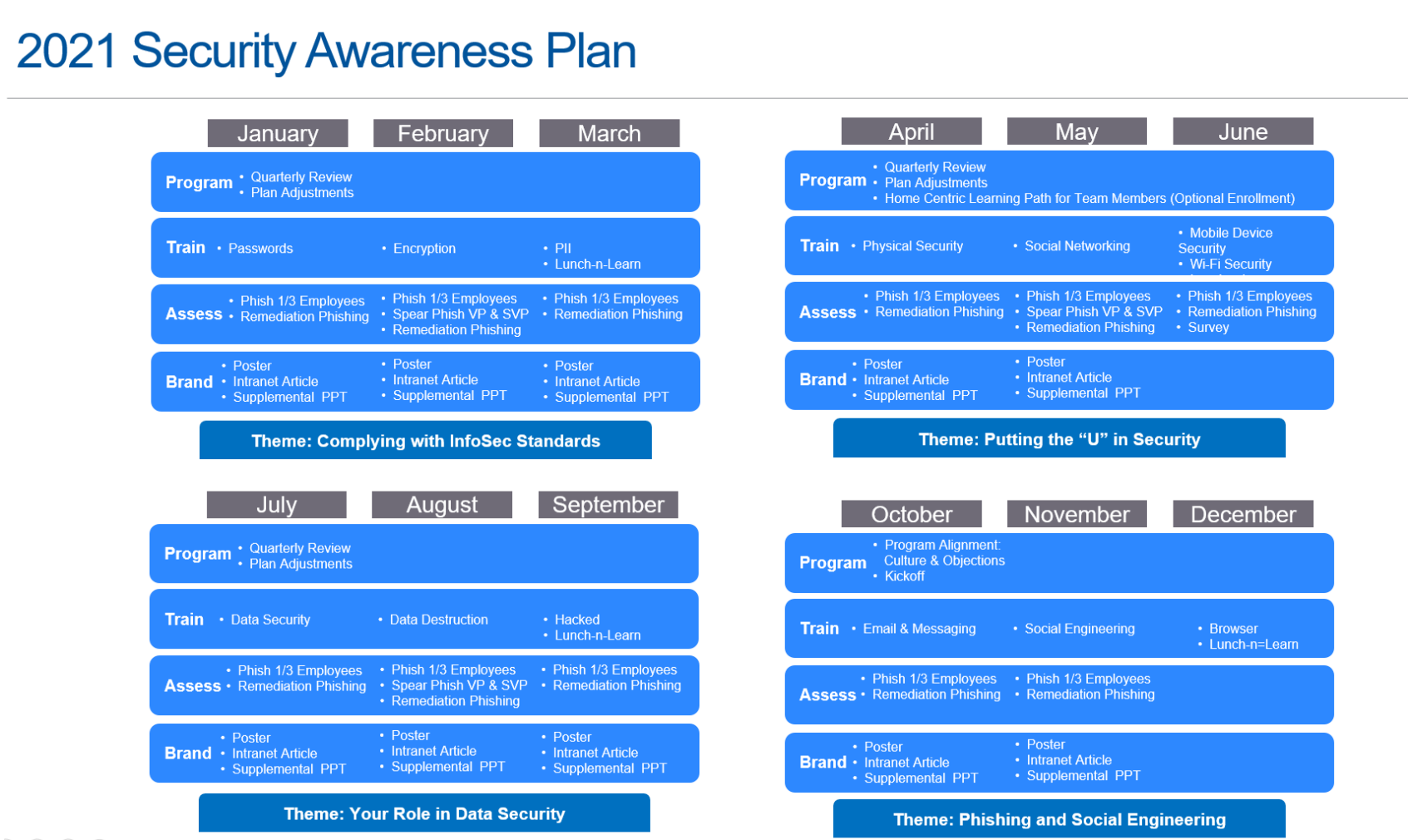
- **Governance, Risk and Compliance (GR&C) (16 percent)**:
  - Activities securing the company via an approved and certified framework, as well as complying with industry-specific regulations.

- **Application security (14 percent)**:
  - Combination of penetration testing practices geared towards improving hardware, software **and employees** from evolving threats.

