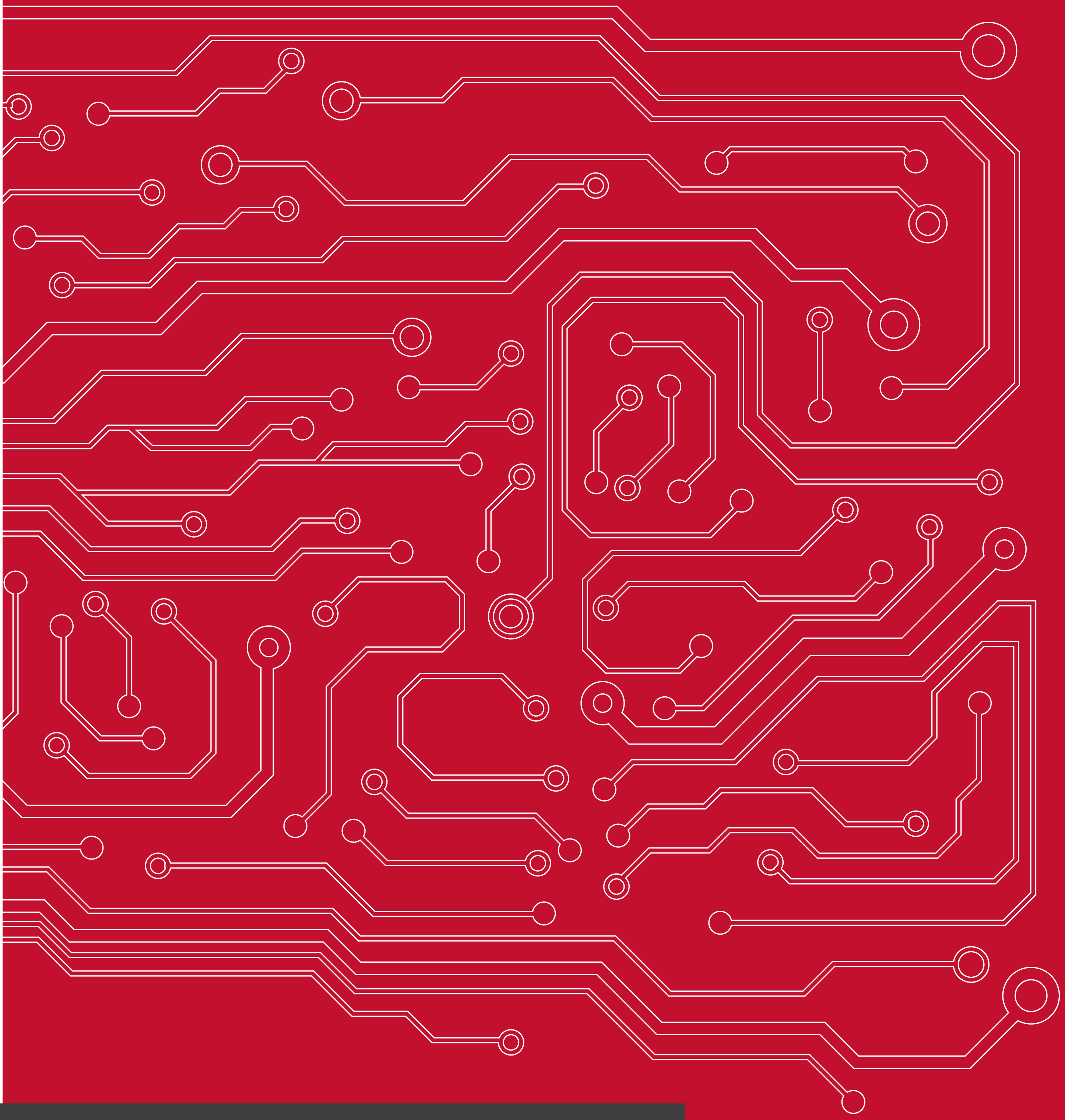
