quocirca

Network modelling for IT compliance

Regulatory compliance through dynamic network modelling

To be confident that its activities are compliant with all required regulations, an organisation requires a constantly updated view of its use of information technology. Dynamic network modelling is the answer.

GDPR currently dominates the compliance agenda for EU-based organisations. However, they must also consider many other regulations passed down by national governments, industry bodies and other entities.

Taking a separate approach to complying with each one is laborious and leads to inconsistencies. Dynamic network modelling can provide the insight to ensure the use of information technology is, and remains, compliant with all relevant regulations.

Report Authors

Bob Tarzey Analyst and Director, Quocirca
Tel: +44 7900 275517
Email: bob.tarzey@quocirca.com

Bernt Østergaard Senior Analyst, Quocirca
Tel: +45 45 50 51 83
Email: bernt.ostergaard@quocirca.com

COMMISSIONED BY
REDSEAL

Introduction:
Network modelling to provide IT infrastructure insight

It is hard to understand a complex system and how it might be impacted by changes through looking at the system itself. For example, it is risky for planners to make experimental changes to the signalling on a city's actual road system in case traffic grinds to a halt. Instead, computer models are built of complex systems to provide visibility into how they work and the impact that changes might have.

Information technology (IT) networks are just such complex systems. A large organisation's network may consist of tens of thousands of physical and virtual devices, getting more complex as the network extends into new areas. These include the remote IT infrastructure of public cloud service providers, as the use of their services increases, and other elements of physical infrastructure, such as vehicle fleets, pipelines and buildings, which are being digitised for monitoring and management through Internet of Things (IoT) deployments. Furthermore, the decision about what is deployed is increasingly being made outside of IT departments with the increase in so-called shadow IT, whereby lines-of-business and individuals make their own additions to networks.

All this means that the need to model IT networks has become ever more necessary and the models themselves, just like the real networks, have become more complex. A comprehensive, dynamic and regularly maintained model enables even the largest networks to be visualised and tested on a day-to-day basis. Some of the tools that build and maintain such models allow quantification of the networks, providing scores for resilience and security and ensuring the integrity of given network segments is understood. Imagine being able to continuously assess the integrity and resilience of the IT infrastructure that underpins a given business process.

Network models can identify areas of networks that have become insecure through unauthorised changes elsewhere. Fixing vulnerabilities can be prioritised based on both their severity and network context. Access rights can be checked and privileges limited, helping to mitigate the rising tide of cybercrime. Planned changes can be tested before actual deployments; for example, checking if a new router, deployed to handle increased traffic to a cloud service provider, impacts performance and/or security elsewhere. This helps ensure that new IT investments deliver on expectations.

The tools that build and support network models automate many tasks which would otherwise drain manpower. Automated tools do not miss minor configuration errors and policy mistakes which might be overlooked by tired, less efficient human operators. IT managers, freed from mundane details, can operate at a higher level focussing on new digital initiatives and the overall user experience. In short, a network model can measure and improve an organisation's overall digital resilience (the ability of IT infrastructure to withstand a range of threats and continue to provide on-going services).

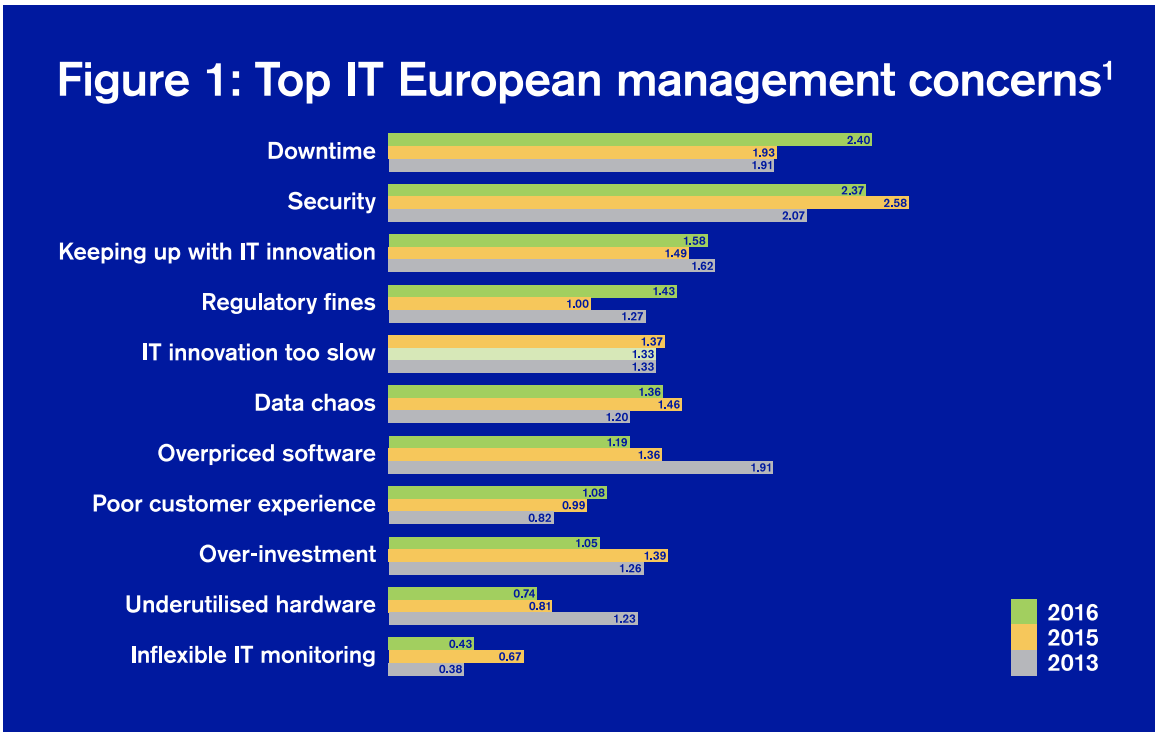
There is, however, another powerful spin-off from network modelling: the ability to answer many regulatory questions with ease. Imagine being able to confirm compliance to different auditors at any time by running standard reports from a single tool that confirms relevant processes have been continuously running on isolated network segments with proven levels of security. The need to do so is evermore necessary as regulators clamp down on how IT risk is managed and data privacy ensured, whilst expecting open services.