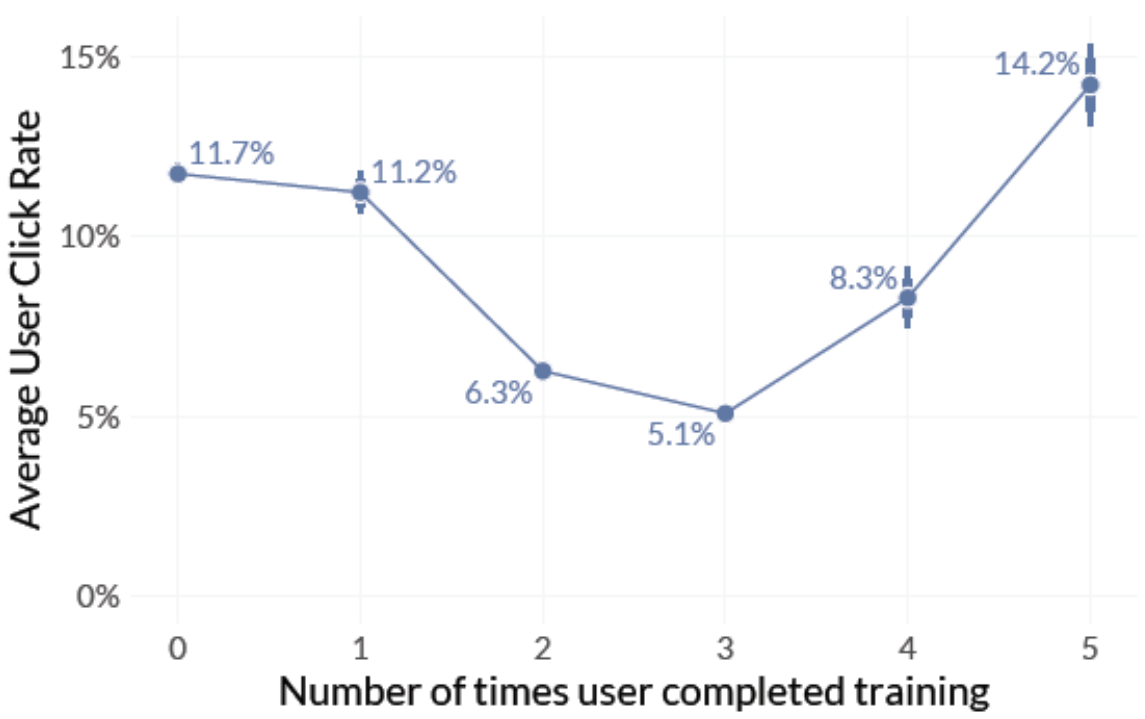
Source:- Gartner "IT Key Metrics Data 2019: Key IT Security Measures: by Industry," Eric Stegman

