IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

The Four Keys to Improving Network Visibility

Alastair Hartrup

Alastair Hartrup
Founder and
Global CEO
Network Critical

Biography

Alastair Hartrup is the Founder and Global CEO of network security experts, Network Critical (https://www.networkcritical.com).

Founded in 1997, Network Critical has been providing high-quality Network TAPs and Network Packet Brokers.

CEO and founder Alastair Hartrup has been at the helm since its foundation and under his leadership the company has grown from zero to a global multinational business.

Alastair blogs at https://www.networkcritical.com/blog

Keywords Network, Visibility, Traffic, Political, Financial, Technical, Legal
Paper type Research

Abstract

There are many questions that organisations ask themselves when looking at network visibility. These include questions like, what is a visibility strategy, and when should organisations start developing a visibility strategy? In this article, it is the author's opinion that there are four key components in a visibility strategy and these are technical, financial, political and legal. Developing sound practices around these key dimensions is not only the purview of IT staff, it is a strategic imperative that requires attention and commitment throughout the organisation.

Introduction – So, what is network visibility?

First, let us look at what we mean when we talk about network visibility. Network visibility is enabling network administrators to capture and see network traffic and applications that are traveling across Wide Area and Local Area network links. Once captured, traffic can be mapped to various tools for analytics, performance enhancement and security. There are many specialised tools to perform these functions that all must be connected to network links to provide traffic data to tools.

The four key dimensions mentioned above work in tandem to deliver better network visibility as follows:

1. **Technical dimension**
   Network design, management, monitoring, performance and security are highly technical, and all sit squarely in the Information Technology group. Determining what visibility platform is utilised and what tools are needed requires deep technical expertise. However, what is often not solicited, is input from other departments in the organisation. The scope, scale and


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

functionality of this strategy will impact the entire organisation – not just the various controlling IT functions – and broader input is required.

2. Financial dimension

It is easy to rationalise a small budget for visibility. Many organisations feel comfortable putting minimal architecture in place; architecture that provides some intrusion protection and allows the network manager to analyse network traffic when needed. As long as no one complains, why complicate things? The simple answer is that being prepared and protected for advanced threats is less expensive than trying to repair the damage after an attack or breach.

No one pays much attention to IT when everything works, but we all notice when things go wrong:

- Being hit by a malicious attack that cripples the infrastructure can shut down a business. When the Amazon website crashed, it cost the company $1,000,000 per minute of downtime.

- According to Bloomberg News[1], the 2017 Equifax breach affected as many as 147.9 million consumers. The New York Times reported that this breach cost the company over $87.9 million in expenses and the company lost $3.5 billion in market capitalisation.

These are extreme examples, but it is easy to see that investing time, effort and money in a robust visibility strategy and strong defence can actually demonstrate a great return on investment. The problem is that spending on defence prior to an attack can be hard to justify. The news, however, is full of companies like Amazon and Equifax that help quantify the potential return from full visibility and strong defence strategy.

3. Political dimension

Organisational politics vary widely from company to company. Generally, smaller organisations have managers performing a broad scope of duties. Larger organisations, by contrast, have what are typically called ‘functional silos’. In large networks, for example, switches might be managed by a different group than that responsible for security. Another group manages infrastructure, another for applications, another for operating systems and so on.

When developing a visibility strategy, there may be many stakeholders involved in just the IT portion of the plan but who pays for what and where does the responsibility lie when things go wrong?

This is not to say that multiple silos cannot work together as a team. Using an independent TAP as the foundation of the visibility strategy simplifies management across demarcation lines. The TAPs touch the switch and they also touch the connected tools. This allows each functional silo to manage its own purview without impinging on or impacting other groups. It becomes simple to pass budget and responsibility according to function.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

Another political component of 4D visibility strategy is managing non-IT organisations. The entire organisation is impacted by the success or failure of the network. As demonstrated in the examples above, managing and protecting the network goes well beyond the IT department. When things go wrong, the pain is felt throughout the organisation. All users of the network have a responsibility to safely manage their access to corporate network resources. Network usage training for Non-IT personnel is helpful but not fool proof. The physical protection against malicious attacks on all fronts must be in place in addition to continual training throughout the organisation.

4. Legal dimension

IT managers are required to adhere to a wide variety of new laws and regulations that are related to network security, access to information and protection of personal privacy. Regulations such as GDPR and others require various protections for network users both inside and outside the organisation. Stiff penalties and fines can be levied for non-compliance. The other component of protecting the legal dimension is liability. Beyond regulatory compliance, unauthorised distribution and malicious use of information that is entrusted to the organisation by a user can create a very expensive liability. People entrust very personal information to organisations through websites every day – social security numbers, credit card and bank account numbers – and when this information finds its way into the wrong hands, it can be devastating to the individual both personally and financially.

Organisations that do not adequately protect that private data can be vulnerable to large financial penalties. Associated costs after an attack may be only a small part of a much greater cost. There can be fines from regulatory bodies, legal costs, and potentially, large punitive awards to third parties damaged by the unauthorised release of their personal information. Returning to normal operations after an attack can be very expensive, time consuming and painful.

In conclusion

Visibility is the foundational piece to a larger strategy of network and organisational protection against security threats. Good visibility strategy is critical to day-to-day analytics and management for efficient operation of the network. While there are many specialised tools required to understand and protect network traffic, they must be deployed efficiently with the proper foundation.

Network management touches all parts of the organisation and beyond. Often, the reach is global. Liability, therefore, can also extend beyond international boundaries. Addressing technical, financial, political and legal dimensions in the early planning stages allows organisations to efficiently build and manage a robust network infrastructure with strong defences.

Reference

[1] https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros