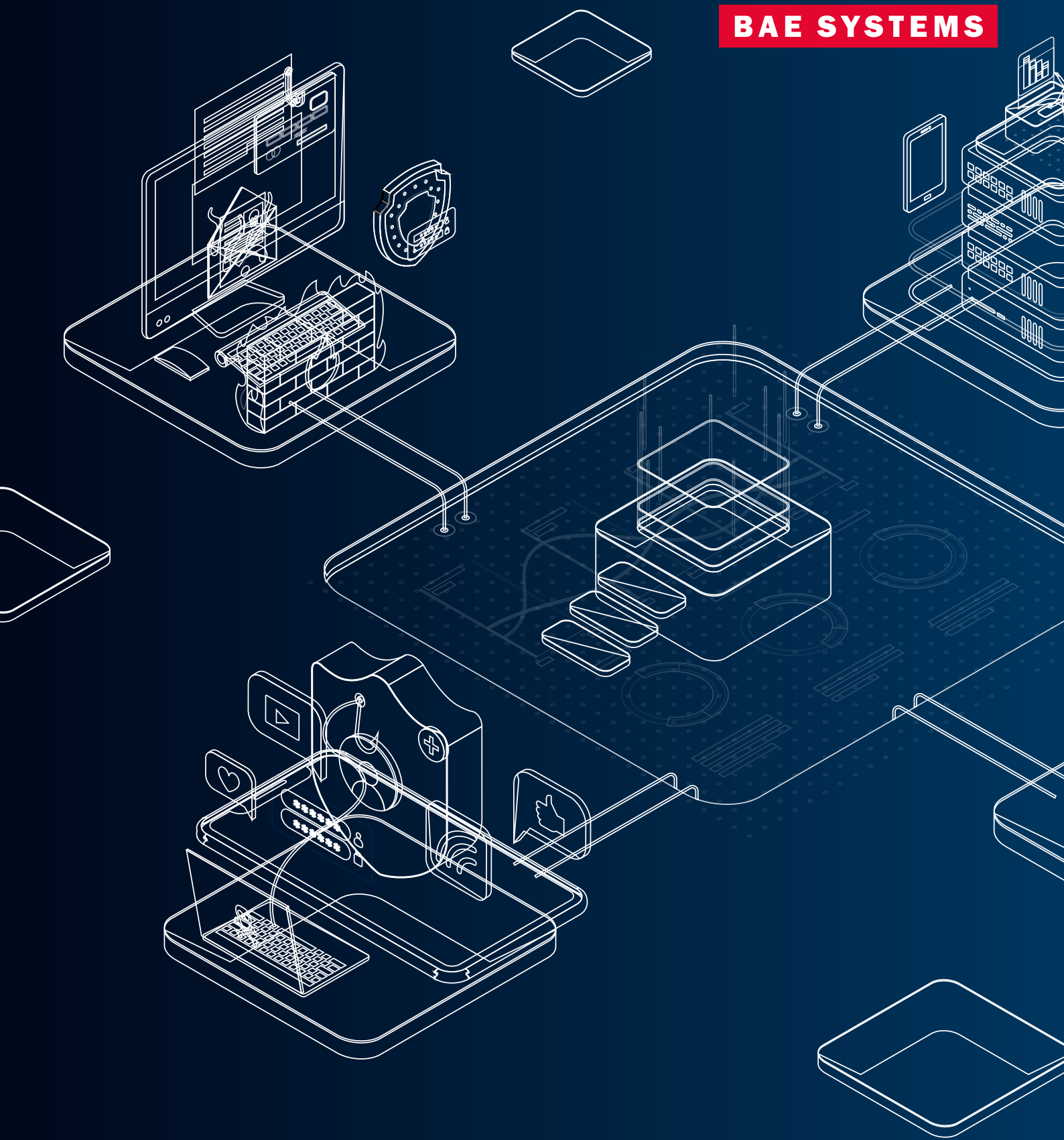
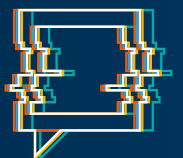


**BAE SYSTEMS**



# The **Intelligence** Network

Our Vision for **Tackling Cyber Fraud**



# Introducing our Vision for Tackling Cyber Fraud

When we launched The Intelligence Network a year ago, it was with the mission to safeguard society in the digital age. Since then, over 1,500 members have joined our cause, and our Steering Committee has established seven areas of focus, all of which we intend to tackle over time.

