axians

Insight Paper

Network Security

Website
axians.co.uk/services/security

Achieve strong network security ecosystems to protect customer data

Steps to a more secure network

EXECUTIVE SUMMARY

A recent survey of 2,000 IT professionals revealed UK Businesses are struggling to detect, prevent and respond to cyber threats. With preparations needed for the General Data Protection Regulation (GDPR) and Network Information Security (NIS) directive, UK companies are expected to invest heavily in upgrading their existing systems as they look to provide better protection against cyber-attacks, data losses and incidents from unauthorised systems.

Building and maintaining a positive and visible brand reputation is vital for business success. But reputation can very easily be destroyed by a hacker on a mission, which is why reliable and secure technology is essential for today's organisations. With a growing number of devices becoming connected, demands for transformative technology, along with users' insistence that their data is secure, means the problem is not going to go away.

The impact of cyber-crime and the ability of our systems to protect data is a huge concern across industries and markets. The importance of secure data combined with policies such as GDPR means that there is a clear obligation for organisations to take the appropriate technical measures to keep their customers safe and to avoid negative reputational and revenue impact.

GDPR COMPLIANCE

With GDPR, any business that handles personal data must now be on track towards compliance. These stringent regulations, combined with the obvious reputational damage that accompanies a data breach, means that companies will need to implement a strong security ecosystem to protect their customers' information.

The terms of GDPR ensure that businesses face concrete sanctions for non-compliance – namely administrative fines of up to €20m or 4% of a company's annual turnover

GDPR COMPLIANCE cont'

(whichever is greater). In practice, organisations have a legal obligation to alert the relevant supervisory authority, and in some cases the customers affected, of a data breach within 72 hours of it occurring

RATE OF CHANGE

LEADING INTERNET SECURITY COMPANY VERISIGN OBSERVED THAT DDOS ATTACKS REMAIN UNPREDICTABLE AND PERSISTENT, AND VARY WIDELY IN TERMS OF VOLUME, SPEED AND COMPLEXITY. TO COMBAT THESE ATTACKS, IT IS BECOMING INCREASINGLY IMPORTANT TO CONSTANTLY MONITOR FOR CHANGES IN ORDER TO OPTIMIZE MITIGATION STRATEGIES

The variety of structured and unstructured attacks that cybercriminals can deploy has increased, and with it, threats relating to cybersecurity are growing. For example, cybersecurity company Kaspersky Lab reported that they discover around 70,000 new viruses every day. For this reason, both national and international legislation is aimed towards adopting appropriate measures. ICT resources have changed significantly over recent years, data is often sent to third parties, and more and more applications and software is needed to keep a business running. The rate of transformation in technology means users expectations also change rapidly. Data protection must therefore form an integral part of the architecture of every organisation, considering the way people work and communicate and how it can be done as safely and efficiently as possible.

TRENDS

Securing customer and employee data privacy in a cloud environment

Cloud-based technologies can provide powerful and agile content to deliver the best customer experiences and flexibility for an increasingly digital workforce. All organisations need to balance the level of importance of the data held, where it comes from, how it is hosted, and who it goes to (including all interactions with internal operations, partners, suppliers and so on), with the level of security measures they put in place. Ultimately, whether you secure it in house or through cloud-based technologies, the organisation is responsible.

Business changing regulatory developments

Regulators around the world are imposing more controls and penalties against organisations in three key areas: **privacy for the consumer, protection of Personally Identifiable Information (PII), and the right to erasure.** Fines, sanctions and reputational damage will be issued for non-compliance if regulations are not met, with the new EU General Data Protection Regulation being the toughest of all.

TRENDS cont'

Managing fraud in a multichannel environment

Fraud is well understood and most organisations have dedicated solutions for this. However, in a multichannel environment, with sales being taken in one channel and fulfilment handled by another, it's easy to become a target for exploitation if they do not have a complete understanding of all the processes involved.

The new kid on the block: Internet of Things

High profile attacks on Internet of Things (IoT) devices such as the Mirai botnet have left businesses pondering how to harness the undoubted power of IoT without sacrificing security. Whilst threats to PCs, servers and networked devices are widely understood, there are many unknown or poorly understood threats that IoT brings. It is therefore up to the business to ensure these devices - which are essentially remote controls for the world to operate - are secure and remain accessible by authorised personnel and devices only.