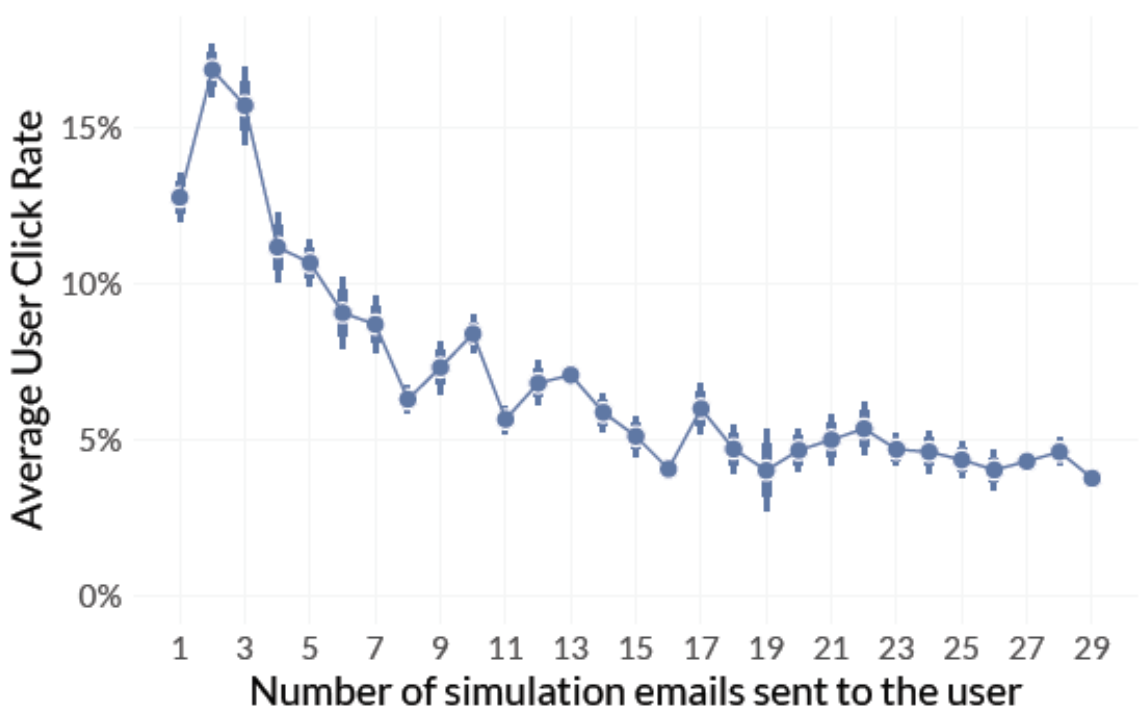
# Typical Security Awareness Programs

- Phishing Simulations
- Phish Report Button
- Training Courses
- Training Videos
- Policies
- Quizzes
- Reports
- In-person events
- Mascots
- Branded Collateral



# The results of just phishing and scheduled training....




Source:- Verizon DBIR over the last 5 years

# Observations to be aware of ....

**Traditional "spray and pray" staff training is not changing risky behaviour and is just a tick in the box exercise**

*Staff don't benefit from more tick-the-box training, they need help in the exact moment they conduct risky behaviour*

**Companies do not know who to train, nor on what topic, as they have no visibility into staff behaviour or knowledge gaps**

*Staff recidivism of risky actions, increases at an alarming rate when not provided with the correct security awareness training*

**Unable to measure or demonstrate the effectiveness of a security awareness training program**

*Phishing statistics and training completion rates alone, are wholly inadequate as they do not measure behaviour change*

# Human Cyber Risk Management


1. Identifying an organisation's top human risks.

2. Defining the key behaviours that most effectively manage those risks.

3. Communicating to, training, and engaging your workforce so they exhibit those key behaviours.

# Define Outcome Metrics

| Activity Metrics | Performance Metrics | Outcome Metrics |
| --- | --- | --- |
| **Mock Phishing** | | |
| # of mock phishing campaigns | Mock phishing click rate | Real phishing click rate |
| **Training** | | |
| # of training modules created | Training module completion rate | Targeted behaviour change after training |

# Instant learning moments, on any device, in any location, in response to actual user activity.

## Human Cyber Risk Assessments

Knowledge Assessments
Email Phishing Tests
SMS Phishing Tests

## Behaviour Database & Data Analytics

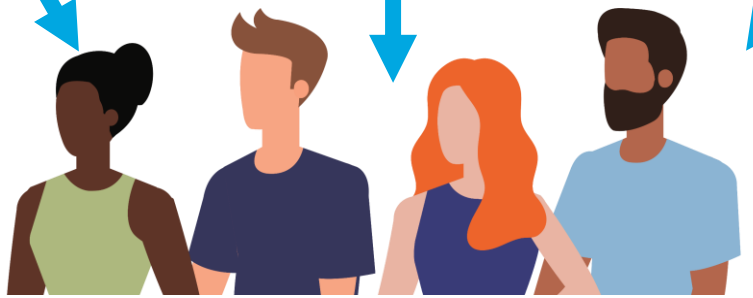
Behaviour Database
Behaviour Models
Tracking Behaviour Change
Human Cyber Risk Scoring
Cyber Essentials, GDPR, CCPA
ISO27001,NIST Compliance

## SOARDphish™ Phishing Analysis & Incident Response

Security Orchestration & Automation
Threat Intelligence
Security Incident Response Platform
Detect > Prioritise > Triage > Respond

## Contextual Training & Awareness Content Library

Training Content
(GCHQ Accredited)
available in 31 languages
Security Videos
Company Policies
Policy Breach Notices
Security Tips
Behaviour Alerts
Upload Existing Content