After consulting with members on where to start, we are first taking on the challenge of Tackling Cyber Fraud. You can find more detail about our other topics, and our journey so far, on our website.

With the guidance of our Steering Committee, and with valuable input from experts across industry, academia, government and law enforcement, we have researched the current cyber fraud landscape. This has allowed us to establish a vision for what we think 'good' would look like, if we are to tackle this major global problem.

The following document sets out our vision for change.

The process has been inspirational and stimulating, and on behalf of the Steering Committee I'd like to thank everyone for their involvement so far. Our commitment, as we continue to evolve our thinking, is to keep engaging the community in everything we do.

We therefore look forward to working closely together as we establish an action plan that will help us make our vision a reality.

James Hatch,

**Chair, The Intelligence Network**



# Why Tackling Cyber Fraud Requires Change

Fraud accounts for nearly half of all crimes, and over half of all frauds are cyber-enabled<sup>1</sup>. Cyber fraud is also a primary motivator for cyber attacks on all organisations, so should be high on the agenda for security teams, business decision makers, and more.

If it's so prevalent, and if it impacts so many of us, why haven't we managed to crack down on cyber fraud yet?

Over **1,500** members of The Intelligence Network  
**Six months** of research

## It's Time for Significant Change

By understanding the nuances of the problem space, we've mapped out a vision for stimulating change in four problem areas. **We believe that making these changes will significantly reduce society's vulnerability to cyber fraud.**

1. **Endemic attacks:** the prevailing mind set in cyber security is that organisations should think about "when" not "if" they suffer a successful cyber attack. But the high number of attacks is making it too easy for criminals to access the data they need to commit fraud.
2. **Operating in silos:** while there is some sharing of information between security teams and fraud teams, sharing across functions and industries is limited and joint action is rare.
3. **The cyber to fraud gap:** effective cyber security, counter fraud and law enforcement are all critical to tackling cyber fraud, but are currently treated as ends in themselves and have their own objectives and terminology.
4. **Social engineering:** the ability of criminals to deceive people is at the heart of both cyber attacks and fraud. Most current effort goes into training people to make near impossible judgements, rather than making their tasks easier.

The goal to introduce change in these areas breaks down into 12 more detailed demands.

# Our vision for tackling cyber fraud

## Four crucial areas of change

The goal to introduce change in these areas breaks down into 12 detailed demands

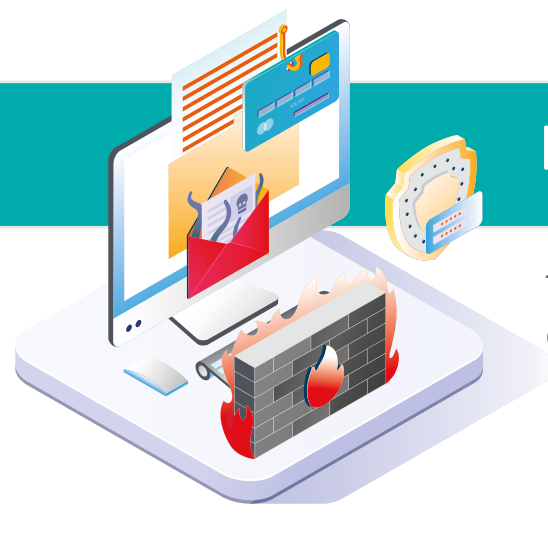


We are continuing to **gather proof** that these changes are important



Let us know if you have evidence to share  
[theintellancenetwork@boesystems.com](mailto:theintellancenetwork@boesystems.com)  
[www.boesystems.com/intellancenetworkhub](http://www.boesystems.com/intellancenetworkhub)