Actions speak louder than words

It's not just customers that are affected if security is breached; suppliers and partners are too. After a serious attack takes place and becomes public, the perception of the organisation and its partners can nosedive within minutes. Cyber attackers are very organised, deploying sophisticated and dangerous threats to the data held by a organisation. Today, an attack is virtually impossible to contain before anyone hears about it. Taking years to gain and seconds to lose, reputation is intangible but should be taken as seriously as the 'physical' risks to a business. As industrialist, Henry Ford, said: "You can't build a reputation on what you are going to do."

Retailers, for example, are constantly looking for ways to enhance their customer offering and squeeze extra margin and, with the additional pressures to transform digitally and keep customer data protected, means new technology provides an opportunity to address a number of challenges.

APPROXIMATELY 50% OF EMPLOYEES THINK THAT THEIR IT DEPARTMENT IS NOT AWARE OF ALL THE COMPANIES CONNECTED DEVICES, AND AROUND 70% PERCEIVE THEIR ORGANISATION AS AT RISK FROM A CONNECTED DEVICE RELATED SECURITY ISSUE.

SURVEY, CONDUCTED BY AXIANS UK THROUGH ARLINGTON RESEARCH

SECURING KEY MARKETS

ORGANISATIONS NEED TO SET IN PLACE SUSTAINABLE FRAMEWORKS FOR DATA GOVERNANCE AND SECURITY, CRISIS MANAGEMENT PROCEDURES AND IT ARCHITECTURE, WHICH CAN COMBINE TO ACHIEVE A STRONG SECURITY ECOSYSTEM.

Research and Education

Education is strengthening with moves towards digitisation; from teaching methods, research data and becoming increasingly accessible online. The availability and integrity of these resources is crucial and every institution must manage their security to protect staff, students and critical research.

Industry and Manufacturing

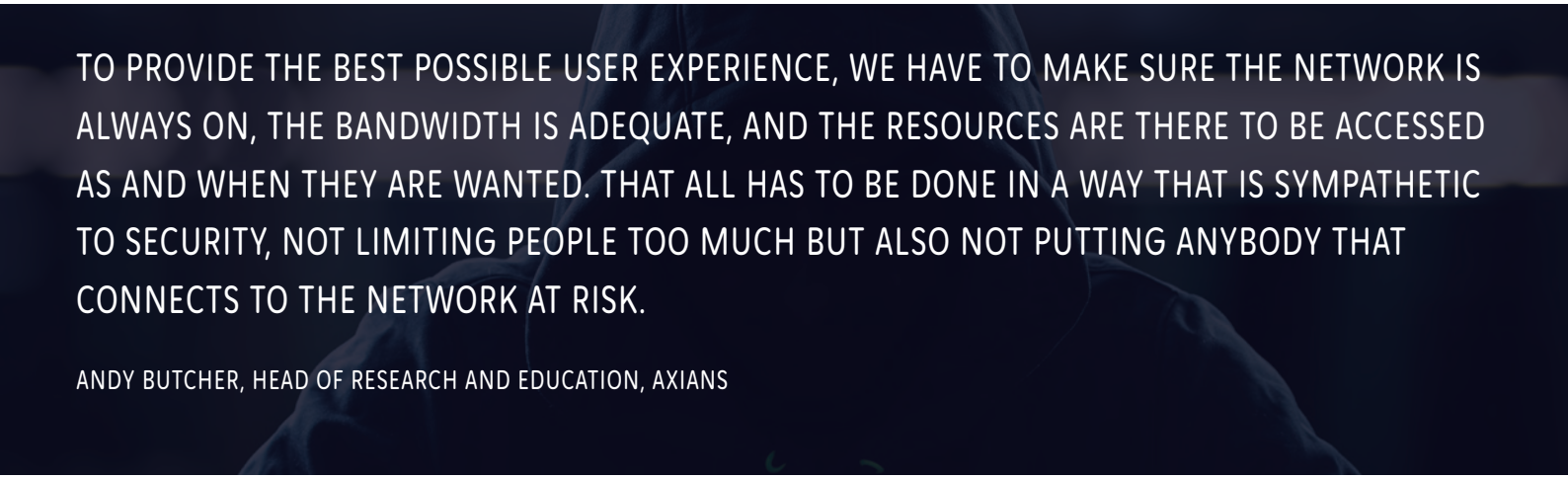
Protecting intellectual property is of the upmost importance while also complying with quality standards. Also, with a range of operational production processes, this market is a clear indication of a sector becoming more reliant on IT. Effective prevention and reduced risk from downtime is essential.

