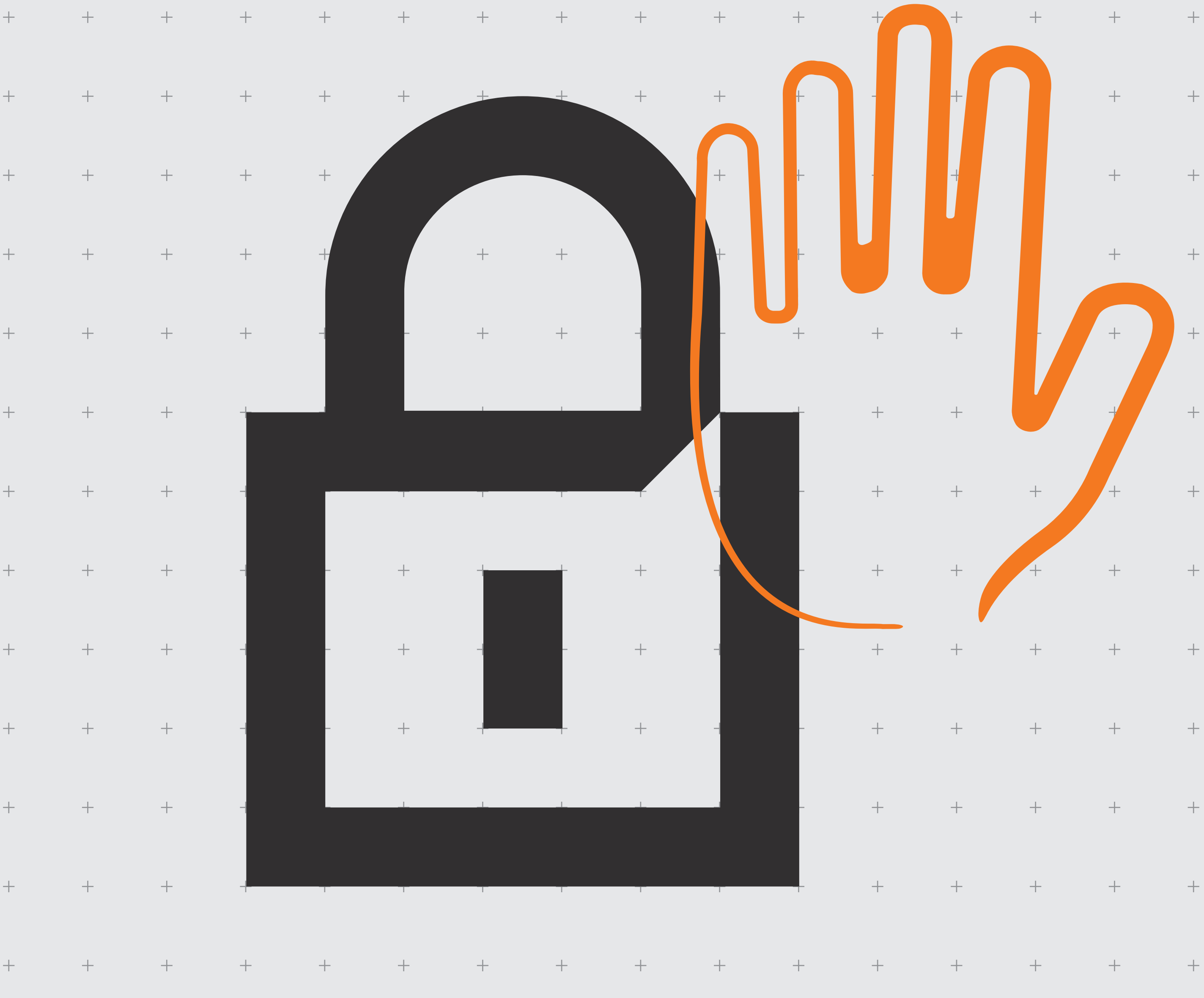
kyoceradocumentsolutions.co.uk

A comprehensive strategy for digital success



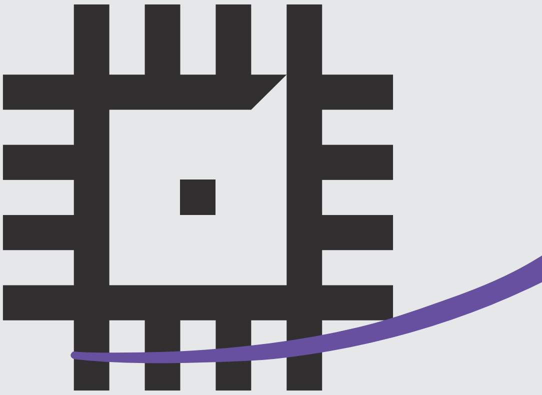
Introduction

As we advance into the information age, converging digital technologies, ultrafast networks and 'Anything-as-a-Service' subscription models are rapidly making themselves felt in the enterprise. The incredible pace of innovation is enabling organisations of all sizes and sectors to enhance their competitive edge by becoming more agile, efficient and productive, and when managed effectively, digital transformation can help to supercharge growth.

