Data security:

How to keep your IP safe

The importance of data security

Every business is reliant on its data. Whether proprietary information about upcoming products, important legal or financial records, or customer details stored in a CRM database, the very survival of a business depends on its data remaining accurate and safe from intruders, both from within and outside the company.

With cloud computing, mobile devices and the emerging Internet of Things creating increasingly sophisticated security concerns, no business can afford to put its data safety on the back burner. A recent Symantec study found that data breaches due to malicious or criminal attacks now cost Australian companies an average of AU$175 per compromised record – and that Australia now leads the world in total number of records compromised per breach, at 34,249.

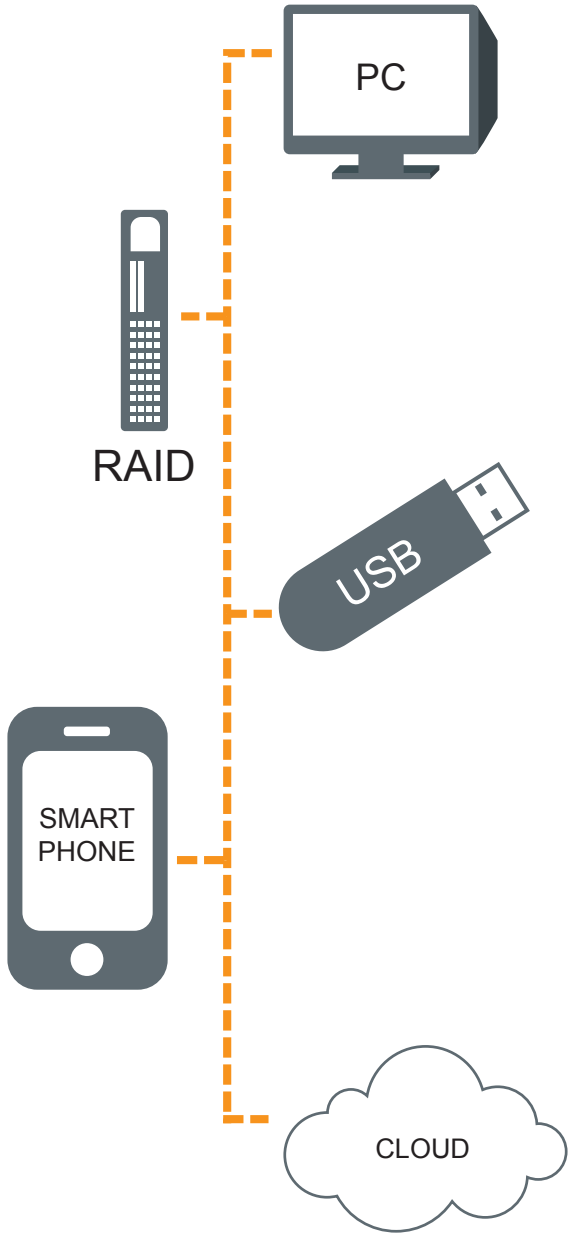
In this e-book, we take an in-depth look at commercial data security, including the threat and impact of cybercrime, the latest mobility trends and why mobile computing requires a seismic shift in how business leaders think about security. We also explore data-storage options in the cloud and identify some best-practice tips that businesses can use to keep their data secure and protected.

A brief history of data-storage security

Ever since textile manufacturers used punched cards in the 19th century to control textile looms, the ability to store data within a physical medium has been a key driver of the modern age.

Over the last three decades, storage capacities have increased exponentially as the cost of media has plummeted. Portable flash-based USB drives, smartphones and music players can carry as much data as high-end PCs did just a decade ago, and at a fraction of the price. And starting with the introduction of RAID storage in 1987, devices have become far more robust and reliable.

On-demand access to data has also advanced – most notably in line with the growth of data networks and the internet. While this has benefited knowledge-based enterprises immeasurably, it's also opened up a whole new area of business risk. With their data exposed like never before, it's time for businesses to get serious about their data security. They must think of it as not just a supporting function, but as a fundamental concern that directly impacts their ability to deliver to their customers.