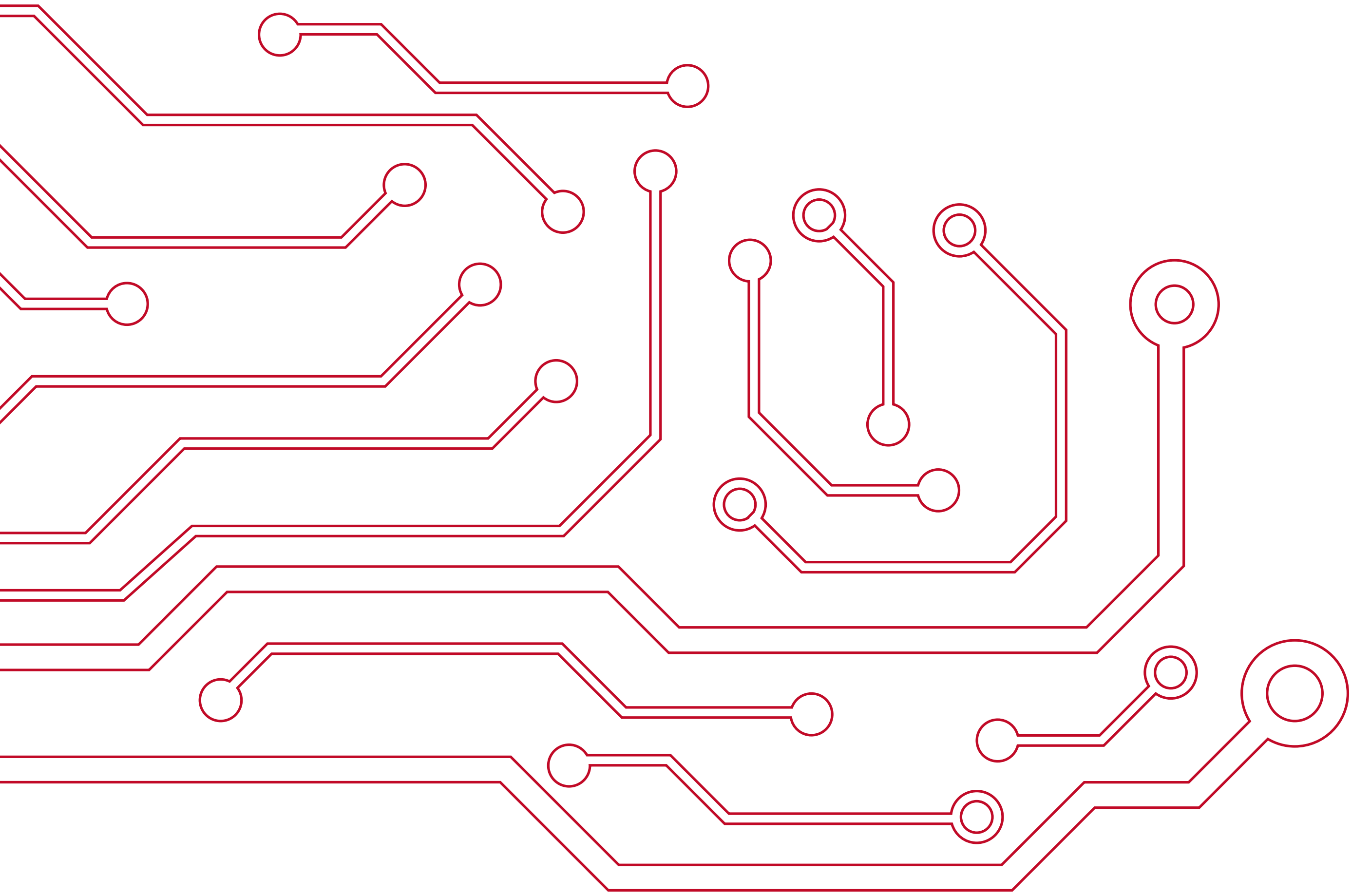