© QUOCIRCA 2017

This report looks at how network models can help European IT managers ensure their organisation's networks have the security and resilience to meet the requirements of some of the most demanding regulations to have emerged or be modified in recent years: GDPR, NIS, PCI-DSS, PSD2 and the E-Privacy Directive. It also looks at NESA, an example of recent regulation in the Middle East, which gives an indication of where government legislation may be heading.

Where regulations come from

Regulatory requirements do not top the list of IT concerns for most European organisations. Quocirca has been tracking IT concerns across Europe for five years; security, downtime and innovation are consistently placed ahead of regulatory fines (Figure 1). A network model helps in all three areas, improving security, reducing downtime and enabling safer innovation through the testing of new ideas. However, a network model can also play a key role in meeting regulatory requirements, concerns about which were on the rise in 2016.

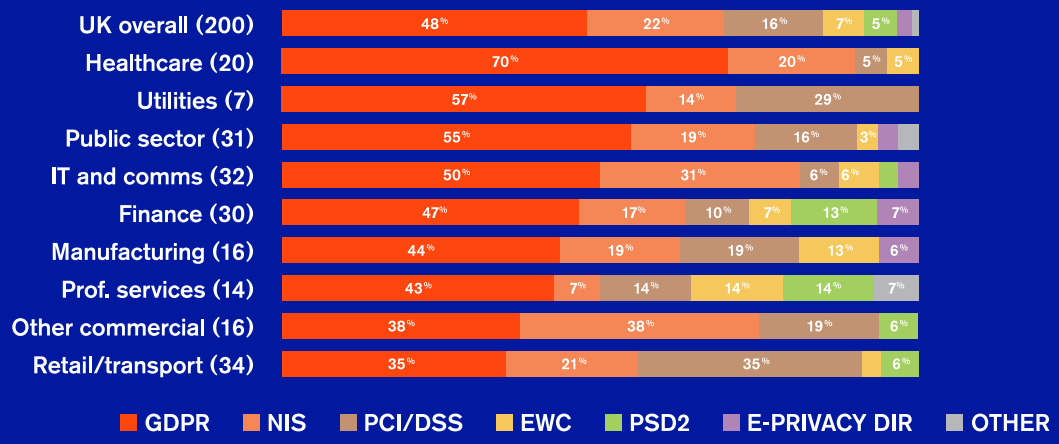


The decision to upgrade network modelling capabilities can be justified on all these grounds, it does not need to rely solely on the need to satisfy auditors. However, regulation is unavoidable and failure to comply has huge potential cost, and most organisations accept there is room for improvement in their ability to do so; satisfaction with existing tools to support regulatory requirements was rated at 3.7 out of 5 in a 2017 survey conducted to support this report[2].

© QUOCIRCA 2017

Regulations are passed down by various levels of governance. The EU plays a major role for member states. The General Data Protection Regulation (GDPR), set to come into force in May 2018, currently dominates thinking; the regulation will replace existing local data protection laws such as Germany's BDSG and France's DPA. Even in the UK, with its plans to leave the EU, GDPR tops the list (Figure 2) and is scheduled to replace the local DPA. Other regulations high on the list are the EU Network Information Security (NIS) Directive for protecting critical infrastructure and the global Payment Card Industry Data Security Standard (PCI-DSS).

