CYBEHAVE

GUIDANCE

Title: Social Network Analysis (SNA) in Cybersecurity: A Practical Guide for Behavioural Change

Date: May 30th, 2025

Author: Andy Wood

Abstract:

This guide introduces **Social Network Analysis (SNA)** as a practical tool for security professionals seeking to influence and embed secure behaviours across their organisations. With cybersecurity risks increasingly rooted in human behaviour, understanding informal social structures and influence pathways is essential. SNA enables practitioners to map relationships, identify key influencers, and design data-driven interventions that reflect how information and behaviours actually spread in real-world settings. This comprehensive resource explains the value of SNA at each stage of behavioural change, diagnosing, understanding, designing, and sustaining interventions, and provides a straightforward step-by-step process from data collection to action. Featuring real-life case studies and accessible guidance, the guide equips professionals with no prior SNA experience to confidently apply this method and drive measurable, culturally embedded change.

Introduction

Cybersecurity is as much about people as it is about technology. Human error, habits, and relationships often define the effectiveness of security controls. Social Network Analysis (SNA) is a powerful yet underutilised approach in behavioural cybersecurity that allows practitioners to map, measure, and understand the social structures within an organisation. By understanding how people connect, influence, and share information, security professionals can design more targeted, sustainable, and impactful behavioural interventions.

This guide provides a comprehensive introduction to SNA specifically tailored for cybersecurity behavioural change. It is written for professionals with no prior experience in SNA, featuring a clear structure and step-by-step guidance to help you understand and apply it with confidence. By the end, you should be able to hold an informed conversation about SNA, explain its relevance to cybersecurity culture, and take meaningful steps to apply it in your organisation.

CYBEHAVE

What is Social Network Analysis?

SNA is the study of social structures through networks and graph theory. It visualises and quantifies relationships between individuals (nodes) and their connections (edges). These connections could represent anything from communication frequency to trust, collaboration, or shared knowledge.

Rather than focusing on individual attributes, such as job titles, SNA explores relational data. This helps uncover informal influence, collaboration patterns, and hidden leaders who might not appear in formal hierarchies but play key roles in cultural or behavioural dynamics. SNA can also identify structural holes, information silos, or key bridges that help or hinder the flow of behaviourally relevant information.

When visualised as a graph, SNA allows you to see the shape of your organisation's social fabric - who is connected to whom, how tightly, and where gaps, bottlenecks, or clusters might exist.

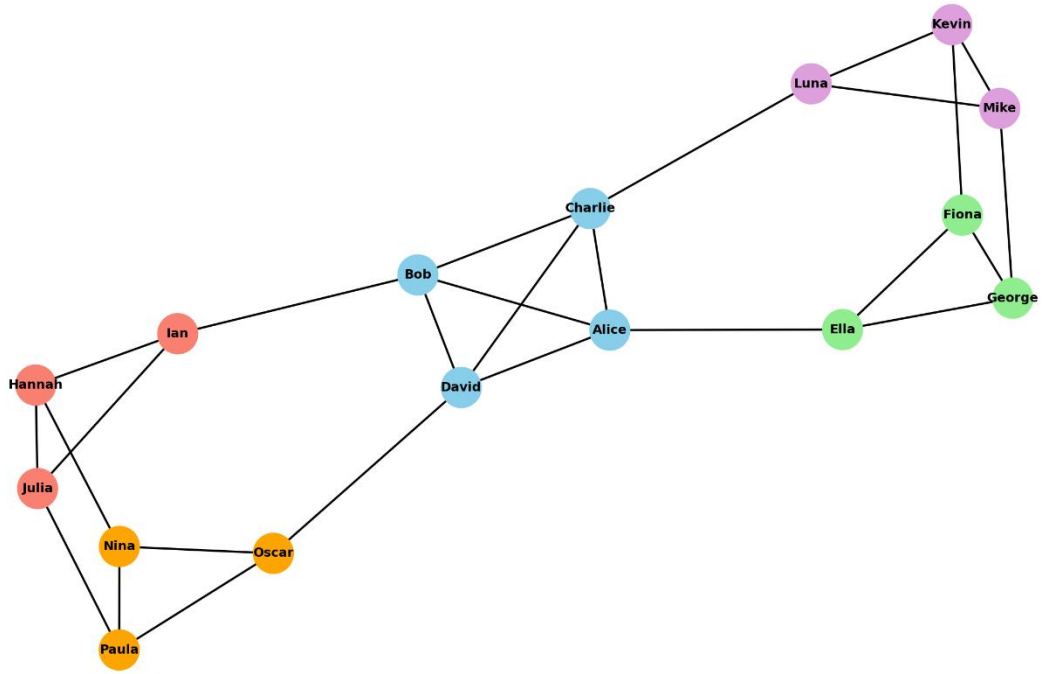

Figure 1: Basic example of an SNA modelled network

CYBEHAVE

Why Use SNA in Cybersecurity?

We often rely on top-down awareness campaigns and training that assume formal roles and structures reflect real-world influence. SNA offers a more accurate picture. It helps answer crucial questions like:

- Who are the informal influencers that others turn to for advice?
- Where are the communication bottlenecks or silos that hinder security awareness?
- How does information about risks or incidents actually flow across the organisation?

SNA is especially valuable in complex or distributed organisations where communication and collaboration extend beyond job roles or team charts. It makes the invisible visible.

By applying SNA, you can move away from one-size-fits-all strategies and toward targeted interventions based on how people actually interact. This is crucial when introducing new behaviours, such as phishing reporting, secure file sharing, or password management.