## I. Endemic Attacks



To tackle cyber fraud we need to address the issue of endemic attacks

### Why do we need to see change?

The prevailing mind set in cyber security is that organisations should think about ‘when’ not ‘if’ they suffer a successful cyber attack. But the high number of successful attacks is simply making it too easy for criminals to access the data they need to commit fraud. Making a real difference to the endemic level of cyber attacks is difficult. In the long term the only viable answer is that security becomes built-in to technology and working practices. This will not be enough to stop all cyber attacks, but will shift the economics of cyber fraud in society’s favour.

### 1a. **Vision:** cyber hygiene is the default across all sectors – prioritised by businesses and built in by suppliers

Purchasers of technology and business services have considerable power to demand levels of security in the aggregate, but as individuals their power is reduced. On the one hand, market demand is improving the level of security that suppliers provide, but that is not true of the cheapest or default options. Collective action and campaigning has the potential to accelerate improvements. In fact, in situations where purchasers (especially consumers) do not have the information or power to protect themselves, there is a case for moving towards regulation, for example, to support a secure by design approach<sup>2</sup>.

“There is currently a culture of ‘going through the motions’ when it comes to cyber hygiene. This is coupled with an ‘ease over security’ attitude where people do the minimum to protect themselves, leading to data hacks and subsequently to fraud.”

Phil Chapmon, Firebrand  
The Intelligence Network Corporate Supporter

### 1b. **Vision:** cyber and fraud risk are an integral part of business strategy and new service development

Rather than being a retrospective consideration, we need security to be built-in to organisations, with a move towards cyber security models which are able to adapt along with the ever-evolving attack landscape. As situations evolve, so too should the management of risk and funding of controls, making it harder for criminals to achieve a breach that leads to fraud.

We need to see security considerations built into decision-making, and security should be an integral part of non technical roles. Certainly, where larger organisations may have enterprise risk management processes in place, these considerations are sometimes already covered, but a more pervasive approach will benefit the whole community.

“A recent roundtable event on fraud between The Intelligence Network and ADS members in the cyber security sector found that we need to move towards a culture where security is as important to organisations and their customers, as user experience. Having established this vision, we can now plot out a valuable action plan that will help all parts of industry make the crucial changes necessary. This needs to be a collaborative endeavour and, if we can improve our collective resilience against attacks, we will ultimately make cyber fraud a harder crime to commit.”

Dr Hugo Rosemont, Director – Security and Resilience Sector, ADS Group  
The Intelligence Network Corporate Supporter

### How do we make change happen?

We want to put in place some clear actions to shift the economics of fraud by making breaches harder to achieve. These may include some of the following actions and we are consulting with our members to confirm our approach:

- **Support cyber hygiene initiatives** (e.g. Cyber Essentials) and particularly the convergence of these internationally to improve consistency and reduce costs
- **Develop a simple model of security by default**, especially for new and smaller businesses that can operate fully in the cloud
- **Work with cloud platform providers** to make secure configurations the default ‘opt-out’ option rather than the ‘opt-in’ exception
- **Promote security-centric approaches** to moving to the cloud so security and cloud benefits reinforce each other rather than conflict
- **Support the long term evolution of the cyber insurance sector** to strengthen the economic incentives for cyber hygiene
- **Support community sharing initiatives** (eg Open Security Summit) that encourage reuse of both technical security approaches and business approaches such as investment cases for security

If you would like to contribute to delivering these changes, please get in touch with us.



