CIO FROM IDG

BlackBerry

Security as a Business Enabler

How to protect and enable your business through information security

Enterprise CIOs are divided when it comes to security. Some find it a big challenge, due to its ever-changing nature. Others manage to harness security as a business enabler, improving their flexibility and productivity and extending their boundaries.

Whatever your stance towards enterprise security and data privacy, these disciplines continue to be of paramount importance, with GDPR looming, data breaches on the increase and more workers going mobile. The question is: how do you balance security and flexibility? Is it possible to secure the organisation, manage risk and meet your information governance requirements but still have the breathing space to innovate?

BlackBerry Security Director, Nader Henein, comments that the latest security technologies will help secure your data - and they can also be a business enabler. However, you need to have the right approach to your information: understanding its financial value and risk, as well as determining other aspects such as its life-cycle – how it begins and ends its life – as well as how it's used and by whom. These things will help you to use security as a business enabler.

Only 13% of CIOs are "very confident" their mobile users are secure.

How conservative is your enterprise?

The main obstacle that prevents organisations from using security to innovate is that many large businesses still have a conservative approach to security, Henein observes. This is confirmed by our research, which found that IT organisations tend to see their employees as a security risk. (For this white paper, CIO, in association with BlackBerry, surveyed over 100 CIOs and IT decision-makers from companies with 500+ employees across the industry sectors.)

The highest security concern for over two fifths of respondents is mobile user carelessness or error, more troubling than an external cyber attack on the corporate IT/communications infrastructure. In fact, only 13% of CIOs are "very confident" their mobile users are secure. A fifth say they are "not very confident".

This leads on to the finding that businesses are generally more comfortable strongly locking down corporate-owned mobile devices (43%) than offering BYOD (14%), CYOD (6%) and CLEO (corporate- liable, employee owned: 4%).

With the industry hype surrounding those more flexible options, it's perhaps surprising that fewer enterprises in our sample are comfortable with them. However, it indicates the perceived trade-off between security, on the one hand, and flexibility, choice and greater digital access on the other.

Tensions rise between employees and IT

The problem is that employees want more. The requests that survey respondents hear most from mobile users are: for "better usability from the apps the business offers them", followed by "a better range of apps from the business". Users are also asking for "freedom to choose their own mobile devices or apps"; with many also wanting "better productivity from their mobile business apps".

Consequently, a number of enterprises experience some degree of tension between employees and IT, as workers find their company mobile devices and apps restrictive and frustrating. One survey respondent complains, "everyone wants a smart phone", with another saying, "users want these new mobile apps quicker than IT can provide."

Another IS leader comments, "users want more functionality, meaning a security compromise needs to be reached." There was also an observation that, "staff do not appreciate or understand security, so see it as a burden," with another experiencing moderate tension from employees: "pressure for BYOD but poor end-user understanding of risk."

It's worth pointing out that many enterprises maintain a healthy balance between employees and IT staff, with some saying there is no tension at all, or their workers are fine with the level of mobile security. Others note that any tensions are monitored and addressed through service improvement.

Why it pays to prepare for GDPR

Another major issue large businesses are having to face is the forthcoming General Data Protection Regulation (GDPR) legislation. Significantly, many organisations are not prepared to meet the regulatory compliance standards for GDPR – or other incoming regulations such as MIFID 2. A sizeable minority, 41% of CIOs, say they are not very prepared, compared with 46% who are relatively prepared, and only 6% who are fully prepared.

Companies that have a strong understanding of personal data are generally at a good starting point with regard to GDPR

GDPR protects the privacy of individuals in the EU and will apply to any organisation providing products and services to EU residents regardless of where a company is located around the world. The personally-Identifiable Information (PII) protected by the legislation could be anything from a name, a photo, an email address, bank details, social networking posts, medical information, or IP address.

Consequently, the security and privacy controls and procedures you need in place to locate, track, anonymise, and erase data need to be granular and comprehensive, in order to comply with GDPR and avoid the well-publicised sanctions and fines.