However, with new opportunities comes new risks, which many aren't well-placed to defend against. The rush towards digital transformation has increased the attack surface of a company's infrastructure, creating additional weak points and threat vectors that can be easily exploited by opportunistic cyber criminals and hackers operating from anywhere in the world. As a result, rates of cyber-crime and data breaches are on the rise, at a time when GDPR fines are starting to come into force.

The problem, in large part, owes to the fact that security is still considered a technology issue and something for the IT department to sort out, which means there's often insufficient attention paid to it in across other areas of the business. Yes, technology is a critical factor, but just as important is how people are using it.

At Kyocera, we believe organisations need to take a more holistic approach to cyber security by incorporating, leadership, culture and people into the process. This white paper sets out how organisations can achieve a safe, secure and successful digital transformation strategy.



Lead from the top

There is a common misconception that cyber security is the sole responsibility of IT teams and departments, and, as a result, there's often limited recognition of the need to address security at a company-wide level or to pay attention to it at the board level. Indeed, according to research from PwC, only 44% of respondents say their corporate boards actively participate in their companies' overall security strategy. In addition, just over a third of businesses (35%) have a board member or trustee with specific responsibility for cyber security.

When we consider that a severe breach could send reputational, operational, and financial shockwaves through an organisation, this lack of engagement is troubling, if not altogether surprising, given that cyber security takes many execs into areas they're not comfortable in.

However, we are fast arriving at a point when it's no longer acceptable for directors to say that they don't understand technology or cyber security, which begs the question: When does ignorance become negligence?

The Companies Act 2006 states that directors have a legal responsibility to act within their powers and promote the success of their companies, and to exercise independent judgement, reasonable care, skills and diligence. As a result, it's critical that Board members and Non-Executive directors have a complete understanding of their data protection strategies, the cyber risks posed and are able to demonstrate that they have taken the appropriate measures to protect their company from an attack.

Without greater engagement in the world of cyber security in the C-suite, it's more difficult for the IT leaders to secure the funding it needs to secure their IT estates, and more challenging to enact the sort of operational and cultural changes needed to fend of attacks.

In addition, senior executives' level of responsibility and privileged access to valuable company information makes them prime targets for hackers, phishing scams and fraud. This means they may unknowingly be the weakest link in their organisation's cyber security chain, making improving cyber literacy a priority.

At the very least, organisations should appoint a member of staff whose primary remit is to stress test their security posture and who can present on security problems and challenges at board meetings. However, as a next step, dedicated training and penetration testing should be considered. Seeing the ease with which an ethical hacker can break into an email account can go a long way to concentrating the C-suites' minds on the issue!

Put people at the heart of digital transformation

When considering the issue of security, it's easy to get blinded by external threats and focus on keeping bad actors out of your network. But much less attention is paid to threats from within the business.

Businesses are readily investing in new technologies to defend against cyber threats, but these technologies can only go so far and do little to account for the human factor. According to figures from the Department for Digital, Culture, Media and Sport, 7% of breaches are caused by basic human error, and 7% are the result of staff lacking awareness. These figures may not sound like much but when we consider that 50% of the worst breaches faced by businesses are caused by internal staff, the significance becomes clear.

Training on good cyber security hygiene practices can go some way to address this issue, training staff on the importance of using strong passwords, the risks associated with opening attachments from unknown senders, and the most commonly-deployed phishing techniques. This should include working closely with trusted security consultants and organisations that can provide regular penetration testing services, that can identify weak points and vulnerabilities across the infrastructure.

Relying on the best firewall systems and antivirus software will not mitigate the probability of an attack if each member of the workforce has not been educated on the latest compliance, policies and standards. A 'security first' philosophy and workplace culture needs to be supported by regularly updated training programmes for each member of staff — from senior leaders to new starters. This is the most effective way to reduce the probability of a security breach or cyber attacks.