Private sector cyber resilience and the role of data diodes

An NCC Group Publication

Contents

Modern Cyber Resilience Expectations



Governments and businesses recognise that absolute cyber security is neither possible nor practical. In the public sector the risks are in part addressed by the adoption of various compensating controls that align with various protective marking schemes. The nations which have adopted these controls have also developed resilience strategies, in some cases for nearly a decade [1] [2] [3] [4] [5], both at a national, and increasingly a local government level [6], to help outline expectations of the public and private sector outside of these protective marking schemes.

resilience

noun

The quality or fact of being able to recover quickly or easily from, or resist being affected by, a misfortune, shock, illness, etc.; robustness; adaptability.

Oxford English Dictionary

More recently we have seen regulators [7] [8] [9], predominantly in financial services, also recognise that cyber security is not a binary state of being secure or insecure, but rather that incidents will happen, that they will be both internal and external in origin, and that some will be accidental and others malicious. Given how critical these organisations and their services are to the stability and competitiveness of nations, making them resilient to cyber threats is the only realistic way to address the problem.

So what are the modern expectations of resilience? Broadly speaking, they are that an organisation will have credible blended countermeasures designed to stop attacks from occurring, and that when attacks aren't stopped, the impact on the organisation, its operations and its customers is minimised, while the organisation remains competitive (and in the case of private-sector organisations profitable).