## 2. Operating in Silos



To tackle cyber fraud we need to stop operating in silos

### Why do we need to see change?

While there is some sharing of information between security teams and fraud teams, sharing across functions and industries is limited and joint action is rare. There's no doubt that sharing can be difficult, particularly when it involves trusting others with sensitive information, but it's important to build models for this, in order to enable joint action.

#### 2a. **Vision:** cyber fraud is understood across functions within and between organisations

We must create a culture where information sharing is the norm, and where each party considers their information in relation to the bigger picture. Cyber fraud, security and financial crime teams frequently hold different pieces of the same puzzle, but struggle to collaborate in order to tackle instances of cyber fraud. Therefore, practical joint teams, or separate teams with shared objectives, could be established within and between organisations to speed up the process of dealing with fraud.

#### 2b. **Vision:** organisations are recognised for sharing useful information not punished for suffering an attack

We need to move towards a landscape where the importance of sharing information is acknowledged, and where it is possible to share effectively. As seen in the development of safety mechanisms in other sectors, such as aviation, there are significant long term benefits to be gained from continued learning and improvement.

Currently, organisations are reluctant to be transparent, and this is often because post-breach stories from media and industry commentators tend to focus on the negative, rather than the positive point that organisations sharing information are trying to do the right thing.

"A recent well-publicised attack resulted in the affected power company adopting a transparent approach, arguably helping to limit further damage. But this is uncommon. Often, communication problems stem from a misunderstanding of how valuable the information held can be in a wider context. Linked to this is the fear of embarrassment and exposure of weaknesses."

Robert Clifford, BAE Systems Applied Intelligence  
The Intelligence Network Member

#### 2c. **Vision:** business and law enforcement collaborate effectively to tackle cyber fraud

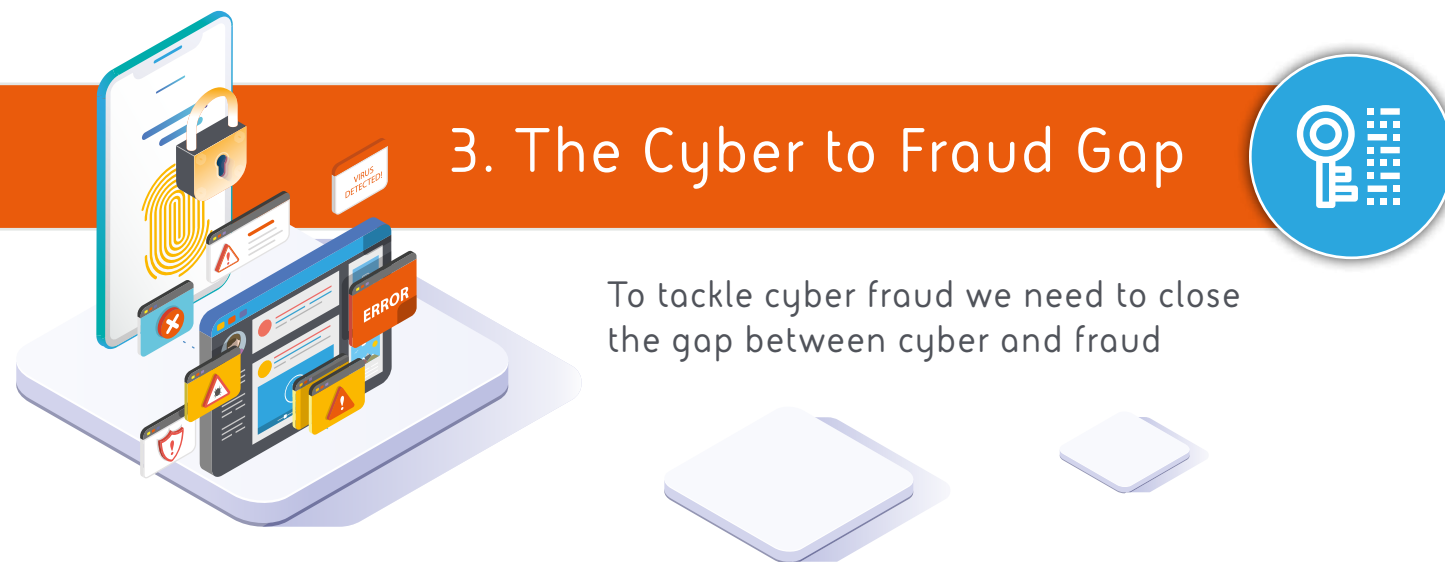
If information sharing is difficult, joint action is even more difficult but also more valuable – because different parties have different information, power and resources that could together have a significant impact. However, law enforcement and businesses understandably have different objectives – whereas businesses will mostly focus on damage limitation, law enforcement will look to prosecute the perpetrators. Their differing objectives naturally mean that levels of joint action have been limited to date. Improved information sharing and understanding of the wider fraud economy is the starting point, but organisations need help to remove the barriers to joint action.