Figure 2: The regulation that will have greatest impact on cyber security and resilience plans[2]



Beyond regulations passed down by governments and industries, many organisations elect to follow certain standards. These include the ISO-27000 family of standards around information management, COBIT for IT management and the guidance of the US-based Center for Internet Security (CIS) which aligns with ISO-27001.17 (for example, recommending *continuous vulnerability assessment and remediation).* Aligning with such standards may be a governance choice, part of ensuring compliance readiness, or reflect requirements passed down by other organisations; cross-organisational processes such as supply chains and sales channels that a business opts in to may impose such standards.

Prescriptive versus non-prescriptive regulations

Some regulations are **prescriptive**, stating that penalties can be imposed if certain stated capabilities are not in place. For example, PCI-DSS lists security technologies and procedures that should be deployed to compliantly process payments, including specific network segmentation requirements, the integrity of which can be tested and verified with network modelling. There is a direct cost to prescriptive regulations: if the rules say you must have a web-application firewall in place, so be it, that investment must be made to tick the necessary box, even if your organisation deems it unnecessary.

© QUOCIRCA 2017

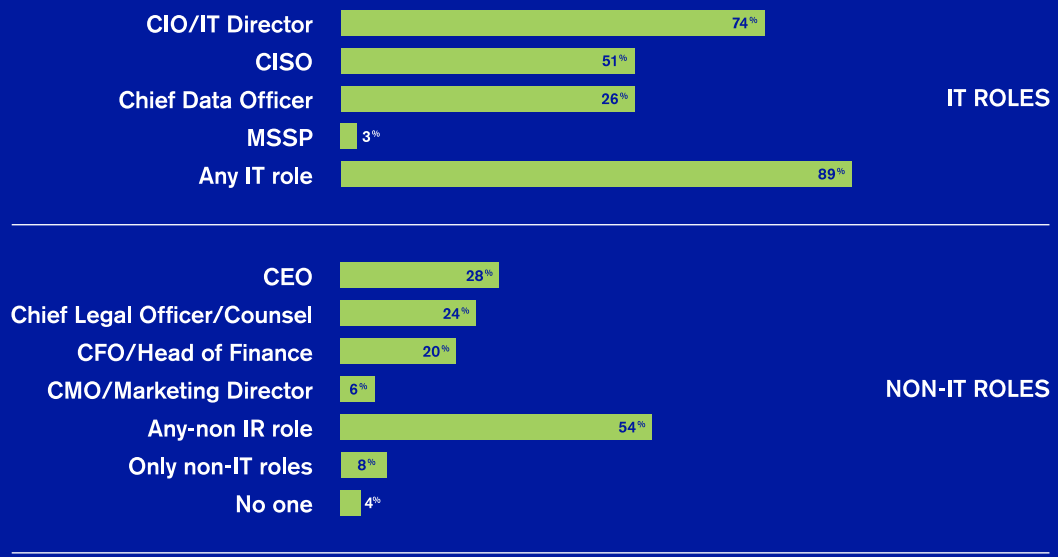
Most regulations are **non-prescriptive,** stating a certain service level must be met and what the penalty is for failing to do so, but not stipulating how this should be done. For example, GDPR says you must protect the rights of *data subjects* and could be fined for failing to do so. However, it does not say how this should be achieved. Even with non-prescriptive regulations there is an obvious need to understand the areas of a network where certain workloads are running and/or certain data types are being processed and who has access to these areas.

How do network models and risk scoring enable compliance?

Terms such as digital resilience, risk scoring, continuous testing and verification, change management, hardened security, finding and fixing vulnerabilities, proven integrity of network segments, access controls and safe cloud use, are integral to network models. They will also be compelling to IT management teams and the boards they serve, to whom they must appeal for funds to invest in new tools. These terms are found, in one form or another, in the language of regulators too.

So, the case for investing in network modelling tools to support regulatory compliance, need not be made in isolation. Board-level managers should be receptive, they have the ultimate responsibility for ensuring governance controls. In more than 50% of the organisations surveyed in the supporting research for this report, senior non-IT managers are involved in ensuring that regulatory requirements are met (Figure 3).

Figure 3: Involvement of management roles in ensuring that regulatory requirements are met[2]



Network modelling tools can provide many of the outputs needed for compliance reports at audit time and, perhaps more importantly, up-to-date interim reports can be generated at any time, especially when an incident has occurred. This replaces impractical, expensive and error-prone manual processes, that will often involve irregularly updated check-lists compiled using spreadsheets or tick-list style compliance products, which are often only opened and modified to provide a rushed snapshot when the auditors are on their way. Organisations operating in this way need to change, some of the checks required to ensure regulatory needs are met will require technical skills which compliance team members do not have.