Benefits of Air Gaps in Network Security Resilience

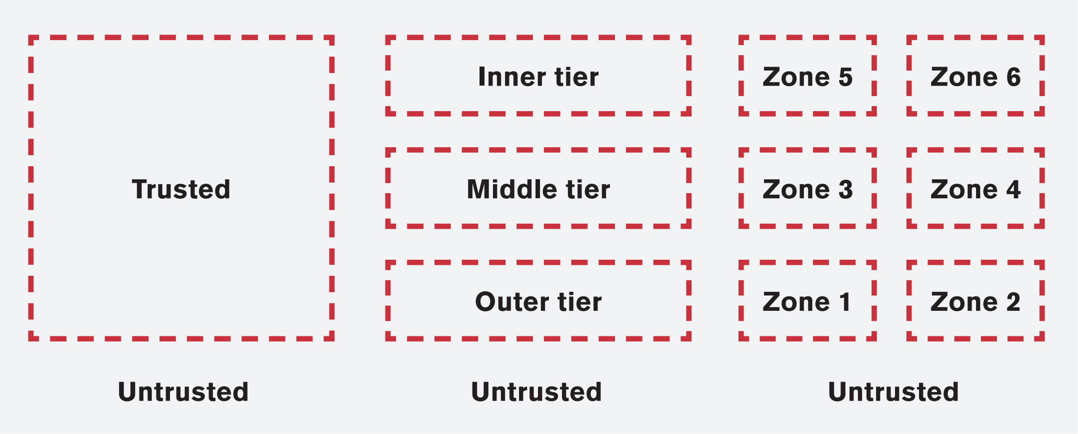
Benefits of Air Gaps Overruled by Practicality

It has long been received wisdom that the way to ensure that a network can't be compromised remotely is to isolate it using an air gap. However, in today's world, an isolated network is rarely practical given the need for flows between producers and consumers. While these islands might be secure, they are simply not practical given modern demands.

Even for organisations with islands, practical requirements mean data is often transferred between networks using hard to control media such as USB sticks or DVDs. Such media is not without risks, e.g. data leaking out on USB sticks or malware infiltration such as Stuxnet. The benefits of data diodes are that they facilitate network protective monitoring while also providing required segregation.

Wall-Gardened, Zoned, and N-Tier Network Security Design Patterns

To address today's need for connectivity, agility, flexibility and cost-effectiveness, many organisations now use a hybrid of non-cloud and cloud network estates that span across geographically disperse premises or facilities. The connections between these networks are typically secured using wall-gardened, zoned, or n-tier network security design patterns, in order to balance the needs for connectivity and security.

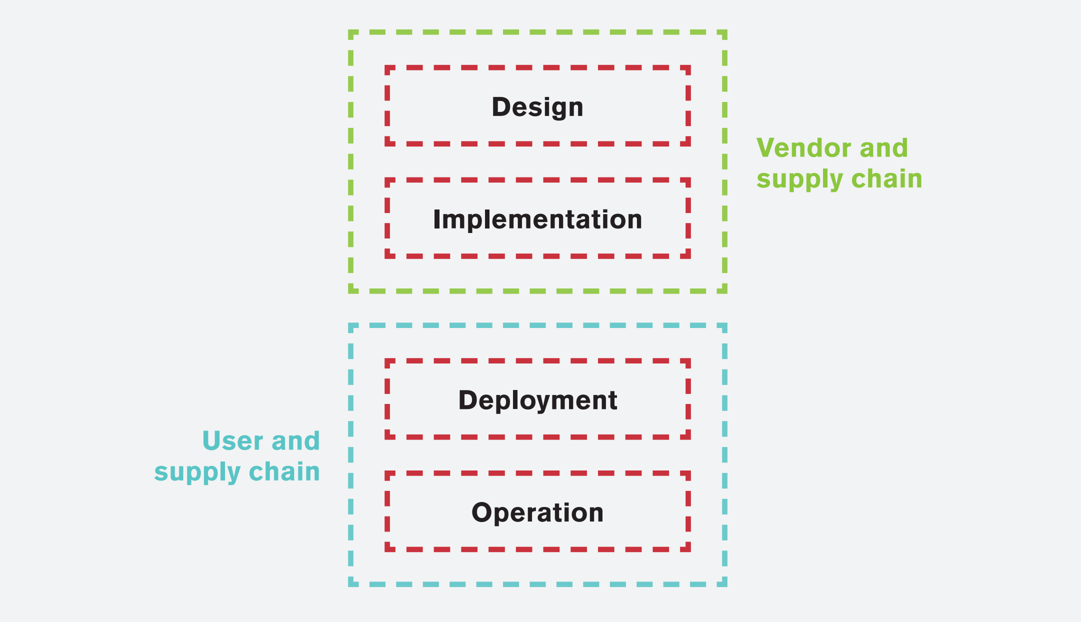


The perimeters between these networks are often implemented using a mixture of logical and physical separation, and a variety of networking and security technologies, all of which are designed to restrict, filter, log, audit, assess or otherwise monitor traffic flowing between networks, devices, and their users of varying trust levels.

