Data protection:

Not just about personal data and compliance

In this e-guide

In this e-guide:

Despite the focus on data protection, many organisations are still leaving their data wide open for attack through the digital equivalent of leaving the front door open and the windows unlocked from a hacker perspective.

Fortunately, the need to comply with the General Data Protection Regulation (GDPR) from 25 May 2018 and planned UK legislation designed to align perfectly with the GDPR is likely to drive most companies handling EU citizens' data to reassess their data protection capabilities, particularly in relation to personal data.

However, the need for every business to pay attention to data protection is underlined by the fact that data breaches have been shown to have a direct correlation to falls in share prices, sometimes wiping off tens of millions from the market value.

Data protection is not only important from a compliance and business value protection point of view, it is also key to fostering

In this e-guide

the digital economy and gaining a competitive edge, according to UK information commissioner Elizabeth Denham.

Failure to protect and handle data correctly can also result in punitive actions for companies participating in the digital economy, as Google found out recently when a consumer protection organisation in Denmark asked the government to investigate allegations that Google is breaking privacy laws by not limiting how long it stores personal data.

As companies move increasingly into the cloud, it is important that they adapt their data protection strategies accordingly, but at the same time, experts say enterprises should not forget tape storage when it comes to data protection, nor should they overlook cloud storage because of the agility it affords.

However, before launching into cloud-based storage, there are several key questions organisations need to ask to ensure that a cloud-based data storage and protection strategy is right for them.

Warwick Ashford, security editor

In this e-guide

How UK organisations are leaving themselves open for cyber attack

Warwick Ashford, security editor

Organisations such as UK phone and broadband provider TalkTalk claim to take security seriously and have made significant investments in cyber defences, and yet still fall prey to data breaches.

The reason is that organisations, including large and well-resourced ones, are failing in several key basic areas, according to former hackers Cal Leeming and Darren Martyn.

Leeming is a security advisor and risk mitigation professional, but in a previous life he was the UK's youngest convicted hacker after he was arrested at 12 years old for hacking.

Martyn is a security researcher and engineer. After being arrested in 2012 for his involvement with hacking group LulzSec, he went on to use his skills to help protect companies across the world.

Basic failings expose most organisations to cyber risks, they told Computer Weekly, citing the fact that the TalkTalk hackers used a SQL-injection attack, which is a well-known technique, as an example.

One of the biggest problems, however, continues to be compromised passwords, says Martyn, who breaks into organisations as part of enterprise network security assessments.

The easiest way into any organisation, he says, is to search for people's usernames and passwords online from previous breaches and trying them in their work environment.

"You don't need to do anything complicated or fancy when someone in the organisation somewhere has re-used their work password on LinkedIn or MySpace with a leaked database out there," says Martyn.

"If a business is sufficiently large enough you are going to get in. There is nothing spectacularly complicated required."

Once an attacker has a valid password, they are able to bypass any firewall or other security system because they have the same access to corporate systems as the employee they are impersonating.

Phishing for passwords

Another easy way in with unfettered access to corporate networks, applications and systems is to use a phishing email to trick employees into revealing their usernames and passwords.

In this e-guide

"It is simple stuff. If you send a phishing email to every single employee, you are going to get in, that is pretty much guaranteed. From an attacker's point of view, that is usually the cheapest and easiest way to go about things," says Martyn.

Default credentials are another golden opportunity for attackers. Organisations routinely install new kit such as routers and switches but fail to change the default passwords set by the manufacturers. They do not realise that these default passwords are easy for attackers to find with a simple internet search.

If further credentials are required, hackers will typically capture password hashes (encrypted passwords) from network traffic generated by client applications using the server message block (SMB) protocol to read and write to files or to request services from server applications.

Hackers will then crack those hashes to find the passwords, which can then be used to access more systems and crucially elevate privileges using stolen or cracked administrator passwords.

"Gaining administrative privileges usually does not take long, but if people used something like two-factor authentication and a password manager it would make an attacker's life infinitely more difficult because they couldn't rely on credential re-use and phishing as they would still need the second factor," says Martyn.

In this e-guide

"After [you do] that, then [you can] go about stuff like configuring mail filters to block phishing attempts, but you have to get the basics down first – kill off credential re-use by introducing appropriate policies and technical controls."

Blocking access to corporate systems using stolen credentials is extremely important, but many organisations are still failing to do this, rendering costly intrusion detection systems (IDS) useless because someone logging in remotely using a valid username and password looks normal.

Once hackers have access to legitimate credentials, they typically can make an inventory of an organisation's assets because they are free to move anywhere on the network, due to another common basic failure to segregate networks to ensure only appropriate people can access sensitive data sets.