Furthermore, SNA can help:

- ✓ Identify employees who are ideally placed to act as Security Champions
- ✓ Detect groups at risk of exclusion from security communications
- ✓ Measure the ripple effect of interventions over time
- ✓ Support merger or reorganisation efforts by mapping integration points

When to Use SNA in the Behaviour Change Process

SNA aligns with the broader behavioural change lifecycle and complements other models, such as COM-B and the Behaviour Change Wheel.

1. **Diagnosing:** SNA helps you diagnose how information and influence currently flow within your organisation. This diagnostic step goes beyond attitude surveys and reveals the network's real structural strengths and weaknesses.
2. **Understanding:** SNA allows you to understand why certain behaviours persist and how social norms are maintained. It can surface the influence of informal leaders or cultural brokers, individuals who hold sway over their peers even if they lack formal authority.
3. **Designing Interventions:** Use SNA to identify the most strategically placed individuals for intervention, those who are most connected or most trusted. This means selecting the right people to trial a new behaviour, test a campaign message, or model a secure practice for others.
4. **Supporting Long-Term Change:** Behavioural change is not a one-off event. SNA allows you to track progress over time. By mapping the same network periodically, you can assess whether security norms are becoming embedded, if social silos are dissolving, and whether your Champions remain well-positioned or need support.

Engage. Educate. Empower.

https://CyBehave.org

CYBEHAVE

Step-by-Step: Applying SNA in Cybersecurity Behaviour Change

Step 1: Define Your Purpose: Begin by clearly stating what you want to understand or achieve. For example, are you trying to identify the most influential people in your organisation to promote security behaviours? Or are you looking to understand how security information spreads?

Step 2: Choose the Network Type: Decide what kind of network to analyse. Common types include:

- Communication network: Who regularly talks to whom?
- Trust network: Who do people confide in or rely on for support?
- Advice network: Who do people turn to for guidance on security or work-related matters?
- Collaboration network: Who works together or shares projects?

Your network type will depend on the behaviour you're trying to influence.

Step 3: Collect Network Data: Gather data that reflects real relationships. This could come from:

- Structured surveys asking questions like "Who do you speak to about cybersecurity?"
- Anonymised communication logs (emails, chat platforms)
- Observations or meeting attendance records
- Workflow systems showing shared task ownership

Be transparent about data use, respect privacy laws, and engage your Data Protection Officer or HR team to ensure the ethical use of data.

Step 4: Construct the Network: Transform your data into a graph. Each person becomes a node; their connections become edges. You can use open-source or commercial tools such as:

- Gephi (visual exploration and manipulation)
- NodeXL (Excel-based)
- UCINET (advanced metrics and modelling)
- Python's NetworkX (for programmers)

Visualising the network helps spot patterns that might otherwise be hidden in spreadsheets.

Step 5: Analyse Network Properties: Key metrics to examine include:

- Degree centrality: Who has the most connections?
- Betweenness centrality: Who connects different groups?
- Closeness centrality: Who can access others quickly?

- Eigenvector centrality: Who is connected to other well-connected people?
- Clusters: Which groups interact mostly with each other?
- Bridges: Who links otherwise disconnected groups?

These insights help you determine who to involve, where vulnerabilities exist, and how to spread behavioural change more effectively.

Step 6: Interpret the Insights: Use the metrics to generate actionable insights. Ask questions such as:

- Are our Security Champions positioned in a way that allows them to influence others?
- Are there key people with low cybersecurity awareness but high influence?
- Are specific departments or job levels disconnected from the security conversation?

This stage often benefits from combining SNA insights with qualitative input from interviews or focus groups.

Step 7: Design and Test Behavioural Interventions: Now that you understand the network, tailor your intervention:

- Train central individuals as behaviour role models
- Use peer influence in key communities to promote change
- Deliver targeted communications to under-connected or siloed teams
- Avoid overwhelming the same nodes with multiple responsibilities

Pilot your intervention in one part of the network and observe how it spreads. This agile approach allows you to adapt quickly.

Step 8: Monitor and Adjust: After implementation, re-map the network. Look for:

- Increased connectivity between previously disconnected groups
- Changes in the centrality of key influencers
- Higher security engagement among previously disengaged staff

Compare SNA results over time to demonstrate behavioural change and cultural shifts in a compelling visual format.

Real-World Examples of CFIR in Action

Example 1: Identifying the Right Security Champions

A large financial services firm used SNA to identify informal influencers across its departments. These individuals were not managers but had high betweenness centrality, acting as bridges

between teams. By training them as Security Champions, the firm achieved higher engagement and faster spread of cyber awareness practices than in previous top-down campaigns.

Example 2: Breaking Down Silos in a Multinational Corporation

A global tech company faced issues with siloed security practices across regions. SNA revealed that certain regions had almost no cross-border communication about threats. The organisation created cross-functional champion clusters and introduced regular virtual exchanges. Over the course of six months, follow-up SNA showed increased inter-regional connectivity and consistency in secure behaviour reporting.

Example 3: Measuring the Spread of a Phishing Simulation Campaign

After launching a phishing simulation, a public sector agency mapped internal communications to see how quickly knowledge of the campaign spread. SNA revealed that some departments discussed the event widely, reinforcing learning, while others remained unaware. The agency used these findings to deploy follow-up sessions led by well-connected individuals.

Conclusion

SNA is more than a visualisation tool; it is a strategic enabler for behavioural change. It empowers security professionals to understand the informal dynamics that shape secure behaviour, design more innovative interventions, and build sustainable cultural change.

You don’t need to be a data scientist to start using SNA. Begin with a clear purpose, a simple survey, and free tools like Gephi or NodeXL. Engage your organisation’s network of people as intentionally as you would its network of devices. With a solid grasp of SNA, you’ll be better equipped to target your efforts, amplify your message, and create a truly resilient organisation where secure behaviours are shared, supported, and sustained across the network.