The increasing importance and demands placed on these network perimeters is such that the associated complexity of the hardware and software stacks that implement them is also increasing. This increasing complexity is at times a source of vulnerability and weaknesses, due to the challenges of implementing software in a secure fashion, free from logical and code-level security-impacting bugs.

Security Boundary Implementation Complexities

Various factors can undermine the effectiveness of any security boundary. The overriding factor is complexity. The complicating factors for a network boundary can be summarised as follows:



Examples of this complexity and fragility on the vendor side once again became as it has already happened evident in late 2015 and early 2016 when Juniper [10], Fortinet [11] and Cisco [12] all disclosed vulnerabilities that significantly undermined the security of their solutions due to issues arising in implementation.

The above examples, of which there are more, demonstrate the fragility of Firewalls and VPN implementations as edge security devices. Thus in situations where security between security zones needs to be assured, the lack of verified security separation may not be sufficient, resulting in the need for most robust solutions.

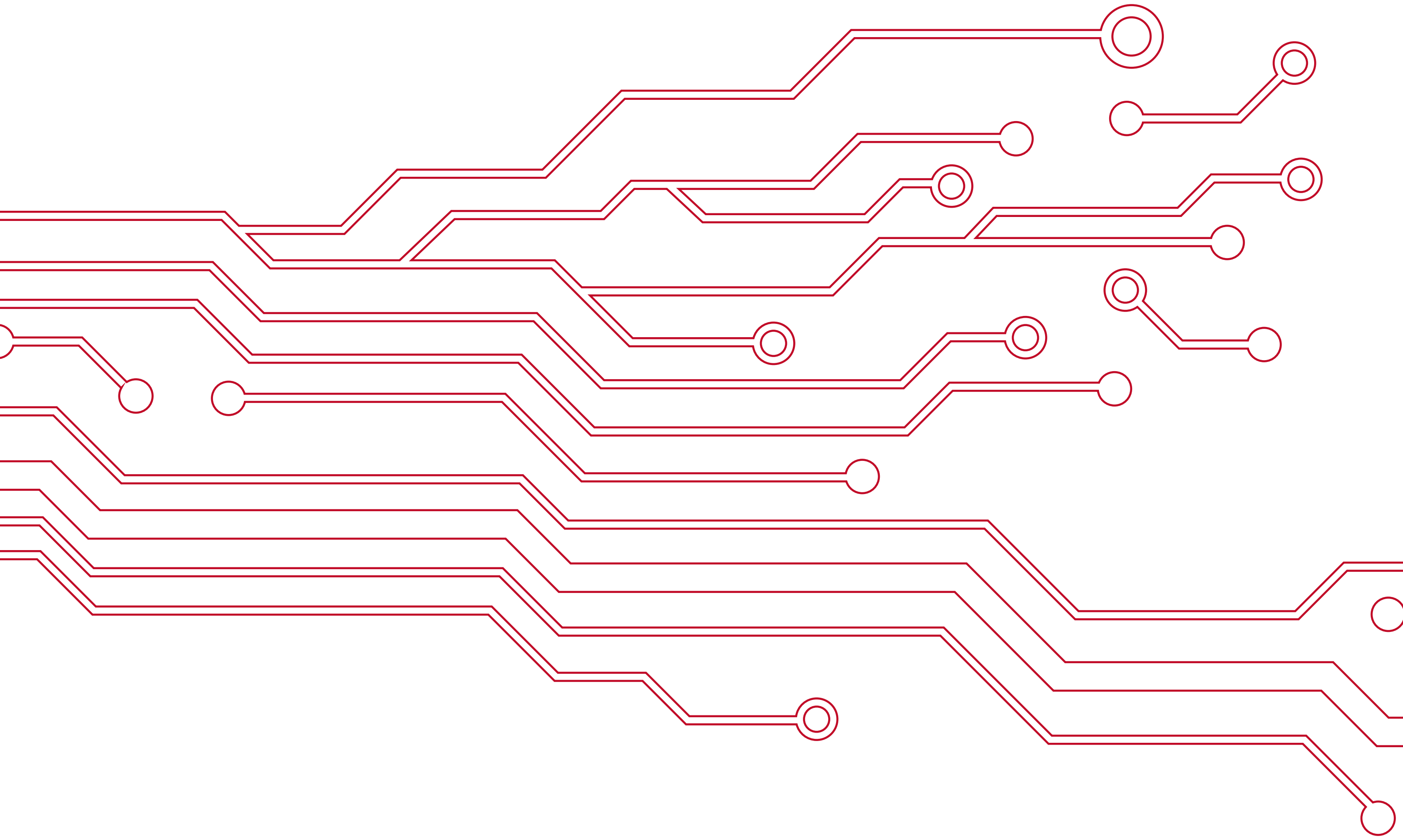
Protecting Secrets and Protecting Assets