With both IT infrastructure and the risk landscape now being so dynamic, the continuous verification of network infrastructure that network models provide is the easiest way to ensure networks are always compliant and that regulatory alignment does not drift as changes are made. This can be quantified through the resilience and risk scores that the modelling tools provide for an organisation's whole network or any given segment of it at any time. Scores should be based on several metrics including completeness of the network model (i.e. are there any parts of your network you don't know about?), the comprehensiveness of vulnerability scanning and the completion of configuration checks across thousands of devices.

Network segmentation is the best way to ensure that relevant applications, for example those processing personal data, are isolated. By analysing the configuration of layer-3 network devices, a network model shows and verifies the integrity of network segments, identifying any policy deviations for remediation. Ensuring the isolation of utility networks is one of the controls required in the EU's NIS Directive and the cardholder data environment (CDE) must be isolated for PCI-DSS compliance. Network segments may have to reflect real-world geography, ensuring regulated data remains in certain places; for example, the Russian regulator, Roscommandzor, requires that the personal data of Russian citizens is stored only in databases located in Russia.

An integral part of a network model should be the creation of a complete, validated network architecture map with an inventory listing devices, along with contextual information about their location and purpose. Dark areas of the network need to be identified and eliminated (for example a router with an unknown link). Best-practice configurations for firewalls and other devices are required by certain regulations (for example PCI-DSS and NESA), checks for which can become automated and routine. Access points and security products can be tested in context and recommendations for policy updates and device hardening provided and enacted through connections to ticketing systems.

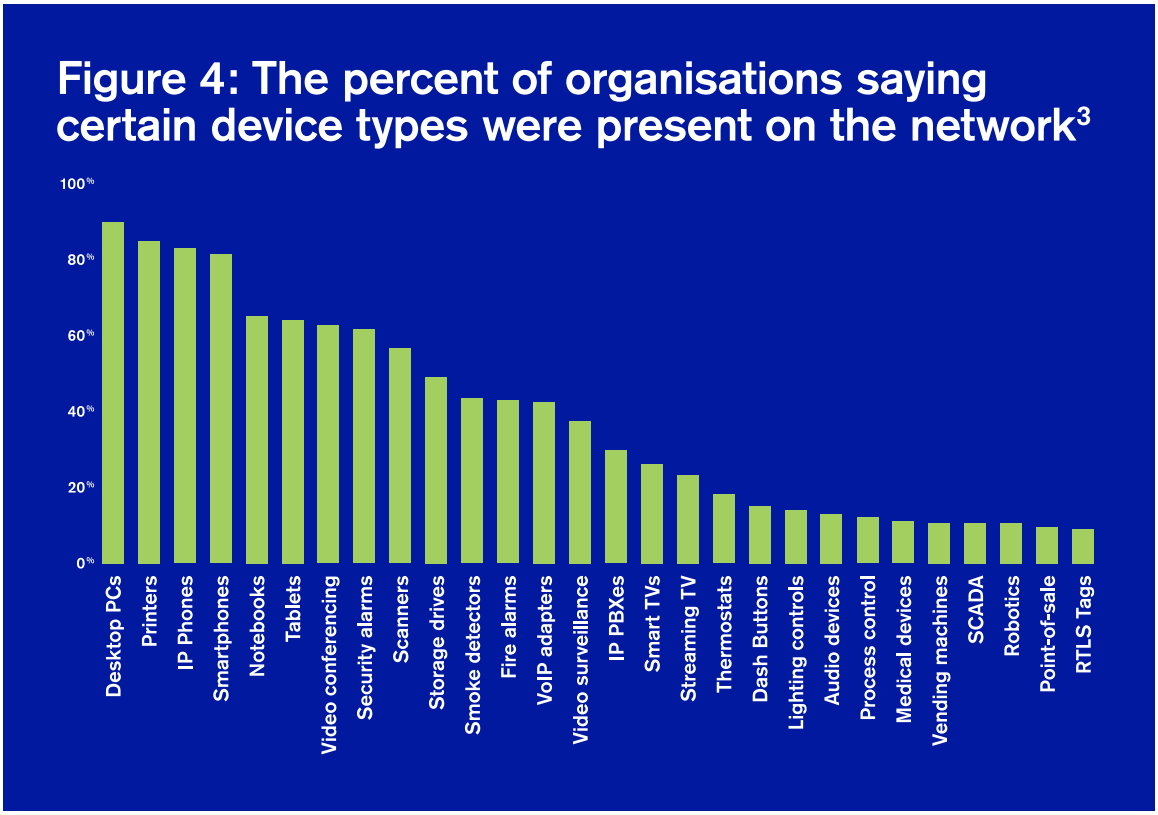
The analytical engine that sits at the heart of a network modelling tool can simulate the impact of configuration changes before they are made. New investments, necessary to comply with a regulatory requirement, can be tested to ensure they meet needs: for example, are all workloads processing sensitive data covered by the deployment of new firewalls? The separation of externally facing de-militarised zones (DMZ) from sensitive network segments can be ensured. PCI-DSS requires that the purpose of all access into DMZs is documented, hard to achieve without an effective network model.