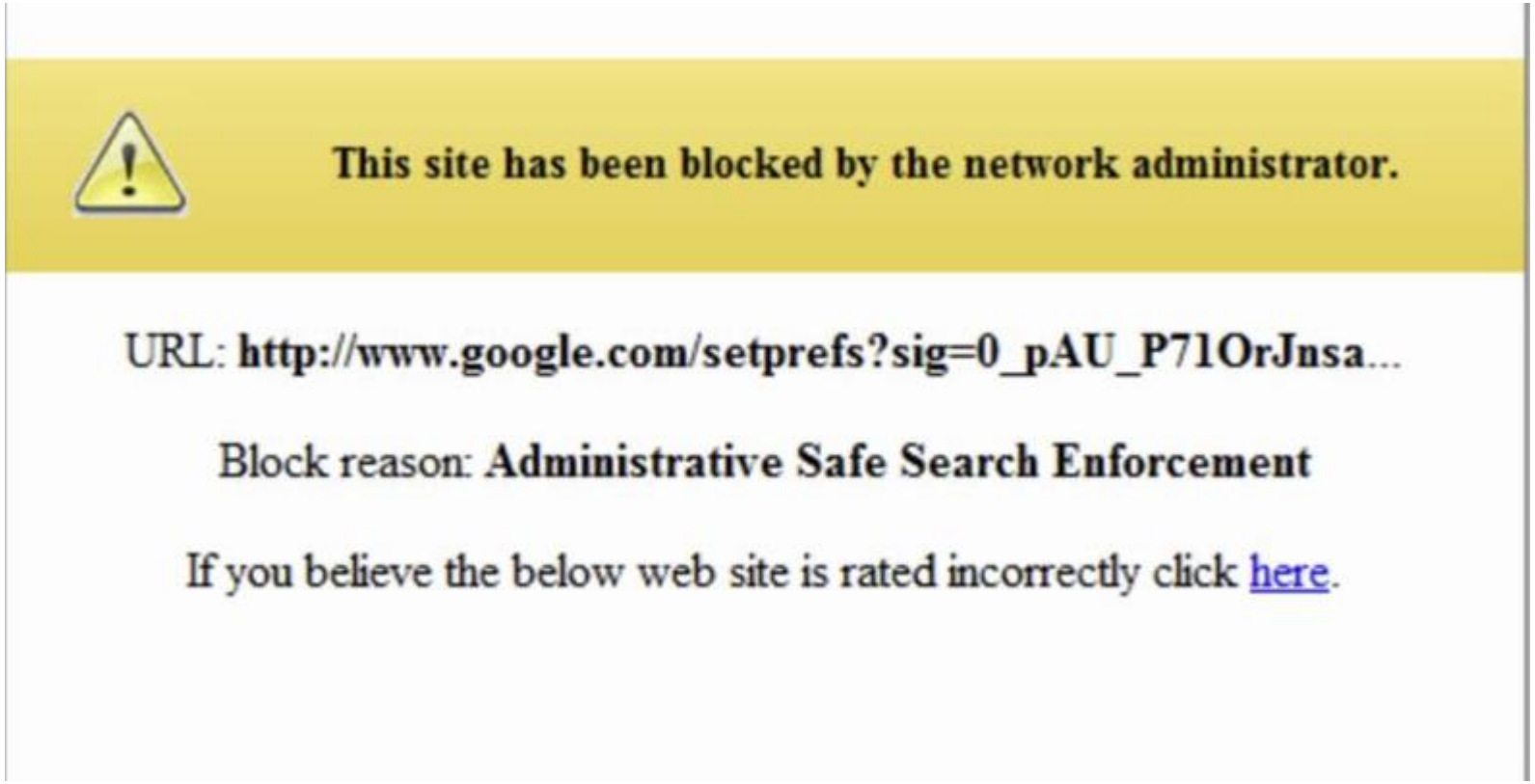
## Leverage Client Technical Defences

Network Behaviour Analytics
User Behaviour Analytics
Endpoint Behaviour Analytics
Data protection
Firewalls / Web Gateways
Anti-Virus
SIEM

(E.g. LogRhythm, Splunk, Azure Sentinel, LogPoint, DTEX)

**Human Cyber Risk Management and Employee Behaviour Change**

# USER TRIES TO DOWNLOAD FREE SOFTWARE




**What will the user do now ?**

# USER TRIES TO DOWNLOAD FREE SOFTWARE

Cyber Risk Aware
Creating your human firewall!

## Unapproved Software Detected!

Hey Stephen

We have detected an attempt to download or install unapproved software.