In the report "Ready or Not? GDPR Preparedness across Vertical Industries", IDC analyst Duncan Brown comments, "how are companies approaching GDPR? In many ways, the answer depends on their starting point. Companies that have a strong understanding of personal data throughout the organisation, with rigorous data management processes and controls, are generally at a good starting point with regard to GDPR."

Brown continues, "Companies that have been less focused on personal data, and have been loose in their adherence to existing laws, will struggle."

A chance to re-architect information governance

For some companies, says Brown, GDPR represents the chance to re-architect their information governance regimes. "The motivation for this could be a desire to operate efficiently and cost effectively, or even to create competitive advantage by processing customer data appropriately. For other companies, GDPR is a chore, a distraction from other business priorities that must be addressed, but with the minimum effort."

Regarding mobile working and devices, GDPR preparation throws a spotlight on how well the company is securing, among other things, its endpoints, data in transit, and mobile access. It raises the spectres of financial and reputational damage to the enterprise if an unprotected laptop or smart phone were to go missing.

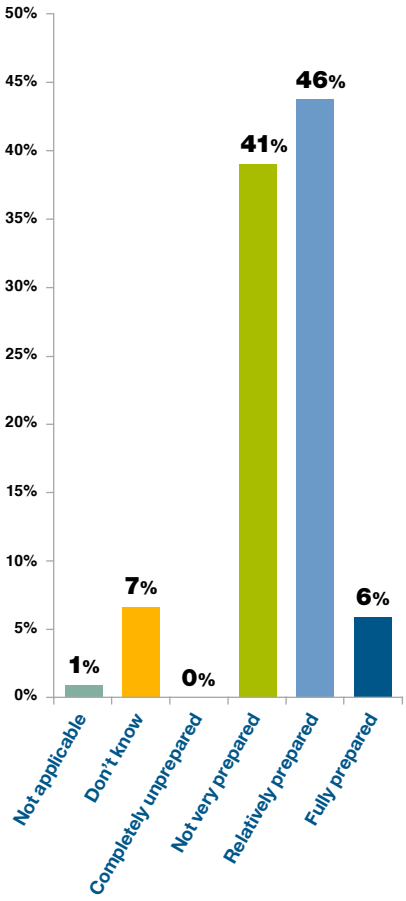
Interestingly, reputational damage is by far the greatest concern in the event of a security breach, cited by two fifths our survey respondents. CIOs consider this more alarming than losing valuable customer information, loss of competitiveness, or regulatory penalties, despite the likelihood of GDPR fines to be punitive. No doubt many IT leaders believe the fallout from reputational damage can affect customer, shareholder and industry confidence which could have a catastrophic financial effect on the enterprise.

How security can be used as a business enabler

Despite many large businesses being unprepared for GDPR, or serving their employees satisfactorily with mobile technology, senior IT decision-makers recognise that security could enable their businesses for a range of purposes.

According to the survey respondents, the biggest reason to enhance mobile security would be "to improve compliance with data regulations such as GDPR and MIFID". Moreover, CIOs identified a range of other ways in which security can be an enabler. These are, in order of popularity: to "provide the foundation for deeper integration with other business applications"; "extend the security perimeter to allow more people to use their own devices"; and "allow the business to offer

How prepared is your organisation to meet the latest regulatory compliance standards such as GDPR and MIFID 2?



users apps that give them greater productivity and flexibility".

Other benefits identified by respondents were: "enhanced mobile security can help enable employees to use personal and business apps securely on the same device"; and "enable the organisation to build more apps to mobilise more processes".

On that latter point, secure mobile technology can help businesses to innovate the way they work, particularly when security and collaboration are part of the same solution and incorporate new technologies. This can enable new use cases, especially mobile ones.

"With BlackBerry Secure, we feel we can confidently provide a framework for our customers to ensure information is shared within a secure and privileged means."

Peter Humphries, CEO, Secure Sense

Secure mobile and remote collaboration

An example of this is BlackBerry's Workspaces. The secure file sharing platform replaces disparate and insecure file sharing through email and popular consumer file sharing apps. Workspaces includes the ability to edit documents on a mobile device within the secure app. This is not possible to do securely if the document is opened in a standard, unprotected file editor.