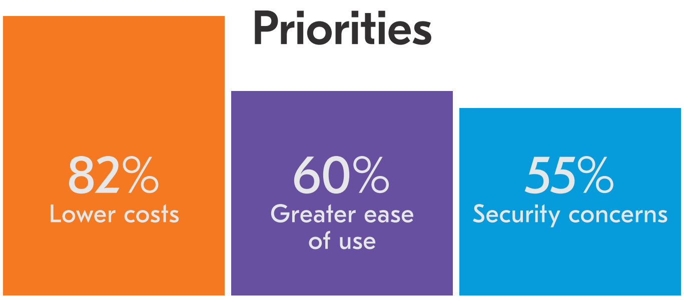
Technology, documents and data

The convergence of new technologies is creating a global workplace, in which each person within an organisation can easily connect to the network, collaborating and sharing documents and data in real-time from anywhere in the world. As the network perimeter expands into the cloud and beyond the traditional office walls, this creates new security challenges.

Digital transformation typically attempts to streamline a company's assets and infrastructure by prioritising agility and efficiency. Although this can provide a significant boost to productivity, it can be restricted by a number of infrastructure problems including outdated legacy hardware and/or licenses, shadow IT used by employees, confusion over who is responsible for what, and zombie servers.

Flexible working, unauthorised collaboration tools and big data have coalesced to create many security challenges and the modern workplace makes it increasingly difficult for IT teams to monitor and neutralise all potential threats. If printers and collaboration tools are not being used securely, this can lead to serious cyber attacks, fraud and data leaks.

Although IT leaders are leveraging innovative tools to analyse business information for opportunities to increase revenues and profit margins, the ubiquity of data and increasing reliance on publicly accessed cloud platforms is creating new threats that can have severe consequences. There are many benefits to adopting new technologies, but if they do not conform to the latest security requirements, this can have an adverse effect on the business.



82% of decision makers are more concerned with prioritising lower costs and greater ease of use (60%) than addressing security concerns around access and data sharing (55%)

When looking to purchase the right content management solutions, including Enterprise Content Management (ECM) and Document Management Systems (DMS) here is what to look out for:

Compatibility

A DMS is a highly secure, centralised digital archive, which acts as a repository for all information and content assets. There has been a reluctance to implement these solutions in the past, as previous versions were incompatible with common operating systems and lacked the sophistication of newer software. For digital transformation to be a success, all connected technologies need to be easy to use, intuitive and user friendly, so they work for people, rather than people working for the technology.

The latest generation of DMS and ECM offer seamless integration with all Microsoft Office applications and can be quickly and easily integrated into any existing IT configuration. The right combination of these solutions will create a highly secure data repository for all corporate content.

Technology, documents and data

continued

Accessibility

All documentation must be easily accessible by anyone with the right privileges but restricted from anyone who is unauthorised. This can only be achieved through the adoption of a DMS that allows IT administrators to manage exactly who can access files at particular times. This means controlling whether they are able to view, edit, copy, share, download or delete these assets at a particular time, with all usage recorded for reference.

An effective DMS needs to be highly secure, but also intuitive and easy-to-use. If it is overly complex or difficult to navigate, there is a risk that staff will resort to using their own shadow IT and tools, making the DMS superfluous. All staff should receive proper training so they can use content management tools efficiently and securely, and not create unnecessary risks.

In addition to controlling print and document management costs, once a DMS has been properly established, it can drastically reduce the chances of 'insider threats' or data leaks, as administrators can easily manage and monitor user privileges for all staff from a single dashboard. This means that all documentation can be securely stored on-site and externally, with remote workers only able to access the files they are allowed to.

Compliance, auditing and reporting

ECM and DMS must be closely aligned with latest security policies, especially GDPR. A secure content management solution can substantially fortify all company, employee and customer data by ensuring each individual and department is adhering to all relevant legal requirements and compliance standards. As any interaction is automatically tracked, logged and saved, this speeds up any administrative processing tasks, ensuring invoicing can be processed more efficiently from receipt to final payment.

DMS is invaluable for auditing and expenses processing, as paperwork trails can be accurately monitored through each interaction, depicting who accessed a document at an exact time, and any previous edits that may have been made. Not only does this protect any sensitive legal or financial documents in a secure location, it keeps auditors and financial departments happy, as they can easily find the information they require, boosting organisational productivity and efficiencies.