Many organisations use virtual local area networks (VLans) that not only allow geographically dispersed network nodes communicate as if they were on the same physical network, but also allow network administrators to partition their networks to match the functional and security requirements of their systems. But there is seldom any VLan segregation, says Martyn.

"Flat networks are depressingly common. Few businesses attempt to segregate assets, which is usually because non-IT people typically complain about not being able to access stuff. IT staff tend to take the easier route of having a flat network because there are fewer complaints."

In this e-guide

Overlooked vulnerabilities

A related failing is that few organisations know exactly what their most important data assets are and where they are on the network.

"We often discover that enterprises will protect something such as a client database, but will completely overlook an accountancy server that could provide an attacker access to all sorts of financial and employee information," says Martyn.

"You end up having to explain to them that the attacker will care less about their clients' list than information that will enable them to transfer money into accounts they control. Typically, you have to get across to them where the actual risk is, and that is often different to where the perceived risk is."

Vulnerabilities in commercial applications is also a risk that enterprises typically overlook. Most are unaware, for example, that attackers can abuse some features in Microsoft Outlook and Exchange to install malware on enterprise laptops.

"Outlook's mail rules enable attackers to create malicious mail rules. All attackers have to do is log in to a mail server using stolen credentials, push a malicious mail rule to the server and, when their Oulook client syncs with the server, it will download the mail rule and execute it if certain conditions are met," says Martyn.

In this e-guide

"So you can run code on their computer and completely compromise the end-point device, but a lot of enterprises don't realise this. People are surprised when I use this method to get into places. But essentially I am just using a feature of Outlook, which is just one of many interesting, poorly thought-out functionalities in business applications."

To identify and mitigate or avoid these risks, he says some form of security testing should form part of any enterprise software procurement process. Enterprises should look for features that are, in effect, security vulnerabilities and go back to the supplier to find out if that functionality can be fixed or at least turned off.

In the future, Martyn would like to see the introduction of a quality assurance symbol for business software that provides purchasers an assurance that the product has been rigorously tested and does not have any obvious vulnerabilities that can be exploited by attackers.

"Enterprises need to start treating the security side of it as a minimum requirement in the same way they treat functionality. Security should be one of the things that they look at when deciding whether or not it meets their business requirements," he says.

In the past, there has been little or no incentive for enterprises to add cost to the procurement process and risk delays in implementation, but Martyn

believes the General Data Protection Regulation (GDPR) will help in this regard.

"The GDPR may be enough of an incentive because the penalties for breaches are so high, which may be enough to encourage companies to spend the extra bit of cash and time during the procurement phase to validate that stuff is at least somewhat secure to avoid more pain later," he says.

Customised code ignores security

But commercial off-the-shelf applications are not the only software security challenge. Many organisations are commissioning customised code or creating it themselves, but with little or no regard for security.

"A lot of the time these software development teams are not following good practices or standard practices, and they are typically rushing this code into production," says Leeming.

"Devices and services for the IoT [internet of things] is a good example of an area where everyone is jumping on the bandwagon and putting a computer on everything, but not really thinking about the security behind it," he says.

Leeming says the problems are "very simple" and can be fixed by following good procedures, but software development teams cut corners and skip procedures.

In this e-guide

"Often companies get people straight out of training to write the code and end up in the situation of the blind leading the blind, which is a big problem, especially with IoT. The reason that Mirai botnet was able to infect so many IP-connected devices is because simple mistakes were made from a software engineering point of view," he says.

Any organisation developing custom software should encourage employees to learn from the best. "This can be done online. There is a lot material out there: entire courses available for free that will show how to get good quality code and avoid the common mistakes."

Martyn continually emphasises the importance of getting the basics right, and cautions against the temptation to fix the problem by investing in yet more security technology.

"I go into big places and they tell me they have spent a load of money on some kind of firewall or IDS [intrusion detection system]. It is usually an absurdly expensive one with a support contract that will probably have some words like 'machine learning' or 'anomaly detection' in the marketing material."

The problem is that organisations are buying these products in the belief that they will take care of all security requirements.

"They are buying a false sense of security; they are buying a box they think they can plug in that makes the problems go away – but they haven't solved any of the trivial problems such as employees clicking on malicious link-embedded emails and using the same password everywhere," says Martyn.

AV offers false sense of security

Around 99% of antivirus (AV) systems provide a false sense of security, according to Leeming, but he says while AV is unlikely to offer protection against truly targeted attack, a "good AV" will stop most common or broad opportunistic attacks.

A common mistake many organisations make is to believe that AV will protect them from all threats and that all AV software is equally effective.