Moving forward, mobile and remote collaboration remains an area full of potential but also risk. And as more businesses outsource administrative and other functions – such as HR and payroll - the challenge of secure collaboration becomes more pressing. A survey of risk management professionals from Ponemon Institute found that nearly half of respondents indicated their organisation had experienced a data breach caused by a third-party vendor, and 16% were uncertain whether or not they had.

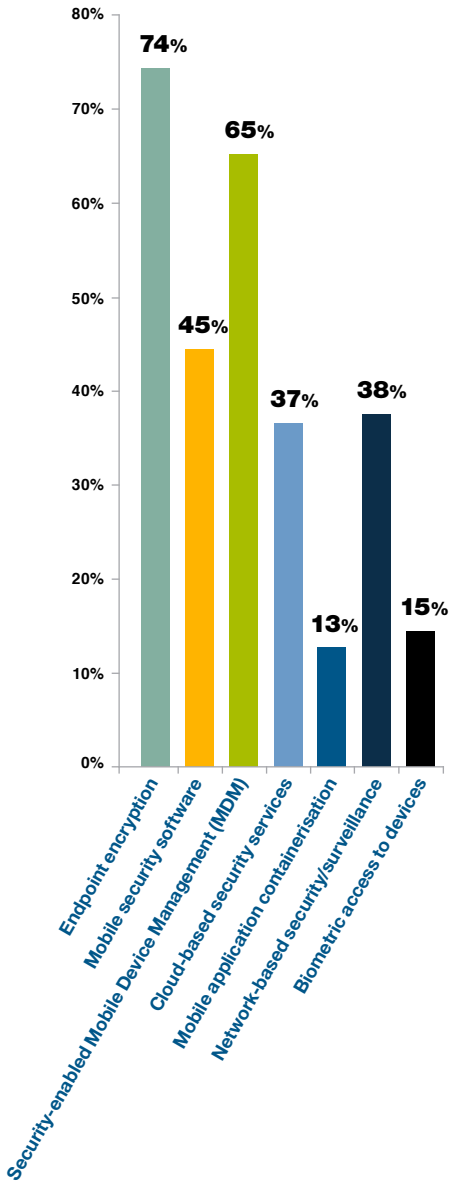
To address this, Workspaces features digital rights management (DRM) technology to protect enterprise data if it becomes compromised by a third party. For example, it uses granular file controls to dictate whether a user can access, view, copy, print, edit, download, or forward a file. File expiration and tracking tells you where, how, and by whom a file is accessed, and can set it to expire after a set period of time. And you can incorporate customisable watermarks on a document, with details such as a user's name, email, or IP address. So, if a document is leaked, your administrators will immediately know who is responsible.

Enterprises are also looking at ways to store and secure their mobile voice, video and messaging, driven by regulation and a rise in mobile and web app usage. This is a feature of BlackBerry's BBME SDK, which can serve as a business enabler by allowing more secure collaboration and productivity.

Tools like Workspaces and BBME SDK can enable enterprises to use security as an enabler for the business, allowing them to confidently extend their boundaries.

Endpoint encryption is the most widely used security technology

Which mobile security technologies are you currently using?



An arsenal of innovative mobile security tools

Enterprises are currently using a range of mobile security technologies to innovate or transform the business, our research discovered.

Many are building bespoke apps, with one CIO saying mobile security is a "lever for the organisation to provide new, feature-rich, but secure native applications". Another senior IT leader comments that their organisation uses "bespoke apps to take paper out of court processes and to streamline processes". Another says that for them, mobile security means: "Mobilising staff, delivering improved customer service, reducing staff numbers, and cutting costs".

Several use application containerisation technology to enable mobile workers to have secure mobile applications. Mobile device management (MDM) is also being used to control and track devices; with encryption to secure devices and media.

When it comes to securing access, some enterprises favour multifactor authentication; with one respondent saying mobile security is "reducing barriers to engagement; for example, biometric authentication can add another level of security, but also improve the user experience".