Much of the risk associated with complex networks is due to vulnerabilities for which exploits may have been developed. Integrated vulnerability scanning and management tools are constantly reporting and providing scores based on vulnerabilities. A network model can be used to enrich this data and schedule changes based on the severity of the vulnerability, its network context and the impact it may have on compliance. A regulated process may need attention first, even if for a lower-order vulnerability. NIS, PCI-DSS and NESA all make specific reference to vulnerability management.

© QUOCIRCA 2017

Most regulations are specific about controlling access rights, including GDPR, NIS, PCI-DSS, the E-Privacy Directive and NESA. Having clarity of network access policy is complicated by the rise of public and hybrid cloud deployments, virtualised networks, the enablement of cross organisational business processes, including the need to provide access for third-party maintenance teams to both IT and non-IT infrastructure, and the proliferation of user and IoT devices (Figure 4). A network model gives insight into which users and applications have access to what network segments and resources and with which privileges, recommending when access can be reduced, for example to ensuring *least privilege.* This limits the impact intruders and malware can have, as attackers almost always seek out privilege to achieve their goals.

Figure 4: The percent of organisations saying certain device types were present on the network[3]



The public cloud platforms an organisation uses must be considered an extension of its network and covered by network models for the models to be comprehensive and effective. The configuration of connections to external resources and the configuration of any software-defined networks involved should be tested daily, as the cloud providers themselves may introduce changes or change-management controls. For example, do links remain restricted to virtual private networks (VPNs) rather than the public internet. Reporting on the use and status of cloud platforms is also an increasing regulatory requirement, for example in GDPR and NESA; much of NIS is aimed at cloud service providers. Germany's BSI sets, out in a document called C5[4], the minimum requirements for cloud service providers. The UK's Financial Conduct Authority has issued a guidance document for using cloud services[5]. 93% of organisations surveyed in the supporting research said they are adapting the way they are meeting regulatory requirements due to the use of public cloud.

© QUOCIRCA 2017

Clearly a network model has many attributes that are relevant to meeting the needs of regulators. How do these map to specific regulatory regimes?

Applying network models to specific regulations

With a dynamic, up-to-date network model in place, compliance can become an everyday result of automated processes rather than a once-per-regulatory cycle clean-up. Security teams don't have to panic every time external auditors visit and the audit team get higher quality, technically reliable, up-to-date answers to their questions.

Some specific regulations were identified by respondents to the supporting research as the most important: GDPR, NIS, PCI-DSS, PSD2 and The E-Privacy Directive as well as new prescriptive regulation from the UAE's regulator NESA. For each there is a description of the regulation itself. This is followed by guidance on where network modelling can provide the data required by auditors and identify problems arising that may take a given system outside of compliance requirements. Network modelling tools may also provide dynamic templates for certain of these, further easing the job of keeping IT infrastructure in line with a given regulation.

The EU General Data Protection Regulation (GDPR)

In Europe, the GDPR currently dominates the regulator agenda. GDPR is already law and will be enforced from May 2018. The UK government has said GDPR will remain law in the UK despite Brexit. GDPR is a pan-EU regime that supersedes multiple national data protection laws that were based on the 1995 EU Data Protection Directive. GDPR applies at some level to just about any organisation and is cited by other regulations when it comes to protecting **personally identifiable information** (PII), for example NIS and PSD2.

GDPR places the responsibility for compliance on **data controllers,** that is any organisation processing PII regarding EU *data subjects* (citizens), whether based inside or outside the EU. GDPR also applies to **data processors**, organisations to which the processing of PII has been outsourced by data controllers, for example, public cloud service providers. Enforcement bodies, such as France's CNIL, Germany's DfDI and the UK's ICO can issue enforcement notices and fines for both security and administrative failings.

At the core of GDPR is the concept of *privacy by design and by default,* which gives carte blanche to enforcers to reprimand organisations that are breached after a security failure. Timely breach notifications to both the authorities and data subjects is compulsory, and for an incident to go unnoticed for more than a few days could be considered poorly designed privacy.

GDPR is non-prescriptive; its requirements are all about protecting personal data but not how it should be done. There are 11 chapters with 99 articles, many of which do not relate directly to technology use. How the regulatory bodies police GDPR will not be determined until after it is enforced. However, the enforcement of existing data protection law suggests the regulatory authorities accept that breaches will occur and are lenient when it is evident this has happened despite good practice, rather than due to that of bad practice.

© QUOCIRCA 2017

So, it makes sense establish a good track record for GDPR compliance now, for example putting in place the ability to document and monitor the technology in place for processing PII and the improvements being made to it. There is no end-point to this; part of the challenge, for regulators and data controllers alike, is to keep ahead of the criminals who want to steal PII.