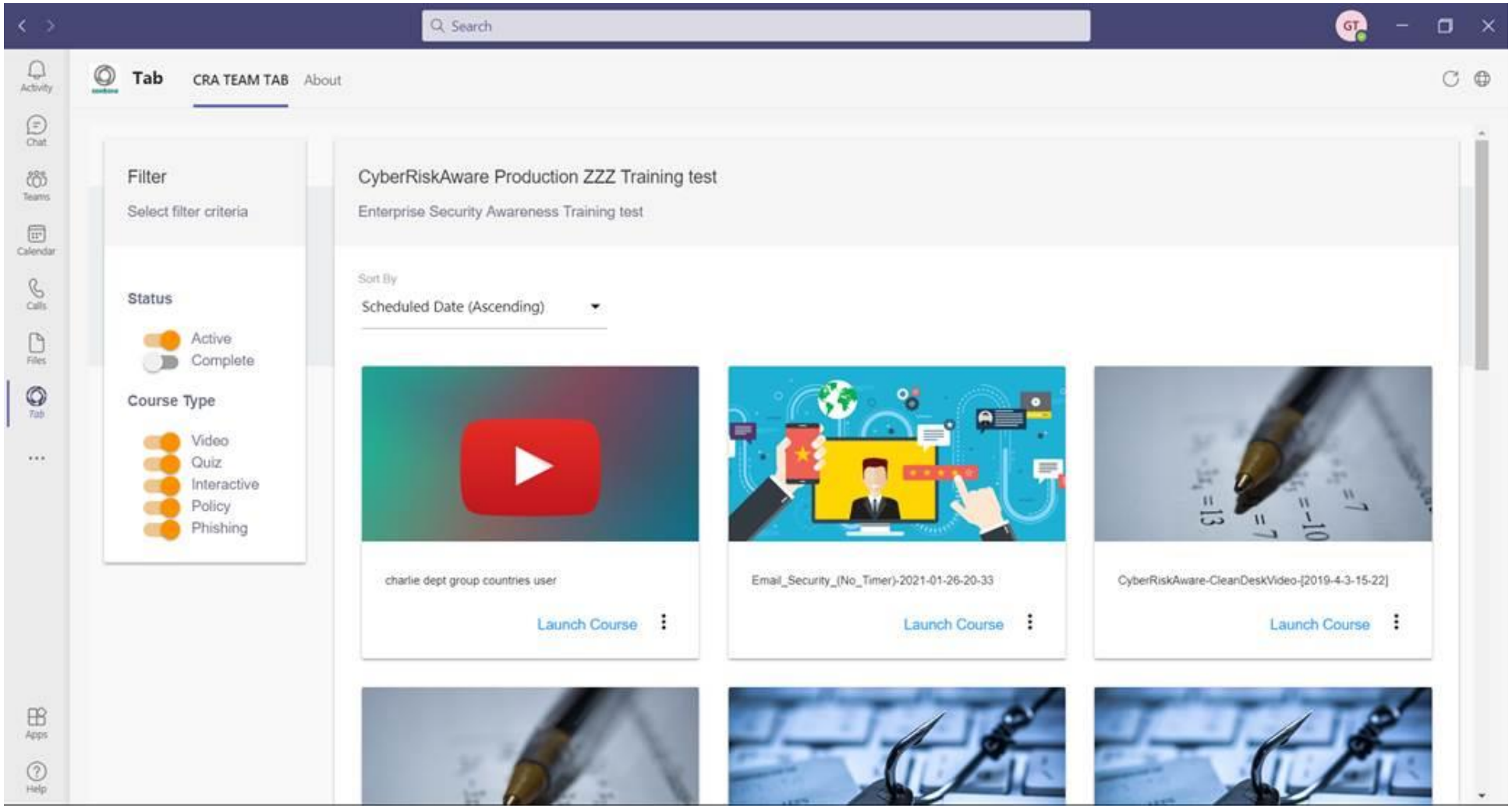
Whilst your intentions are good you may not realise that this creates a very high risk for the company.

Installing or downloading software which has not been approved by your IT Team can lead to malicious computer programs infecting the network and causing all sorts of problems such as Ransomware or Data Theft leading to fines or loss of our customers.