Securing the perimeter

Rather than merely locking down the enterprise, one IT professional notes, "Mobile security will allow us to take better control of our perimeter and the apps available to users operating within our perimeter."

Adequately securing the mobile perimeter was a point of contention for some of the IT decision-makers we questioned. Perimeter security is either difficult, or an ongoing challenge for almost a quarter, with comments including: "the constant change makes it difficult"; "It's ever evolving, requiring constant investment"; and "Our largest issue is data crossing the perimeter."

However, for the majority, maintaining mobile perimeter security was easy, with endpoint encryption (74%) and MDM (65%) being the most popular security technologies. MDM, cloud-based security and biometric access to devices are seen as major adoption areas over the next three years with CIOs seeing a vital need to better secure their endpoints.

BlackBerry advises enterprises to consider using security that travels with the file, so they can extend their security beyond the existing perimeter and outside the firewall - wherever the file travels. This is a feature of Workspaces. Its file-centric DRM, file tracking, and digital watermarks can be used to thwart intellectual property theft, and data leaks.

BlackBerry adds that it's worth noting security is not just about intrusion and endpoints, especially when you are talking about collaboration and productivity. File-level security provides an extra level of protection even when firewalls are breached and files are hacked using malware and ransomware attacks.

Understanding information value and risk

BlackBerry's Security Director, Nader Henein, observes, "Perimeter defences exist to address certain types of attack. But they're not exactly infallible, and they're hard to manage if you're a large organisation. The best way to use security to enable the business and prepare for GDPR is to audit and understand the information you have, and determine its business value and risk."

BlackBerry's Cybersecurity Consultancy approach begins by helping an enterprise to carry out a comprehensive audit of all the information

Henein adds, "being risk averse is symptomatic of not understanding your information environment well enough. It means you are taking a conservative view of data security, beyond what you need to: it gets in the way of doing business."

He explains that BlackBerry's Cybersecurity Consultancy approach begins by helping an enterprise to carry out a comprehensive audit of all the information it holds across the organisation. The next step is to understand and categorise the information, adding meta data - which could be related to its content, importance or creator's identity or IP address.

BlackBerry then helps the enterprise to attribute annualised revenue and risk values to its information: the "dollar value" it could generate in terms of revenue, and the "dollar risk" in terms of fines, recovery and reputation if it's compromised. "You need to ask: what is the value of my files? If you can't answer the question you're probably spending too much money," says Henein.

The final stage is to ensure the company can adequately secure the right data, retain what it needs to for compliance, delete extraneous data, and justify the cost of storing the rest.

Henein believes that CIOs are in the best position to view the business data holistically and develop a "Risk Register" and a "Breach Bible", documenting the enterprise's information processes and governance. Equally important, they can see where additional value can be created across the business.

BlackBerry is working with a large global apparel and sportswear designer which uses BlackBerry Workspaces to successfully mitigate its risk and improve its information governance and security. The business uses the secure file synchronisation and sharing platform on factory workers' iPads. When they need to consult a design document, they do so through Workspaces which allows the business to apply several layers of protection to their intellectual property: including authentication control, logging and tracking, and dynamic, onscreen watermarks. Additionally, access to each design document expires automatically at the end of each working day. So even if an employee took an iPad home, they'd be unable to access any sensitive files.

In another example, Canada-based health informatics startup Oculys uses BlackBerry's BBME SDK secure cloud platform. It enables remotely-located care providers to communicate and collaborate securely; protects healthcare information; and enables Oculys to comply with HIPAA healthcare data privacy legislation.

The right tools for the job

There is no doubt that security can be a business enabler for your enterprise, and it's possible to have effective security with the flexibility and productivity businesses and employees both want. With the right information strategy in place, products such as BlackBerry Workspaces, BBM Enterprise, BBME SDK, and Unified Endpoint Management (UEM), can enhance your security and assist with GDPR compliance.

The key is to understand the value and risk of your information, and then secure it appropriately with the right tools and technologies. As a result, you can move quickly towards GDPR compliance, with data privacy and security being your market differentiator.