APPLYING A NETWORK MODEL TO GDPR

Article 32, *security of processing,* is the main requirement directly addressing the use of technology; it requires measures to be in place that ensure the security of personal data. It recommends some specific security measures, such as encryption; other requirements are vaguer, for example *"the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services",* having processes for *"regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing"* and ensuring there is no *"unauthorised disclosure of, or access to personal data".*

These goals can only be achieved if processing is restricted to segmented parts of the network, and if there are means in place to test and report on the status of, and access to, this area; for example, ensuring continuous monitoring for vulnerabilities and auditing access controls. This is the essence of article 25: *"data protection by design and by default".* Other articles allude to this too: Article 5 requires that controllers can demonstrate that personal data is being *"processed lawfully"* and that this can be demonstrated. This again requires the ability to report on the network segment where processing takes place. Article 30 requires that records are kept of processing activities. All integral capabilities of network modelling tools.

Articles 33 and 34 relate to breach notification to both the data protection authority and data subjects. When a breach is suspected, the initial investigation should be to determine if a breach has indeed occurred and if it needs reporting. If the answer is yes, it is necessary to document the status of the systems at the time of the incident, the blast radius and whether an attack extended into the network segments to which the processing of PII can be proved to be restricted. Demonstrating that the breach happened despite good practice, should lead to more lenient judgement.

Certain elective standard bodies have published mappings to GDPR including ISO[6] and the UK BSI (BS-10012).

EU Network Information Security Directive (NIS)

NIS provides legal measures to improve the cyber security of networked attached services. It covers *operators of essential services* (OES) which run utilities (electricity, gas, water), transport systems (air, rail and road) and banking services, and *digital service providers* (DSP) which includes cloud service providers, online market places and search engines.

NIS applies to non-EU based organisations that operate in the EU and to third parties to which OESs and DSPs outsource. NIS came into force in August 2016; however, EU member states have until May 2018 to enact national laws and six months after this to identify the OESs and DSPs to which it should be applied. The UK government says it supports the aims of NIS and has proposed implementation despite Brexit.

NIS requires regular assessments of the information systems and the security policies involved in

providing networked services. Incidents which affect a certain number of users, continue for a given period of time or have a certain geographic extent must be reported.

The NIS Directive is not prescriptive, requiring the adoption of "appropriate and proportionate technical and organisational measures" to achieve compliance, however it gives plenty of examples. A culture of risk management and assessment is required with the implementation of appropriate security measures. The rules for DSPs and OESs differ, but there is broad overlap.

APPLYING A NETWORK MODEL TO NIS

The European Union Agency for Network and Information Security (ENISA) details compliance for DSPs[7]. There are 27 Security Objectives (SOs). Network monitoring is recommended to ensure certain measures are in place and that on-going changes are documented. Networks should be regularly tested and security proactively improved, with evidence of the steps taken.

SO-10 requires continuous monitoring of *access controls to network and information systems.* Recommended measures include: *network isolation and implementation of segmented network security zones that limit the impact of a malware incident, logs from privileged accounts' usage* and *access control policy.*

SO-11 addresses the *integrity of network components and information systems.* SO-13 requires change management procedures, suggesting that for *each change, a report is available describing the steps and the result of the change.* SO-14 details the need for *asset management and configuration controls for key network and information systems. SO-17* addresses business continuity and SO-15 *the detection, response, mitigation, recovery and remediation from a security incident;* in other words, a way to measure and ensure digital resilience.

SO-20 says appropriate procedures for *testing key network and information systems underpinning the offered services* should be in place and SO-21 procedures for performing security assessments of critical assets. SO-22 requires compliance with national and EU legal requirements and industry best practices and standards (which would include GDPR).

It is hard to see how the requirements of NIS can be met without a capability to model a network, ensuring the isolation of relevant systems, through continuous monitoring and testing.

ENISA provides mappings to other standards and regulations including ISO27001, PCI-DSS, NIST and COBIT.

Payment Card Industry Data Security Standard (PCI/DSS)

PCI-DSS is a global standard and one of the most prescriptive. It is focussed on how payment card data (PCD) is stored and processed (as a type of personal data, in Europe, PCD is also subject to GDPR). The standard is controlled by the PCI Security Standards Council, which represents the card brands: Visa, MasterCard, Amex etc. which police compliance.

PCI-DSS describes specific technologies that must be in place in any organisation that processes PCD. Compliance must be validated annually via self-assessment or by a qualified security assessor. However,

it is expected that compliance activities are conducted in an on-going manner and that fully compliant behaviour should be ***business as usual***. Achieving this requires continuous network monitoring of, what is termed, the card data environment (CDE) rather than just bringing things up to date once a year.