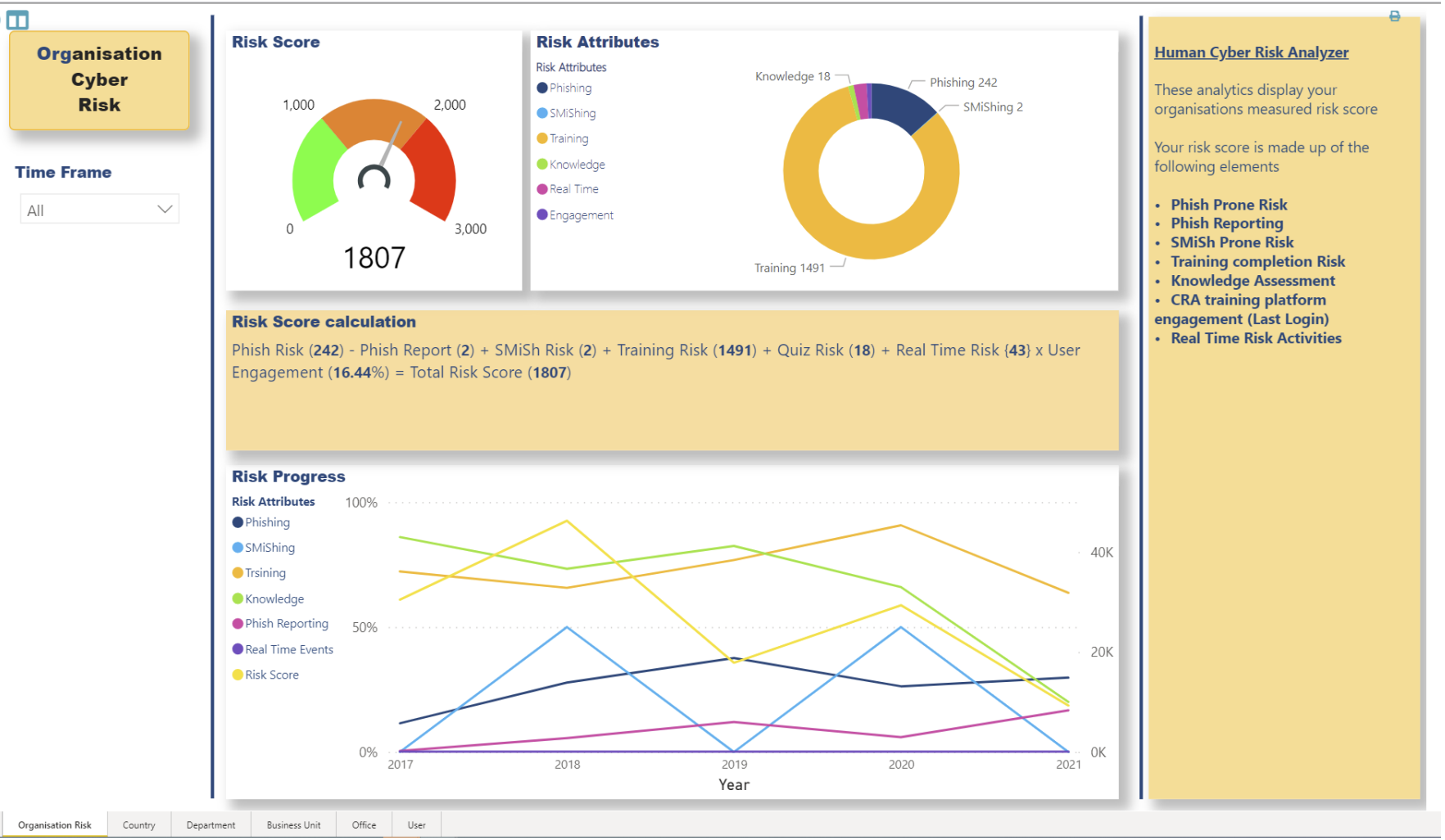
If you need any assistance with obtaining software or would like to see what software is on the approval list please click the button below.

Stay Safe!