### How do we make change happen?

The Intelligence Network was formed to help facilitate collaboration across the industry in order to break down silos. Specifically when it comes to tackling cyber fraud, our activities may include:

- **Develop a cyber fraud intelligence model** for capturing information from all fraud attempts including failed attempts and customer experiences
- **Trial cross-functional sharing and action** (between cyber security and fraud teams both within and between organisations) and publish case study on learnings
- **Develop links** between existing cyber security, fraud and financial crime intelligence sharing platforms to develop a more complete picture of the cyber fraud ecosystem
- **Launch a mechanism for raising Suspicious Activity Reports** for fraud (analogous to existing systems for money laundering), with an appropriate intelligence task force (similar to the UK Joint Money Laundering Intelligence Taskforce) to enable action particularly against criminals carrying out high volume low value fraud
- **Analyse and reduce the barriers to collective action**, including clarifying legal and regulatory constraints

If you would like to contribute to delivering these changes, please get in touch with us.



### 3. The Cyber to Fraud Gap

To tackle cyber fraud we need to close the gap between cyber and fraud

#### Why do we need to see change?

Effective cyber security, counter fraud and law enforcement are all critical to tackling cyber fraud. However, there is a disconnect between legal frameworks, the realities of cyber fraud, and its impact on society. Meanwhile, radically different perspectives have led to complicated and varied cyber fraud terminology among cyber fraud stakeholders. All of this amounts to a 'gap' between cyber and fraud which needs to close if we are to shift towards a society-wide perspective.

#### 3a. Vision: the response to cyber attacks minimises the broader impact of data loss on society

When dealing with a major cyber incident, organisations have many things to consider – the technical details of the attack, legal and regulatory requirements, contractual commitments, large unplanned costs and reputation. It is understandable that the focus is on managing and mitigating the harm to the business (and therefore to its customers and other key stakeholders). But this is not necessarily what will minimise the impact on society. For a pro-social response to become best practice, we need to support organisations that prioritise proactive harm reduction over their own short-term challenges.

#### 3b. Vision: fraud teams in business and law enforcement are fully engaged in tackling cyber attacks as precursors to fraud

We need to move to a state where cyber fraud is investigated as one problem. In the current landscape, fraud is typically tackled as if its existence is simply a fact of life. But this attitude leaves stakeholders in the fraud life-cycle with less incentive to reach back down the chain, investigate tactics, understand what information fraudsters are using, and establish ways of limiting it from happening again.

In the UK, the laws used to prosecute those who commit cyber fraud are the 2006 Fraud Act and the 1990 Computer Misuse Act. Neither of these have a specific clause for dealing with cyber fraud and this is a problem seen elsewhere in the world too.

#### 3c. Vision: enforcement is globalised to tackle remote, industrialised, depersonalised and rapidly evolving cyber fraud

We need to shift from the geographically-based policing of fraud to a state where enforcement is built into the transnational technology platforms and payment systems run by the private sector. The current legal, regulatory, ethical and enforcement framework surrounding cyber fraud simply does not work, because the nature of modern fraud is that it is not limited to traditional enforcement geographies. It is remote, industrialised, depersonalised and rapidly evolving.

