ORGANISATIONAL RISK

Amy Hodler *outlines suggestions on how your security team can calculate exposure and protect against cyber attacks*

When we look at reining in and limiting nefarious activity on organisational networks, it helps to think like a criminal. Criminals look for vulnerabilities. They think in 'graphs,' while the organisations they target usually think in lists, combating crime through elimination. Graphs are a way of representing reality in terms of nodes and the connections or relationships between them. Cybercriminals are looking for undetected relationships to exploit. It is these weaknesses that are inherent vulnerabilities. They are the multiple small connections that criminals seek to circumvent an organisation's security measures.

Technology systems are built to withhold attacks, but many entry points exploit systemic vulnerabilities in an increasingly connected world. They are accessing a hole in the HR system to get to the financial accounts, for example.

Graph databases map out the flows between assets needing protection and the vulnerabilities between them. Graph technology is unique in this relationship-centered approach. And it has reached a point of maturity where we can run off-the-shelf algorithms over a network. These algorithms locate connections that pinpoint your system's vulnerabilities. This lets you take corrective actions to shore up systems.

A pathfinding algorithm essentially finds the shortest path in a network. Security teams can use the algorithm to discover how it links to the largest potential vulnerability and close the door on it. Pathfinding can locate the central system that accesses the majority of the systems in the same network. This could be a system that allows access to important information, but isn't adequately protected. HR systems that connect to your IP storehouse, for example.

Graph technology is being deployed to help fight system breaches in the energy sector, for instance. The recent ransomware takedowns of US East Coast power grids exemplify how this technology works. By identifying vulnerabilities, a customer was able to make its system less connected. Graph thinking has minimised exposure to cyber hacks and possible negative impacts on other components in the system.

Graph technology detects and analyses system irregularities in real-time, based on patterns in the network. It could be an IT network where you know the regular patterns flow in a hub and spoke fashion. An unusual pattern could be when edge devices, such as IoT devices in a telecoms configuration, try to connect or an outside area. This kind of irregularity suggests possible interference by cybercriminals. Cybersecurity teams can set a threshold based on abnormal system behaviour. A breach of this threshold triggers an alarm for intervention or isolation of the suspect part of the system.

A helpful way to employ graph technology is to make predictions to prevent future problems. It is possible to identify previous patterns where cybersecurity was potentially under threat. These seemingly innocuous patterns could easily have been cyber attacks. Taking these patterns and running them in a graph database allows for prediction and comparison with other patterns. You can create models of prior attacks using machine learning to which new data is added. Comparisons can be drawn to determine where weaknesses lie to guard against future attacks.

These comparisons are helpful for AML (anti-money laundering) and anti-fraud work. In AML, an analysis of a customer activity dataset using graph-based machine learning will reveal fraudulent and non-fraudulent behaviour. Another area to explore is personalised PageRank, which examines the influence in a network. Influence refers to people or a type of business, and personalising PageRank focuses on a particular element. An excellent example of this is a financial network where you want to gauge the influence on business-to-business (B2B) transactions. A personalised PageRank algorithm allows the individual to be alerted when regular patterns, appropriate for a specific device, deviate from the norm. An acceptable level of risk is paramount in all situations, so some flexibility is essential. Business continuity is key. You must avoid closing off all access and harming the business.

Financial services companies offer a case in point when dealing with fraud. Credit applications, which could appear fraudulent, risk being rejected across the board. But, you don't want to lock out customers, partners or suppliers completely and alienate them. Find instead a reasonable level of risk tolerance.

Graph technology helps accurately assess the risk and cybersecurity threats your enterprise faces. It shows you where you need to add in defences and how much you need to invest to be adequately protected. In the battle for more robust cybersecurity, you need to know your enemy and exactly how they operate. When you understand this, you'll be able to outsmart them ●

Graph databases map out the flows between assets needing protection and the vulnerabilities between them

Amy Hodler heads up content and evangelism for graph databases, network science & their use in analytics and data science at graph database company Neo4j. She is also co-author of Graph Algorithms: Practical Examples in Apache Spark & Neo4j, published by O'Reilly Media.