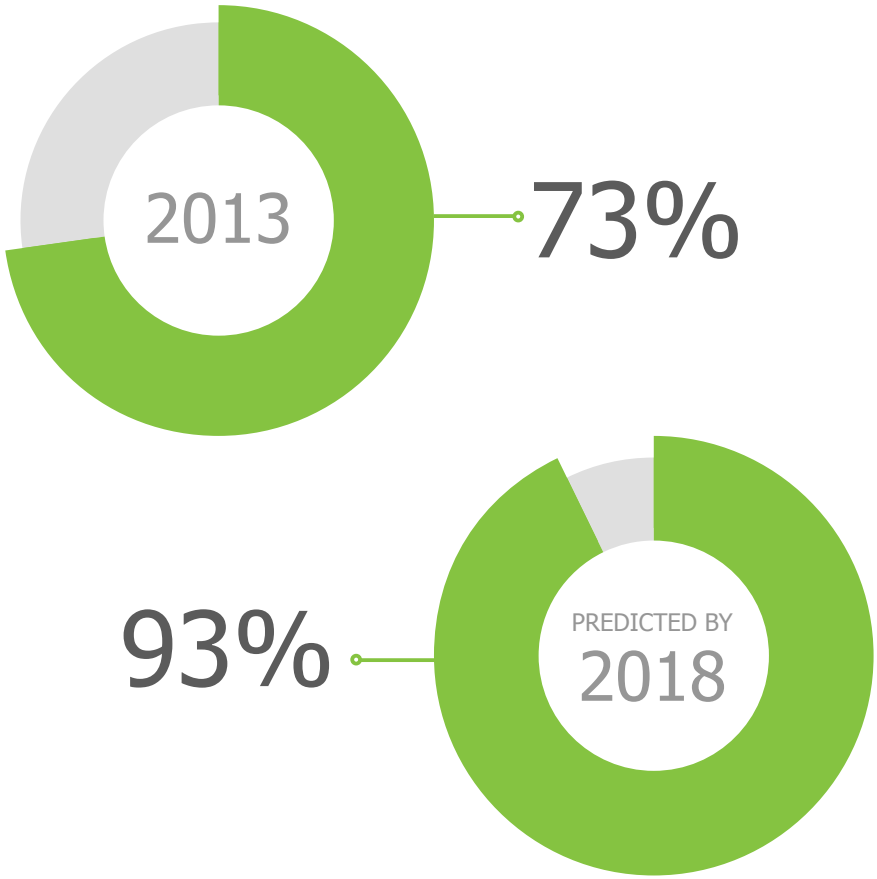
Emerging threats: Mobility trends and cybercrime

The desk-bound worker is becoming a thing of the past as more workers opt for remote and flexible working arrangements driven by the proliferation of mobile devices and wireless internet. This should be no surprise, with a Frost & Sullivan report finding that Australia's smartphone penetration in 2013 was at 73 per cent in the 15-to-65 age group, and is predicted to reach 93 per cent by 2018.

Bring your own device (BYOD) is a practice that can work wonders for productivity, but from the viewpoint of an IT manager, it can also be a serious security headache. BYOD strategies potentially mean having critical business data present on an unknown number of mobile devices that are outside company control. The risk goes beyond data breaches – just one misguided tweet or Facebook update can damage a company's reputation.

To mitigate this threat, IT managers will need to advocate a clear separation of personas or roles on employee-owned devices. They must also ensure that employees are informed about the risks of accessing cloud-stored data through unsecured wireless networks in public hotspots, such as cafes and airports.

Australia's smartphone penetration in the 15–65 age group



Emerging threats: Mobility trends and cybercrime

According to Nick Savvides, senior principal systems engineer (security) at Symantec, the human factor is vital.

"BYOD security can be significantly enhanced by making security simple for end users to use. Mobile-application management, used to control the use and flow of mobile data, can help secure the data while providing the user with the freedom to use their device as they wish.