APPLYING A NETWORK MODEL TO PCI-DSS

PCI-DSS 3.2 is the current iteration of the standard[8]. It lists the best practices for implementing business-as-usual processes (on page 13), which would be cumbersome to achieve without a constantly updated network model. These include *"monitoring of security controls—such as firewalls, intrusion-detection systems/intrusion-prevention systems, file-integrity monitoring, anti-virus, access controls, etc.—to ensure they are operating effectively and as intended", "Ensuring that all failures in security controls are detected and responded to in a timely manner"* and *"reviewing changes to the [card holder] environment (for example, addition of new systems, changes in system or network configurations) prior to completion of the change".* So, the CDE needs be a distinct, tightly controlled and monitored network segment.

Beyond these generalisations PCI-DSS has 12 high-level requirements each with several sub-clauses. At least five of these include specific technical controls, the validation of which can be automated through reference to an up-to-date network model. Requirement 1 includes the ability to produce an up-to-date *firewall configuration diagram;* provide *access path analysis to the network segments* where card data is being processed; and *validation of network device hardening and best practices* (which are expected to be in place by Requirement 2).

Requirement 4 covers the encrypted transmission of cardholder data across open, public networks (specifically TLS rather than outdated SSL encryption). Requirement 5, says a *vulnerability management program* must be in place. Requirement 6 states that the processing applications must run on *isolated network segments* and suggests the use of web application firewalls in conjunction with network-based firewalls. Requirement 11 stipulates the regular testing of security systems and processes or automated daily network segmentation change detection. Requirement 7 says *access to cardholder data is restricted and requirement 10 the tracking and monitoring all access to network resources and cardholder data* in the CDE.

Payment Services Directive (PSD/PSD2)

The EU PSD (2007) and its successor PSD2 (2015) is a legal framework that payment service providers (PSP) must operate within. A PSP is any organisation providing a payment service: services such as PayPal, Apple Pay and Worldpay. PSD promotes the development and use of innovative digital payments across the EU as part of a drive towards a digital single market. PSD aims to improve access to payment systems (including open APIs for developers), ensure high availability (digital resilience) and protect consumers whilst guaranteeing faster payments.

PSD2 includes 117 articles, the majority of which are non-technical focussed on financial risk and customer service. With the data sharing envisaged to provide open payment services there are significant overlaps between the GDPR and NIS, and many of the requirements of these two regulations are also relevant. Article 94 addresses data protection and references the exiting 1995 EU Data Protection Directive.

APPLYING A NETWORK MODEL TO PSD2

PSPs are required to establish a framework to manage operational and security risks. This requires setting up and maintaining incident management procedures to include the detection and classification of major incidents, *"the establishment, implementation and monitoring of the security measures, including certification processes where relevant".* Article 95 says PSPs *"shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents".* Article 96 addresses incident reporting.

Network models enable PSPs to ensure that payment processing applications are restricted to controlled network segments and that the access to them, that must be provided, is controlled and audited. The model also ensures the reporting requirements are in place to respond when incidents occur.

The E-Privacy Directive

Formerly European Directive 2002/58/EC, the E-Privacy Directive limits direct marketing activities such as nuisance phone calls and spam SMS and email messages, which cannot be sent without the consent of recipients. It also includes the so-called *Cookie Law,* requiring consent to create and maintain data files on user computers to personalise their experience.

The directive is currently under review to keep it in line with its big brother, GDPR. As a directive, it is expressed through EU nation-state legislation; for example, it is enacted in Germany via the existing Telecommunications Act and in France via Article 32-II of the Data Protection Act. The UK introduced a specific law known as Privacy and Electronic Communications Regulations (PECR) in 2003; the UK ICO has issued more fines under PECR in the last two years than it has under the DPA.

The directive has 21 articles and has much overlap with data protection laws and is usually policed by the same data protection authorities. Many of its requirements are specific to how communication with consumers is handled and how lists are maintained. However, there are specific technical requirements.

APPLYING A NETWORK MODEL TO THE E-PRIVACY DIRECTIVE

Article 4 covers security, requiring an operator to take *appropriate technical and organisational measures to safeguard security of its services.* In the case of a breach, when the cause is due to the operator itself rather than a third-party service, subscribers must be informed. In other words, it must be clear where the network demarcation lies between the provider of a service and its network service providers. Articles 6 and 9 deal with the security of traffic data, including access controls to data. A network model can provide much of the information required.

© QUOCIRCA 2017

The UAE's National Electronic Security Authority Information Assurance Standards

The NESA-IA Standards (NESA) is worth looking at even for organisations with no infrastructure deployed in the UAE, as it is an example of a prescriptive regulation that details how networks should be configured and managed to "sustain the benefits of a trusted digital environment for businesses and individuals across the nation".