# Ease of access = Consumption = Behaviour change



# Enhanced visibility and positive outcomes




Up to 90% reduction in staff phishing susceptibility

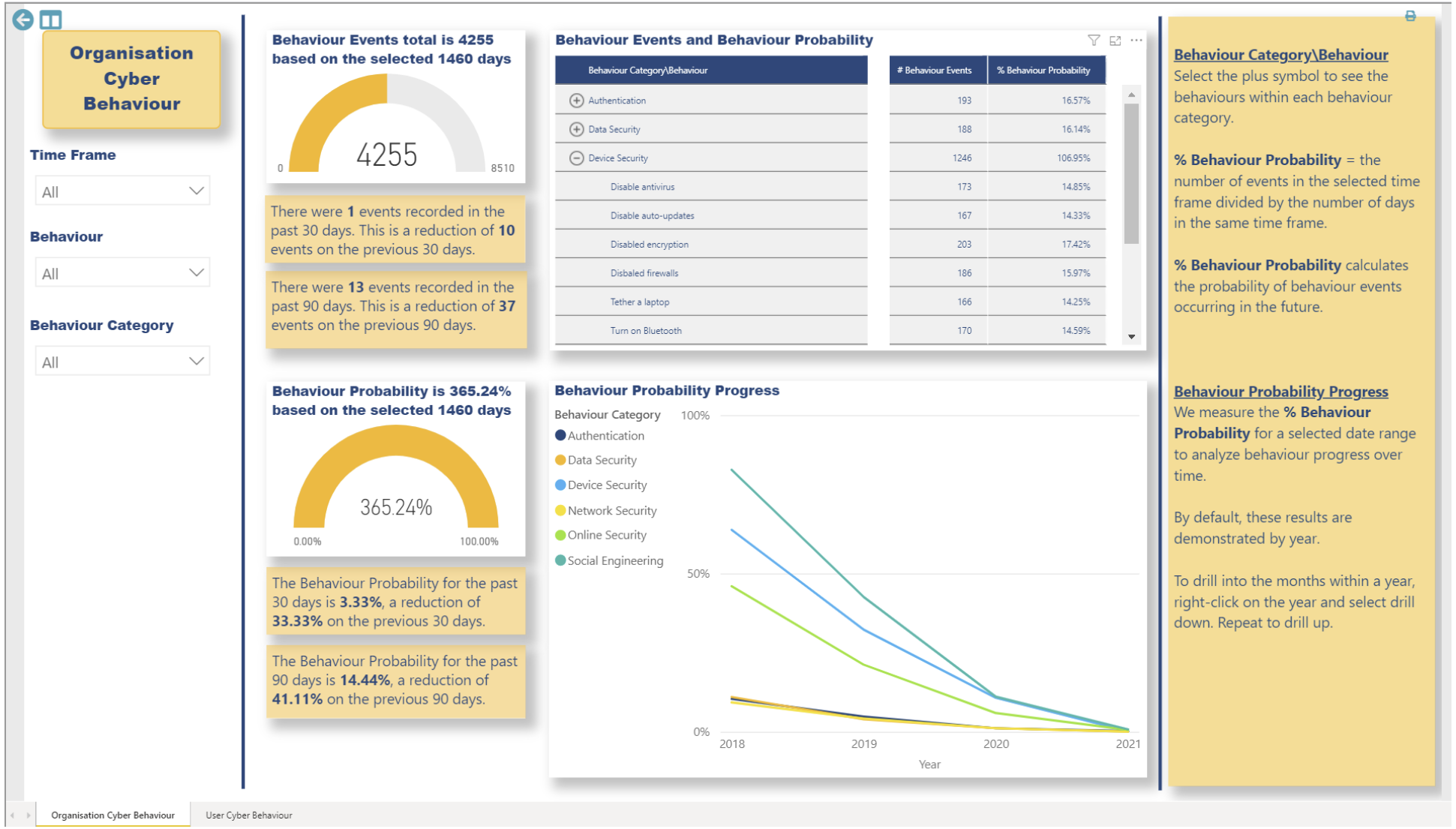
On average, 80% of staff see themselves as part of the security solution

Typical 70% reduction in training costs

Approx. 400% increase in metrics

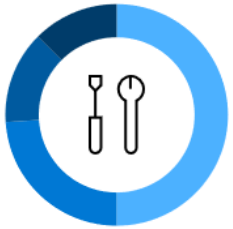
Up to 800% ROI against a single security incident

# Tracking Behaviour Probability



# Takeaways

- Identify Top Human Cyber Risks & Desired Behaviour Outcomes
- Help staff in their exact moment of need and not just on a schedule
- Phishing simulations and Training completions alone are not enough.
- Technical defences may not prevent attacks but do have a role to play.
- Staff are your greatest security asset, if helped in the right way!



Empower employees

Cyber Risk Aware
Creating your human firewall!!

# Thank You


Email: - stephen@cyberriskaware.com

Web: - www.cyberriskaware.com

Demo: - https://www.cyberriskaware.com/request-demo/


Member of
Microsoft Intelligent Security Association

Microsoft

Gartner
Market Guide
Security Awareness Computer-Based Training

PDSC bsi.
DIGITAL SECURITY PROVIDER

GCHQ Certified Training