"Further security benefits can be obtained by using strong public key infrastructure that enables secure authentication on Wi-Fi, VPN and, importantly, Exchange ActiveSync services. This adds assurance that only authorised BYOD devices are connecting to those services."

Top security threats

- The Heartbleed bug: Heartbleed is a flaw in the commonly used OpenSSL cryptographic protocol that allows hackers to steal password details used in secure web communications. Users can check whether a site is still vulnerable to Heartbleed by pasting the URL into this Heartbleed test.
- Phishing scams: The practice of phishing – where users are lured to a malicious website and tricked into handing over personal details – is still a serious security threat. Users should never click on unknown or suspicious links received via email, especially if they request online banking details or other financial information.
- Ransomware: An example if this type of malware is Critoni, which encrypts all your data files and asks for a ransom to release them. Make sure your antivirus software is updated with the latest definitions, and regularly back up critical data.
- Mobile malware: The McAfee Labs 2014 Threats Predictions report found that new PC malware growth was relatively flat, while new Android infections grew by 33 per cent. They also predict an increase in ransomware attacks targeting mobile users. With BYOD here to stay, it is imperative that companies put comprehensive device-usage policies in place.

Data-storage options and the cloud: Risks and benefits

Storage arrays and devices may have gone down in price in per-unit terms, but for many small and mid-sized businesses, the hardware and software can still be an expensive outlay. Add to that the cost of renting storage space, and the time and labour required to keep it maintained, and it's easy to see why data security often becomes a secondary concern, or is neglected altogether.

Cloud-based storage offers a way around these problems. The infrastructure is purchased and maintained by a third-party provider that sells access to the storage, usually for a monthly fee.

Of course, migrating to the cloud doesn't come without risks. You are handing your data over to a third party, so it's important you check the service agreement to ensure it won't be used for unapproved purposes. It's also worth checking that the provider offers the response time, availability, recovery time and service capabilities that you need to run your business effectively.

Savvides says that organisations also often overlook the authentication mechanism used in cloud applications.

"When evaluating a vendor's security, it is important to understand how you will be using that vendor and always keep in mind that although the cloud vendor is providing the service, the business still owns all the risk," he says.

"Organisations should look for comprehensive security policies that can be independently verified. Vendors offering native two-factor authentication, or the ability to exclusively use federation technologies like SAML with two-factor authentication, enable businesses to adopt cloud applications with a greater assurance that only their users have access to the cloud data."

You should also ensure that vendors comply with international ISO security standards, such as ISO 27001 (Information security management) and ISO 20000 (Information technology - Service management).

Data-storage options and the cloud: Risks and benefits

Cloud-based storage delivers multiple benefits:

- Because the customer doesn't have to make a large initial investment, the risk associated with choosing a storage solution is significantly reduced. As a result, it becomes more of a business decision than a financial or technology-based one.
- Typically, the cloud can be accessed from any location, from any networked device with the right security credentials. This extra flexibility is essential for mobile workers and managers who need to make decisions away from the office.
- The cloud can give the customer access to data backup and disaster-recovery capabilities that would otherwise be too complex or expensive to implement.
- The more reputable business cloud providers can also offer robust data security features, such as two-step verification and mobile user authentication.
- In addition to storage, some platforms offer in-cloud applications that provide users with advanced data capture, management, search and retrieval capabilities.

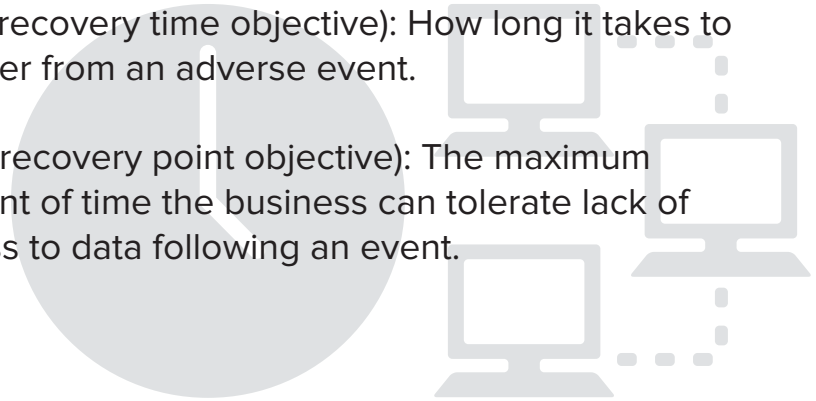
Best practices to secure and protect your data