#### 3d. Vision: cyber and fraud terminology are understood across the relevant stakeholder communities

'Cyber fraud' is a broad term; organisations and specialist professions are using a diverse range of definitions for different parts of the problem. This is a natural result of different perspectives and objectives, but it is ultimately resulting in reduced understanding and is impeding action. We need to make it easier for different stakeholder communities in the fraud life-cycle to understand one another's language.

#### How do we make change happen?

We want to put in place some clear actions to change the cyber to fraud gap. These may include some of the following actions and we are consulting with our members to confirm our approach:

- **Develop a model of 'pro-social response'** for organisations suffering cyber attacks. This should be incentivised by regulators, insurers and the security community
- **Work with investigative journalists** and media organisations to highlight end-to-end case studies that illustrate the cyber fraud lifecycle and ecosystem
- **Develop mechanisms to improve the visibility** that individuals have of their online accounts and information with an indicator of personal cyber fraud risk and ways to reduce this risk
- **Create a common terminology** for cyber fraud – create a simple cross-reference of terminology between cyber security, fraud, financial crime and law enforcement communities. Similar to the MITRE ATT&CK framework, this could be used to check coverage, develop detections, test detections, and more.
- **Support modernisation and harmonisation of cyber fraud legislations** across legal jurisdictions

If you would like to contribute to delivering these changes, please get in touch with us.





## 4. Social Engineering



To tackle cyber fraud we need to address the issue of social engineering

### Why do we need to see change?

The ability of criminals to deceive people is at the heart of both cyber attacks and fraud. Most current effort goes into training people to make near impossible judgements, rather than making their task easier. And sometimes we make it harder for people than it needs to be. For example, we train staff not to click on links or attachments when these are an integral part of business communication. And many consumer organisations communicate with customers in ways that are very hard to differentiate from those of fraudsters. At the same time, social media is making communication between consumers and corporations more public, increasing the potential for cyber-enabled fraud.

#### 4a. **Vision:** opportunities to establish false trust are reduced and those that remain are well publicised and understood

Most people understand not to trust an email or social media notification from a stranger but underestimate how easy it is to impersonate someone online, or even to spoof a phone or text number. While increasing awareness of the risks will help, we will make a bigger difference if we could change the way technology works to reduce the opportunities for false trust. And organisations, which are very focussed on authenticating that a customer or staff member is who they say they are, need to make it easy for individuals to authenticate them.

"There is a proportion of the public that simply thinks 'it will never happen to them,' so they have so far not paid much attention to awareness campaigns."

Phil Chapman, Instructor, Firebrand Training  
The Intelligence Network Corporate Supporter

#### 4b. **Vision:** the way organisations interact with customers and staff reinforces security

We learn what is normal from experience. Organisations can "nudge" how individuals behave through their interactions. We need to stop communicating in ways that unintentionally lead to insecure behaviour, for example reaching out to customers by phone or text and asking the customer to authenticate themselves.

We would like to see a wider understanding of best practice interaction to reinforce security, and a movement away from prioritising ease of communication.

Staff members need to stop being trained to ask customers for personal banking details over the phone, and organisations need to stop prioritising ease of communication over security. We must move to more secure authentication processes, and change current methods of best practise.

"People have an illicit trust in banking institutions, so they do not question interactions and hand over information. This is partly due to how we are neurologically and psychologically designed to build relationships. We need to train people to be less trusting online."

Anon, social engineering expert

#### 4c. **Vision:** the security of interactions with individuals becomes less dependent on widely public information

An increasing number of organisations use social media platforms to interact with their customers in a more public and popular way. However, this has opened up a new gateway for customers and organisations to become vulnerable. We've seen fraudsters exploit this at ease, scouring social media for customer complaints and then spoofing them to extract security details. Some examples<sup>3</sup> have been widely publicised, which may incentivise change over time, but organisations must consider their interactions more closely, and shift to security measures that are less dependent on widely public information.