The two main scenarios for data diodes are Protecting Secrets and Protecting Assets. While similar in their application, their goals are typically radically different:

- **Protecting Secrets:** Protecting government classified data, as well as private sector intellectual property from unauthorised access such as in pharmaceutical, financial services or other high cost R&D sectors.
- **Protecting Assets:** Protecting electronic assets from cyber attack by way of the network e.g. national power generation and distribution, other core utilities such as water, oil production or blast furnaces.

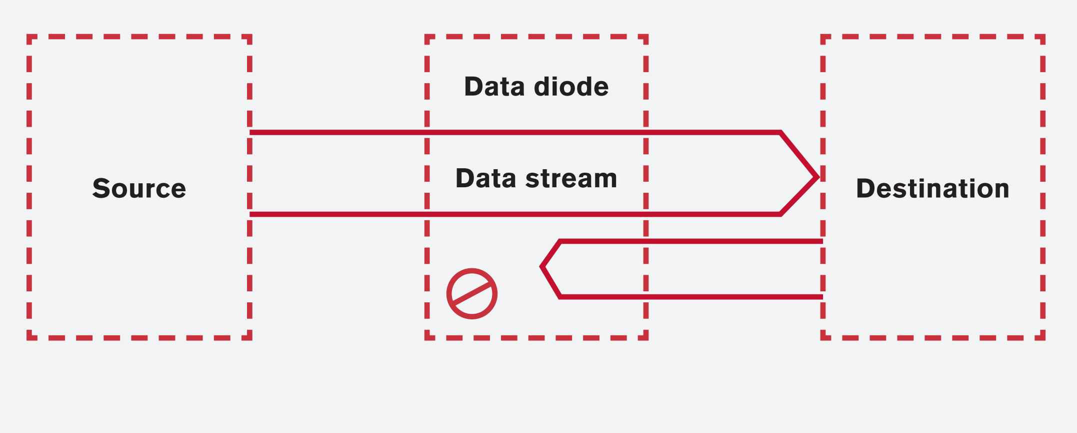
A single data diode could be used to support either or both of these risk resilience goals.

A Brief Introduction to Data Diodes



Data diodes [14] as a concept are extremely simple. Where there exists a need for data to travel from a source to destination, but there is a corresponding need to ensure that a return data path does not exist, then a data diode provides the required assurance.

The data diode provides this assurance through removal of the physical data path between the two networks, physically separating them. This removal is achieved by having a transmission path between the source and destination without the corresponding reception path.



The sophistication in data diode solutions comes from enabling compatibility with existing network protocols, allowing organisations to gain the benefits without substantive changes to their existing systems.

It is also important to understand that not all data diodes are created equal. Various technologies may be used to implement the one-way link, including both software and hardware. The key difference is the level of assurance that is possible: where software is susceptible to vulnerabilities and misconfigurations due to its complexity, a hardware solution can be made much simpler and therefore easier to trust.

These differing levels of assurance are typically reflected in the levels of certification achieved by different products. Using common criteria EAL7 [15] is the highest means of independent level of certification possible. An EAL7 certification covers the design, implementation and supply chain security of the certified product, and represents an extremely high level of confidence in the product.

Using Data Diodes to Address Cyber Security Resilience Challenges

The benefits of data diodes in high-assurance environments have been long understood by governments. Other organisations which are not in high-assurance environments have benefited when they have extended physical estates that need connectivity yet don't always maintain full physical control, such as CCTV. In the private sector the largest adoption of data diodes in NCC Group's experience to date has been seen in industrial control systems (ICS/SCADA) where there has been an increasing need to have telemetry sent from the operational technology (OT) domain to the Internet-connected information technology (IT) domain. In environments such as ICS it is often an imperative, due to the risk of physical damage, that a compromise of the IT domain should not be able to impact the OT domain; hence the employment of data diodes.

Going beyond these environments, data diodes can also help reduce risk in a variety of other commercial scenarios which we cover in the follow sections.

Ensuring Compliance

One of the key business drivers we currently see for data diodes within the Critical National Infrastructure (CNI) sector is compliance. In the USA it is mandatory for CNI to physically segregate certain networks, hence the adoption of data diodes over the last couple of years. NCC Group expects similar requirements will be in place in large parts of the Middle East where there is increasing calls for segregation of OT and IT networks from January 2017 onwards. In Europe, the use of data diodes within the CNI is not prescribed but perceived as the best practice to segregate networks by organisations such as ANSSI, the French Network and Information Security Agency.