01 Do a business-impact analysis on your data

While it's true that all the data used within a business is important in some way, it's also true that some data is more important than others. If sensitive financial data, or software code for an upcoming product, falls into the wrong hands, you potentially have more to lose than if a few emails between support staff are compromised.

Conducting a business-impact analysis on your data can help you determine the level of protection that should be applied to each class of data, how often it should be backed up and how long it should be stored. Metrics to consider include:

- RTO (recovery time objective): How long it takes to recover from an adverse event.
- RPO (recovery point objective): The maximum amount of time the business can tolerate lack of access to data following an event.



02 Run a 'health check' on your security policies

Ask yourself a number of questions while conducting an audit of your security policies and practices:

- Do your policies require that all staff, including management, use strong passwords and change them regularly?
- Have you determined which staff members should be trusted to hold administrator privileges?
- Is the virus, spyware and malware protection on your network up to date?
- Do you keep critical files and folders encrypted?
- Do you routinely erase company data on hard drives, portable devices, SIM cards and other storage media you dispose of or sell?
- Do you have an incident-response plan for dealing with data breaches?

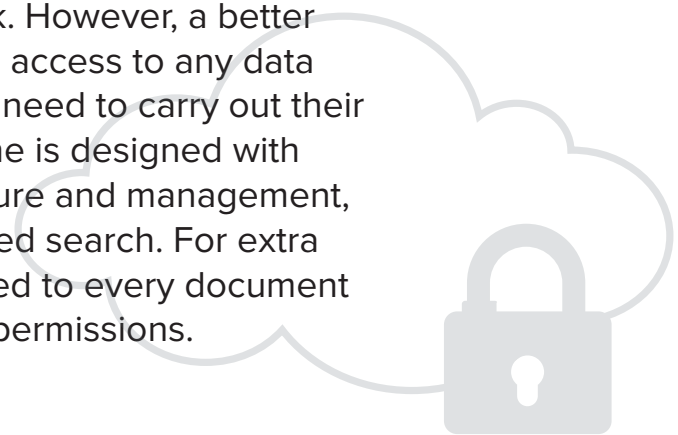
The importance of a regular health check of your data security can't be overstated, with Symantec's research finding that nearly 60 per cent of reported data breaches in Australian businesses are the result of human error, system glitches or process failures.

Best practices to secure and protect your data

03 Secure your storage

The convenience of free online storage solutions, such as Dropbox, makes them popular with business users as well as private individuals. However, they tend not to offer the same level of security, flexibility and functionality as business cloud platforms. This is potentially a huge area of risk for businesses that need to keep their data safe – especially in light of the McAfee Labs research, which claimed that more than 80 per cent of business users use cloud applications without the knowledge or support of corporate IT.

One solution is to block access to non-approved storage platforms from the company network. However, a better approach is to ensure that staff have access to any data sharing and management tools they need to carry out their duties effectively. ThereforeTM Online is designed with this in mind, offering document capture and management, workflow administration and advanced search. For extra security, a digital signature is assigned to every document and each user can be given unique permissions.



Conclusion

The safety of company data – whether it's stored inside the office, in the cloud or on an employee's iPad – can no longer be viewed as simply an IT problem. Entire reputations can now be made and broken on the basis of how secure customers feel handing over their personal information.

As well as making the right tools and safeguards available, business leaders must set an example that others can follow and make strong data security an integral part of company culture.

No one does it like you

canon.com.au/business
1800 444 199

Canon