NESA includes 15 families of technical (T) and management (M) security controls (188 individual controls), each given a priority rating from P1 highest to P4 lowest.

APPLYING A NETWORK MODEL TO NESA

NESA requires the importance of IT assets for processing information to be documented, in other words an up-to-date context-aware device registry (an integral part of a functional network model). This must cover everything from user devices, storage and servers, to both internal and external network services.

T1.2 (P2) requires the automation of processes for tracking assets and access to them, updated as new systems are acquired. T2.3.3 (P4) requires unauthorised devices be identified and refers to T5.4.3 (P1) that requires identification of all equipment connected to networks. T3.6.2 (P2) requires that audit logging is activated and T3.6.3 (P1) that the use of information systems is monitored. T4.5 focusses on network security, requiring all the network components and interconnectivity to them to be understood, the maintenance of a network diagram and the identification and the mitigation of vulnerabilities.

T4.5.1 (P1) and T4.5.3 (P1) require the segregation of groups of information services on networks and that in-place controls are continually monitored for efficiency and effectiveness. T7.7 requires risks resulting from known vulnerabilities to be addressed, including T7.7.1 (P1) acting upon information about technical vulnerabilities.

T5 covers access controls, including T5.1.1 (P2), the establishment of an access-control policy based on business and security requirements. T5.6.2 (P2) requires sensitive system isolation (network segmentation). T6.3.1 (P2) expects cloud environments and, where possible, components to be included in risk assessments.

NESA provides mappings to certain standards including ISO 27001 and NIST. It would be hard to achieve the requirements of NESA without the ability to segment networks and monitor access to them, their integrity and security; all provided via a functional network model.

Conclusion

Businesses have little choice but to accept regulations, but they should go further, and put in place the technology that makes compliance an everyday automated process, working in the interests of all stakeholders. Network modelling enables many current and future compliance requirements to be addressed from the top down through providing the network visibility that has far broader benefits for businesses beyond regulation.

© QUOCIRCA 2017

References

1 – Masters of Machines III, Quocirca 2016:
http://quocirca.com/content/masters-machines-iii

2 – Research commissioned by RedSeal in mid-2017, 200 senior UK IT managers from organisations with 500+ employees

3 – European Perceptions, Preparedness and Strategies for IoT Security, Quocirca 2016:
http://quocirca.com/content/european-perceptions-preparedness-and-strategies-iot-security

4 – C5 – the BSI's Cloud Computing Compliance Controls Catalogue:
https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html

5 – FG 16/5 – Financial Conduct Authority Guidance for firms outsourcing to the 'cloud' and other third-party IT services:
https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf

6 – Mapping between GDPR (the EU General Data Protection Regulation) and ISO27000:
https://view.officeapps.live.com/op/view.aspx?src=http://www.iso27001security.com/ISO27k_GDPR_mapping_release_1.docx

7 – ENISA Technical Guidelines for the implementation of minimum security measures for Digital Service Providers:
https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

8 – PCI SSC, PCI DSS v3.2 Framework for a robust payment card data security process:
https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

© QUOCIRCA 2017

About RedSeal

RedSeal's network modelling and risk scoring platform is the foundation for enabling enterprise networks to be resilient to cyber events and network interruptions in an increasingly digital world. RedSeal helps customers understand their network from the inside, out – and provides rich context, situational awareness and a Digital Resilience Score to help enterprises measure and ultimately build greater resilience into their infrastructure. Government agencies and Global 2000 companies around the world rely on RedSeal to help them improve their overall security posture, accelerate incident response and increase the productivity of their security and network teams. Founded in 2004, RedSeal is headquartered in Sunnyvale, California and serves customers globally through a channel partner network. More about RedSeal

About Quocirca

Quocirca is a research and analysis company with a primary focus on the European market. Quocirca produces free to market content aimed at IT decision makers and those that influence them in business of all sizes and public-sector organisations. Much of the content Quocirca produces is based on its own primary research. For this primary research, Quocirca has native language telephone interviewing capabilities across Europe and is also able to cover North America and the Asia Pacific region. Research is conducted one-to-one with individuals in target job roles to ensure the right questions are being asked of the right people. Comparative results are reported by geography, industry, size of business, job role and other parameters as required. The research is sponsored by a broad spectrum of IT vendors, service providers and channel organisations. However, all Quocirca content is written from an independent standpoint and addresses the issues with regard to the use of IT within the context of an organisation, rather than specific products. Therefore, Quocirca's advice is free from vendor bias and is based purely on the insight gained through research, combined with the broad knowledge and analytical capabilities of Quocirca's analysts who focus on the 'big picture'. Quocirca is widely regarded as one of the most influential analyst companies in Europe. Through its close relationships with the media, Quocirca articles and reports reach millions of influencers and decision makers. More about Quocirca

© QUOCIRCA 2017