Securing Protective Network Monitoring Capabilities

Organisations building protective monitoring often have passive or active collection points across many security domains or large physical estates. These systems can include monitoring, either physical (for example CCTV) or digital (for example network monitoring). Organisations increasingly want separation between the data collection and any centralised aggregated monitoring or security incident event management platforms, due to the complexity of the software in these sensors or variations in physical security afforded.

By employing data diodes in these situations, organisations can gain confidence that data flows from their various data collection points are truly one-way. The benefit of these guaranteed one-way data flows is that should a particular sensor node be compromised either physically or electronically, they might be able to communicate to the centralised system but would not be able to communicate back out to the point of compromise.

An additional benefit is the improved efficiency that's possible by using a single monitoring centre to monitor sources at many different security levels, i.e. both CCTV infrastructure mounted out doors and network sensors monitoring the inner core of the network. Without the use of a data diode, this consolidation would introduce potentially unacceptable risks such as an attacker using access to a camera to gain entrance into the most sensitive parts of the organisation.

Protecting System Integrity of Regulatory Compliance Systems

Compliance regimes around the globe require the integrity of certain back-office and oversight systems. These systems, for example voice or transaction recording, are expected to be working at all times so any regulatory matters can be investigated and complied with in confidence.

As the understanding of threats and vulnerabilities improves, the degree of risk to the integrity of these systems, and their susceptibility to attack, has similarly increased.

In order to address regulatory requirements while minimising risk and total cost of ownership, data diodes can be placed between the source of the voice or transaction data and the recording systems.

In adopting such architectures, organisations and regulators can be confident that the data in the silos is not susceptible to external tampering other than from approved means of access. Along with this confidence comes a lower total cost of ownership due to the strong segregation present.

Providing Business Continuity via Resilient Systems

With the advent of cyber attacks, traditional means of business continuity have been challenged. Historically systems, including the entire software and hardware stack, have been duplicated between live and backup systems, and data has been replicated.

In most systems this entire duplication, coupled with connectivity, creates exposure to a motivated and capable attacker. If a vulnerability should exist in the primary system then the likelihood is that it also exists in the secondary system, along with the means of connectivity to exploit it.

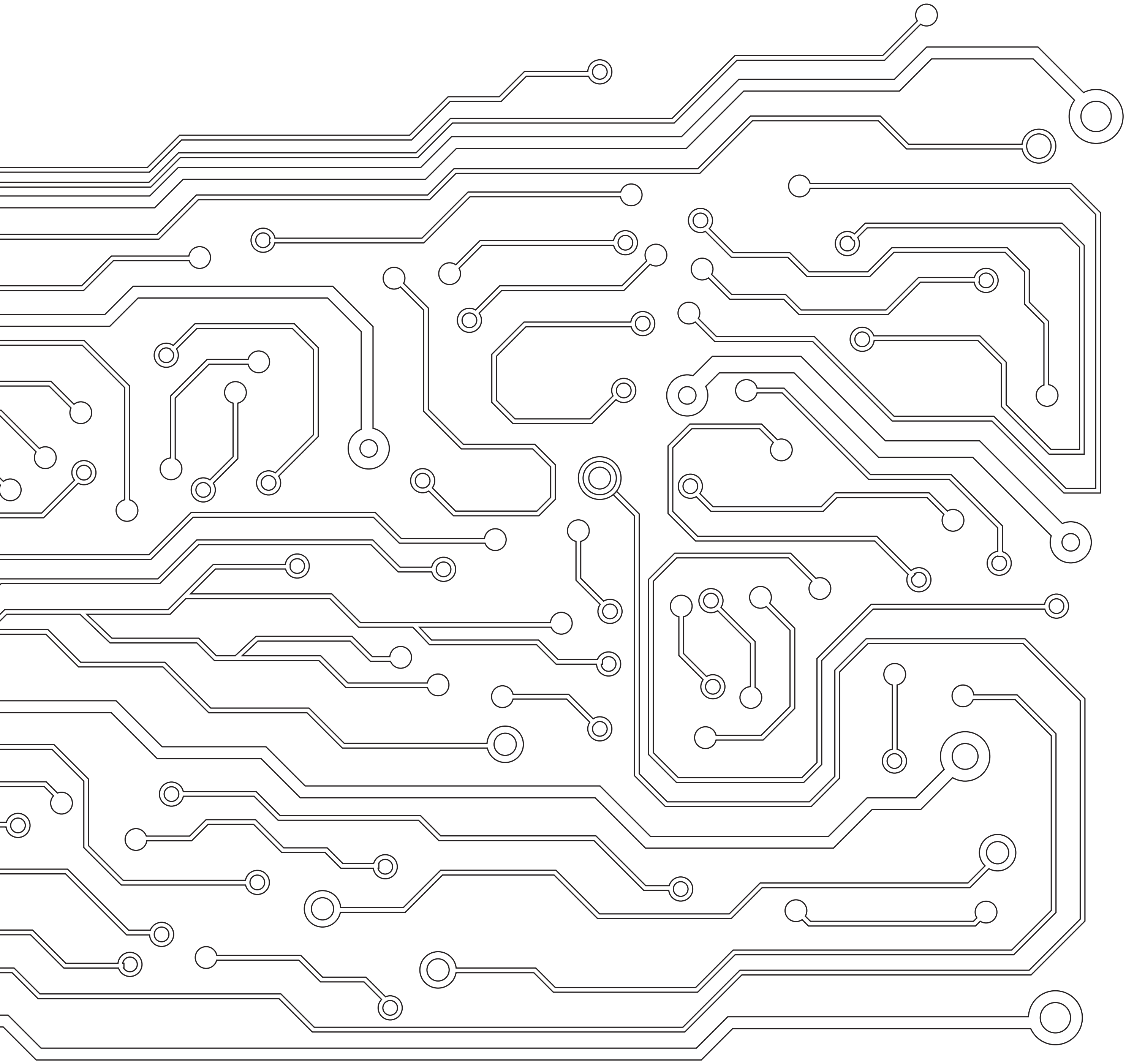
One way to greatly reduce the likelihood of secondary systems succumbing is to provide a one-way data path, so while data can be replicated from the primary to the secondary the opportunity for attack is greatly reduced. During an event, organisations can evaluate the root cause before potentially exposing secondary systems to a similar attack.