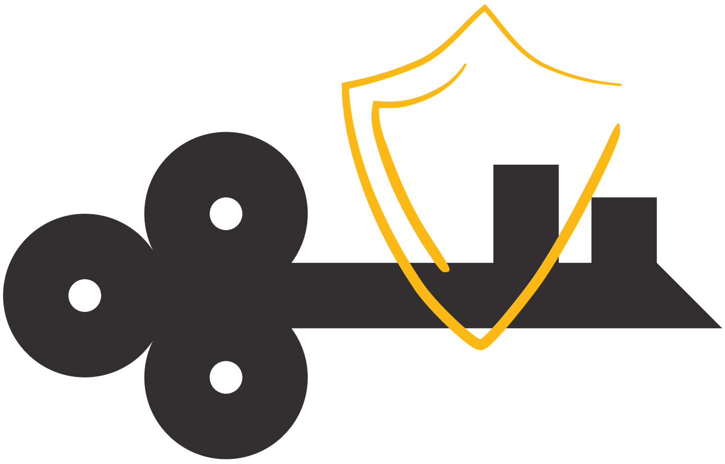
Print security

Most businesses are proactive and efficient when it comes to securing their traditional network assets, including servers, routers and computers, but regrettably, this level of attention is not given to secondary assets and devices, including MFPs, scanners, mobile devices and applications. Although it may not seem a high priority, a poorly secured printer or mobile device could be the Achilles' heel that results in the entire corporate infrastructure being infiltrated.

As printers and associated devices are at the heart of the security ecosystem, they need to be treated as an entry point to internal and external threats. According to our latest industry research, 76% of organisations stated they had a security policy in place for the use of USBs and external drives, but worryingly, only 40% revealed this covers printing and MFPs.

IT and security leaders should conduct a full audit and risk assessment of the entire print estate. Once the team has visibility over the infrastructure, a workflow map can be created to identify potential risks and weaknesses, so the right countermeasures can be taken proactively rather than reactively. Consulting with Kyocera's trusted security experts is vital to support this endeavour and will ensure the latest security considerations are taken into account.

Finally, network security protocols need to include all hardware end points and be implemented from the top level of the organisation. This will help ensure the protection of all data handling interactions, through the entire lifecycle of a document or file, from the moment it enters the business, no matter where it is saved or who is accessing it.



Conclusion

The convergence of new technologies is creating a global workplace, in which each person within an organisation can easily connect to the network, collaborating and sharing documents and data in real-time from anywhere in the world. As the network perimeter expands into the cloud and beyond the traditional office walls, this creates new security challenges.

Choosing the right technology is key, but just as important is promoting a strong culture of data integrity and governance board level, while instilling a culture of compliance, data protection and secure working practices into all staff regardless of their position. Security is the responsibility of the entire workforce and every member of the organisation needs to ensure they are adhering to the latest internal and national security guidelines when operating IP connected devices.

There is a huge incentive for organisations to prioritise security in the digital transformation strategy. A data breach, cyber attacks, fraud incident or accidental data will have severe consequences and therefore short-term investment to protect the infrastructure will help avoid long-term business disruption, reputational damage, regulatory fines and huge potential revenue loss.

This can be achieved by ensuring your network of channel partners is comprised of accredited and trusted experts who can offer the right guidance on the selecting the best available technologies to meet your unique business security requirements. Throwing up a firewall and locking your information down might make your business more secure, but it won't help you reach your digital transformation goals.

How can Kyocera make a difference?

In a digital world, a secure transformation strategy is vital to business success. Kyocera considers security to be of paramount importance and has both the experience and the workforce expertise to act as a strategic advisor to any organisation hoping to bolster its digital infrastructure.

With over 60 years' experience working alongside the best experts in the industry and providing the highest level of digital transformation support to organisations of all sizes, sectors and nationalities. Every product that we manufacture conforms to the highest level of security controls and our longstanding commitment to cyber security means all of our hardware and software solutions comply with the Common Criteria international security standard (ISO/IEC 15408).

To support businesses of all sizes with implementing a safe and secure digital transformation strategy, we have a variety of innovative features designed to protect confidential documents, information and assets. This includes our easy-to-use Data Security Kits which automatically enable encryption and guarantee compliance to the latest standards.

We also provide a Secure Audit service that allows organisations to quickly identify and address any vulnerabilities in just a few clicks, including open ports, protocols, registered accounts, job boxes, installed apps and USB status. The Secure Audit service is compatible with all HyPAS™ enabled MFPs and is the easiest way to ensure ISO compliance. It also enables users to generate saveable printable reports in the JSON format which is required for security audits.

To assist you with your secure digital transformation journey we have also created a selection of white papers to expand on this issue and provide further information and support.

KYOCERA Document Solutions has championed innovative technology for more than 60 years. We enable our customers to turn information into knowledge, excel at learning and surpass others.

With professional expertise and a culture of empathetic partnership, we help organisations put knowledge to work to drive change.

KYOCERA Document Solutions (U.K.) Limited

Eldon Court, 75-77 London Road, Reading, RG1 5BS
Phone: 0118 931 1500

KYOCERA

kyoceradocumentsolutions.co.uk

KYOCERA Document Solutions does not warrant that any specifications mentioned will be error-free. Specifications are subject to change without notice. Information is correct at time of going to press. All other brand and product names may be registered trademarks or trademarks of their respective holders and are hereby acknowledged.