



## Cyber Criminals No.1 Target? People!

Over 90% of security incidents started owing to human involvement.

Despite huge investments in technical defenses, Cyber Security Incidents continue to increase in frequency and severity. Every company has neglected their biggest risk of all, human cyber risk.

At Cyber Risk Aware we don't see staff as being the weakest link. They are in fact, the greatest security asset in every organisation. Our platform measures the level of Human Cyber Risk in a business, mitigates this material risk where found by raising staff awareness and enables clients to meet their compliance (e.g., GDPR, NY DFS, HIPAA, PCI-DSS, ASD4) and security accreditation (e.g., ISO27001, NIST, COBIT ) obligations.



### Why customers use our solution

- Assess the level of staff security awareness
- Assess the level of staff susceptibility to Phishing Emails
- Raise staff awareness and prevent cyber incidents from starting in the first place

### Enhanced Cyber Security

- Phishing Mitigation
- Increased Staff Security Awareness
- Reduced Security Incidents

### Meet Compliance Obligations

- Satisfy Increasing Regulatory Data Security Requirements (e.g., GDPR, HIPAA, PCI-DSS)
- Adhere to Security Best Practices
- Demonstrate Improved Cyber Security Resilience

### Risk Management

- Security Risk Management Framework Alignment (e.g., NIST, COBIT, ISO27001)
- Demonstrable Cyber Security Controls
- Effective Human Cyber Security Risk Management

**Within 12 months, 92% average improvement rate across all sectors.**

**Compliant within 1-3 months**

**Acceptable residual risk level within 1-3 months**

"Cyber Risk Aware provides a great, easy to install security awareness platform that has excellent content and provides the ability to generate simple and effective phishing emails. Staff are now more aware of their security responsibilities which rapidly resulted in fewer security incidents and support desk queries."

- William Magaw, CISO, - Council on International Education Exchange (CIEE)

Cyber Risk Aware solution deployed on Microsoft Azure allows customers to take advantage of the cloud, rapidly reduce human cyber risks and security incidents, meet compliance obligations and maximise their ROI on network technical defenses.



### Cyber Risk Aware effectiveness

- Substantial decrease in human cyber risks and incidents
- Phishing risk of 30% reduced to 2% within 12 months
- Substantial costs savings owing to fewer incidents and less downtime



### Cyber Risk Aware and Microsoft effectiveness

- Enhanced operating efficiencies leveraging CRA and Microsoft products
- CRA native integration with O365, A.D., Sentinel SIEM, A.T.P. and TEAMS
- Reduced B.A.U. administration costs

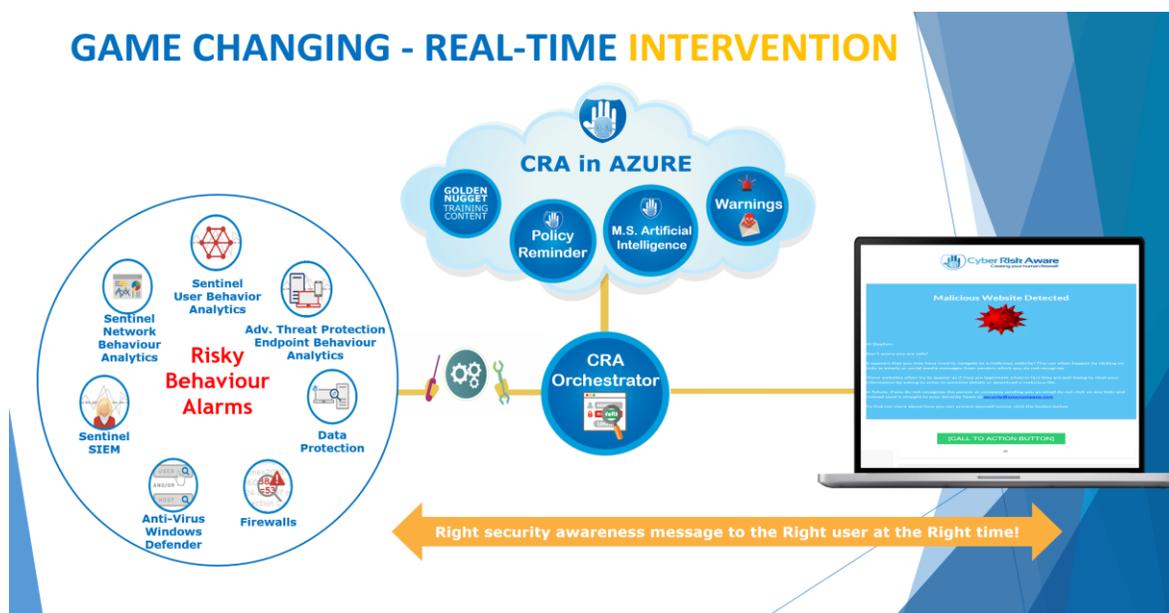
## Human Cyber Risk Solved!

We are confident that within 6 months human cyber risk and security incidents will be reduced by 50%, and a further 90% within a year.

## An offer to get you started

Get an understanding of how well your security awareness training programme measures up against your peers with a **free security awareness assessment**.

## GAME CHANGING - REAL-TIME INTERVENTION



Rather than training staff on a schedule, we offer continuous training to staff based in response to their network activity

- Help staff understand the cyber risks to the company owing to their specific actions on the network
- Eradicate users repeating risky behaviour by delivering messaging immediately in response to their risky actions
- Implement the most effective cyber security strategy by integrating technical defenses and security awareness training

### Why Cyber Risk Aware?

No other security awareness company in the world runs on AZURE nor can they deliver a fully automated and continuous security awareness program to staff. Rather than simply send content to staff on a schedule, we deliver the right message to the right user, immediately in response to their risky user behaviour being detected by a SIEM (e.g., Sentinel) or other technical defenses. In today's world, the only effective security strategy is one that looks at technical and human cyber risks combined.