Telco and Enterprise

Protecting the brand by ensuring data is secure as it travels across the network is vital. All businesses from large Telcos to Enteprise recognise the value of brand loyalty, and that it takes just one security incident to lead to negative headlines that undermines years of building a strong brand reputation.

Automotive

Meeting industry, country and international compliance standards enables automotive companies to ensure they are up-to-date with the latest security policy and procedures. It also demonstrates commitment to giving customers, staff and suppliers the confidence that their data is secure, and that if something does go wrong, they can address the issue.



TO PROVIDE THE BEST POSSIBLE USER EXPERIENCE, WE HAVE TO MAKE SURE THE NETWORK IS ALWAYS ON, THE BANDWIDTH IS ADEQUATE, AND THE RESOURCES ARE THERE TO BE ACCESSED AS AND WHEN THEY ARE WANTED. THAT ALL HAS TO BE DONE IN A WAY THAT IS SYMPATHETIC TO SECURITY, NOT LIMITING PEOPLE TOO MUCH BUT ALSO NOT PUTTING ANYBODY THAT CONNECTS TO THE NETWORK AT RISK.

ANDY BUTCHER, HEAD OF RESEARCH AND EDUCATION, AXIANS

MEASURING SUCCESS

Network Security Management is a serious investment. It is an advanced process which maps out the challenges and risks run by an organisation. Only by analysing and defining the landscape can a decision be reached on the security measures to put in place.

Organisations need to set in place sustainable frameworks for data governance and security, crisis management procedures and IT architecture to achieve a strong security ecosystem.

STEPS TO A MORE SECURE NETWORK

STEP 1. Set up and determination of current procedures

STEP 2. Defining the security landscape and implementation

STEP 3. Evaluate reports and data

STEP 4. Identify actions and implementation requirements

SUMMARY

IN AN AGE OF DIGITAL TRANSFORMATION, WHERE CUSTOMER EXPECTATIONS ARE HIGHER THAN EVER BEFORE, AND COMPETITION IS TIGHT, IT'S CRUCIAL THAT BUSINESSES DELIVER A CONSISTENT, HIGH QUALITY CUSTOMER EXPERIENCE, AND IF SOMETHING DOES GO WRONG, THE ABILITY TO REASSURE CUSTOMERS THEY HAVE THE EXPERTISE TO QUICKLY ADDRESS THE ISSUE.

Reviewing a Secure Technology Infrastructure

Security Intelligence

Assets

Vulnerability across the Network

Threat Detection

Behavioural Monitoring

Organisations can do this by maintaining a high level of network security, and where the skills are lacking within this area, using a company which can design, implement and monitor the network on their behalf. By doing so, companies can grow, whilst retaining customer and stakeholder trust.

A secure experience through the network (and cloud) is at the heart of each organisation's capability to deliver world-class service. Everything springs from it – profitability, market share and brand reputation. Through years of experience working across markets the UK, we understand this mix of pressures, which is why we naturally start looking at securing the network by building an understanding of the customer's objectives and challenges. We then apply our specialist knowledge and expertise to ensure the network can help the business achieve its ambitions in both the short and long-term.

ABOUT AXIANS

If you're looking for a fresh approach, Axians offer a variety of network security services, starting with a network security and risk assessment, that can cover many network security areas. Our network assessment specialises in IT asset protection/risk mitigation, but can extend to cover wider services such as Pen tests and Security Governance.

In today's connected digital world, we help organisations to meet growing customer expectations for immediate access to the information and services that can make their lives easier and better. We specialise in helping organisations to develop secure carrier-grade network connectivity that successfully delivers a better end-user experience. We take a pragmatic approach and use incremental changes to optimise network performance and deliver measurable operational and customer benefits. Axians Network Lifecycle Services bring together teams of experts with business, technical and market knowledge to design, integrate, optimise and support digital networks to deliver our customers' exciting plans and ambitions.

axians

Tel. 01256 312350
axians.co.uk