Even in environments where two-way communications is required the use of data diodes adds significant value in reducing risk over traditional approaches. In these situations data diodes can be employed create independent paths, one for ingress and one for egress.

While on the face of it this design pattern may seem counter intuitive, separate ingress and egress routes have a reduced attack surface while providing defined points at which protective monitoring can be performed with strict expected behaviour and function.

It is also important to note that if this design pattern is to be used it needs to be used in combination with strong filtering and content checking solutions allowing a certain protocol or file type to go in (e.g. PDF) and only SMTP traffic to go out.

Summary and Conclusions

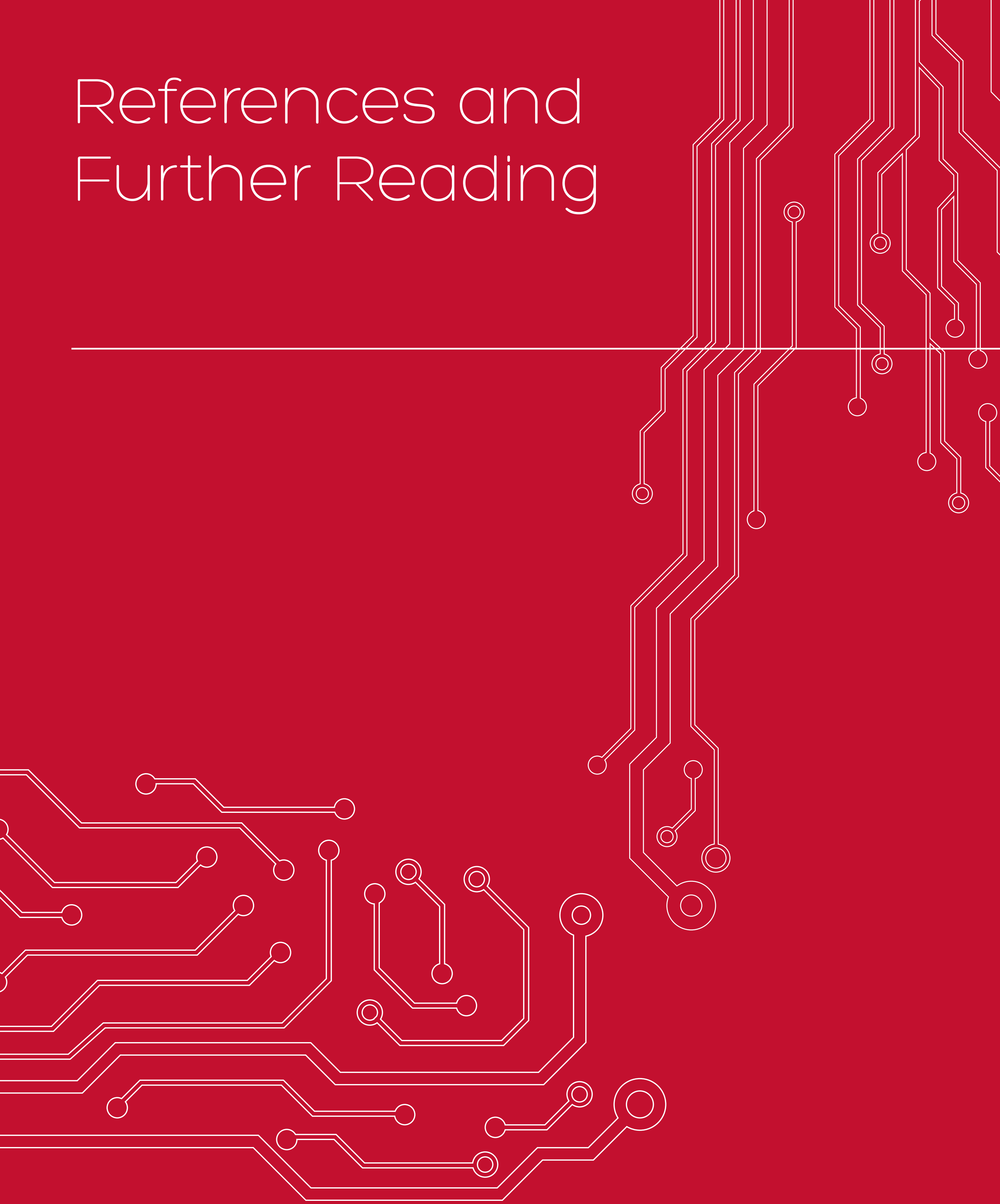


Industry recognises that creating an impenetrable environment is neither cost-effective nor good business sense. Instead, the prevailing wisdom is that the goal should be to create environments which are resilient to cyber events, allowing us to quickly, effectively and confidently recover. Data diodes are one of the most powerful yet underused methods of balancing risk, vulnerability and the businesses need for connectivity. In this paper we have touched on how organisations can safely facilitate connectivity between environments that would have historically been seen as high risk.

We have also discussed various scenarios in which data diodes can reduce total cost ownership due to the robust separation they provide, while allowing organisations to benefit from connectivity.

While governments have long understood the value of data diodes between high and low classifications, their adoption in the commercial sector is today reserved primarily to a limited subset of safety-critical systems. As businesses need to create highly-connected yet secure and integral environments, we can only expect the use of data diodes to grow.

References and Further Reading



1. **Cyber Resilience Review, Department of Homeland Security, United States Government**
   https://en.wikipedia.org/wiki/Cyber_Resilience_Review

2. **Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space**
   https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf

3. **Safe, Secure and Prosperous:**
   A Cyber Resilience Strategy for Scotland, Scottish Government, November 2015
   http://www.gov.scot/Publications/2015/11/2023/3

4. **National Cyber Security Masterplan 2018, Info-communications Development Authority, Singapore, 2013**
   https://www.ida.gov.sg/Programmes-Partnership/Store/National-Cyber-Security-Masterplan-2018

5. **ENISA and Cyber Security Strategies**
   https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss

6. **Understanding Local Cyber Resilience, Department for Communities and Local Government, March 2015**
   https://www.gov.uk/government/publications/understanding-local-cyber-resilience-a-guide-for-local-government-on-cyber-threats

7. **Financial Stability Repot 37: Cyber Risk, Bank of England, July 2015**
   http://www.bankofengland.co.uk/publications/Documents/fsr/2015/fsr37sec6.pdf

8. **Cyber Resilience Capabilities Questionnaire, Prudential Regulation Authority, August 2015**
   http://www.bankofengland.co.uk/pra/documents/about/insuranceletter100815.pdf

9. **Committee on Payments and Market Infrastructures,**
   Cyber resilience in financial market infrastructures, November 2014
   http://www.bis.org/cpmi/publ/d122.pdf

10. **2015-12 Out of Cycle Security Bulletin: ScreenOS: Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756)**
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST

11. **Multiple Products SSH Undocumented Login Vulnerability**
    http://www.fortiguard.com/advisory/multiple-products-ssh-undocumented-login-vulnerability

12. **Cisco ASA Software IKEv1 and IKEv2 Buffer Overflow Vulnerability**
    https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-asa-ike

13. **Centre for Internet Critical Security Controls**
    http://www.cisecurity.org/critical-controls.cfm

14. **NCC Group (Fox-IT) Data Diode Product Website**
    https://www.fox-it.com/datadiode/

15. **NCC Group (Fox-IT) EAL7 Data Diode Certification**
    https://www.fox-it.com/en/files/2012/08/eal7.pdf

nccgroup

freedom from doubt

For more information please contact:

+44 (0) 161 209 5324 response@nccgroup.trust www.nccgroup.trust