### How do we make change happen?

We want to put in place some clear actions to help make it harder for fraudsters to exercise social engineering tactics. These may include some of the following actions and we are consulting with our members to confirm our approach:

- **Explore models for providing cyber security and cyber fraud advice services** to the general public
- **Map out the mechanisms by which criminals can establish false trust** and stimulate research and investment into the removal or prevention of these mechanisms
- **Redirect existing awareness campaigns** to improve the understanding of existing mechanisms used to establish false trust (eg phone number spoofing currently)
- **Develop and publish a best practice guide** for how organisations interact with staff, customers and fraud victims to reinforce rather than undermine secure behaviours
- **Establish the principles and mechanisms by which organisations can authenticate themselves to individuals to distinguish them from fraudsters**
- **Establish an alert service** that monitors interactions on social media and flags to organisations behaviour that appears to be fraudulent towards their customers

If you would like to contribute to delivering these changes, please get in touch with us.

## ■ The Journey to Change

Following our research into the problem of cyber fraud, we have established the challenges that we need to overcome if we are to tackle this global issue, and we have established what we want to achieve. This document maps out our vision for a future state. We're now calling for our members to help us get there.

We have some draft actions for exploration, but we need the help of the wider Network to prioritise activities and agree a way forward.

We are committed to this being a truly collaborative process, so we are inviting members of The Intelligence Network to come forward in support of our vision. We are asking members to provide evidence to help us establish priority areas. Based on the response, we will establish working groups to develop actions further, and build a plan to make our vision a reality.



We encourage all members of The Intelligence Network to share ideas and activities on our LinkedIn Group. Join us there to stay up to date, and to find out more about the upcoming working groups, which you can get involved in.

## Share your ideas and join the conversation



Join the conversation on LinkedIn

[www.baesystems.com/intellancenetworkhub](http://www.baesystems.com/intellancenetworkhub)



Email us direct

[theintellancenetwork@baesystems.com](mailto:theintellancenetwork@baesystems.com)



Discover more on our website

<https://content.baesystems.com/theintellancenetwork/us>

## Useful Resources

- Action Fraud: <https://www.actionfraud.police.uk/>
- NFIB: <https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/nfib/Pages/default.aspx>
- Fraud.org: <https://www.fraud.org/>
- The Little Book of Cyber Scams: <https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/fraud/met/little-book-of-cyber-scams-2.0.pdf>
- Federal Trade Commission, OnGuard: <https://www.consumer.ftc.gov/features/feature-0038-onguardonline>
- Cyber Aware: <https://www.cyberaware.gov.uk/>
- Cifas: <https://www.cifas.org.uk/>
- US Government: <https://www.usa.gov/scams-and-frauds>



With thanks to our Steering Committee and Corporate Supporters for their on-going support of The Intelligence Network

Louise Fisk, BAE Systems Applied Intelligence  
James Hatch, BAE Systems Applied Intelligence  
Siân John MBE, Microsoft  
Peder Jungck, BAE Systems Inc.  
Will Lin, Forgepoint Capital  
Jonathan Luff, CyLon  
Roxanne Morison, The CBI  
Christina Richmond, ESG  
James Sullivan, RUSI  
Mark Swift, Trafigura



## References

<sup>1</sup> <https://www.techuk.org/insights/news/item/13518-ons-crime-stats-fraud-cyber-crime-still-dominate>

<sup>2</sup> <https://www.gov.uk/government/collections/secure-by-design>

<sup>3</sup> <https://www.theguardian.com/money/2019/may/26/metro-bank-fraud-phishing-scam-security> and <https://www.bbc.co.uk/news/business-46309561>