Leeming, who once ran his own hacking group and broke into thousands of company networks across the UK, advises businesses to choose the AV they use based on rating on sites such as AV-TEST, which releases a benchmark of the performance of products every six months.

These benchmarks enable companies to weigh how much a particular product slows down a computer against the protection that it provides and what it costs.

Although it tends to be the same AV products in the top three, Leeming says it does change and companies should review their AV regularly. "If the AV they are using has dropped down, they should consider replacing it.

According to Leeming, there is "a lot of junk out there" and so in choosing AV or any other security product, he says businesses should do as much research as possible online by looking at the comments and reviews.

"Do your research and come to your own conclusion based on your analysis, taking into consideration what other security professionals are saying about it," he says.

Test security systems before you buy

When it comes to new security technologies, Martyn cautions organisations to be wary of claims about things such as anomaly detection capabilities and use of artificial intelligence (AI) and machine learning.

If suppliers making these claims want people to take them seriously, he says they should be willing to allow people in the security industry to take a look and test how well it works.

"A demo of their pretty user interface, a couple of testimonials from their customers and their marketing spiel does not tell me anything about how well it works," he says.

In this e-guide

Martyn advises against investing in any security systems without formal testing or verification that shows the product in question works.

He also underlines the importance of having the technical capability to detecting intruders on the corporate network, which many organisations are still lacking.

"You are never going to have 100% prevention. You are never going to block every attacker. If someone really wants to get in, they will – especially when it comes to state-sponsored stuff."

Martyn says the more time and effort required by the attackers to get in, the more likely it is that they will go somewhere else that is easier to hack.

"Raise the barrier as much as possible so that it takes some effort and an investment in time and resources to get, but also make sure you have stuff for detecting a breach early and responding to it," he says.

"If you have solid detection and response capabilities then you are pretty much golden. If you can flag that something bad has happened and kick the attackers out of the network, then you are good.

"But most organisations are unaware they have been breached for weeks, months and even years. Quite often they find out about a breach only a third party tells them. It is a sorry state of affairs," says Martyn, adding that many

organisations still lack basic intrusion detection and incident response capabilities.

A common reason that organisations' cyber defences are poor is that there is no executive support for cyber security.

"When the IT of the business brings in outside companies to conduct penetration tests, they are often using the test report as leverage to force people above them into giving them budget to implement security controls," says Martyn.

"In enterprise, you often have a relatively small IT team and the rest of the business tends to assume the IT people do 'IT stuff' and don't really need a budget," he says.

"Business people often do not understand what the IT team does and typically do not see them as the people responsible for guarding the company's intellectual property."

From experience, Martyn says it is only when management understands that those responsible for IT security keep critical business data safe that companies adopt a better overall security posture.

Corporate culture one of 'the biggest failings'

Corporate culture is a big part of good cyber security, according to Leeming, who sees it as one of the biggest failings.

"If you've got a bad culture it does not matter how good your processes are, you are going to have employees that just don't care. When you have employees that don't care, it doesn't matter how good your equipment is because you are going to have problems," he says.

At the core of the security problem is the fact that humans are fallible. "There is always someone who is going to be on the take that you can get information from. Although some organisations are using behavioural analysis, these systems are not foolproof and can be bypassed," says Leeming.

A poor corporate culture, he says, is typically the result of poor leadership and an emphasis on productivity and profit over job satisfaction.

"If employees are underpaid, undervalued and working for a company simply because they need to pay bills rather than for love of what they are doing, security is just going to fly out the window."

Leeming says Glassdoor, a website that shows employees' thoughts about the company in an anonymous fashion, shows a clear correlation between

companies with a poor culture and those that have a track record for terrible security.

He also emphasises the importance of ensuring that employees get regular security training to ensure they have a good understanding of security systems and processes. "You can't just plug in a black box and have good security without the team and training around it."

"â€‹It is a lack of understanding at all levels about what security really means that is holding most organisations back from ensuring that the basics have been done and that they have been done properly," says Leeming.

Cyber security seen as 'chore'

Leeming believes that because of all the recent hype around cyber security, companies and individuals are becoming de-sensitised to the phrase "cyber security".

"People see cyber security as a chore and don't understand that cyber security is not just about keeping your machine secure, it is also the impact it will have them, their company or their team."

Instead of saying "don't reuse your passwords", he says it is important to use terms that people will understand more easily.

"Instead, say, 'If you use your password on website A and reuse that password on website B, if website A gets hacked the hackers will also get access to your account on website B'," says Leeming.

"Then help them understand the true risk by considering the data they enter, store and share using online services and pointing out that all that data can be accessed by the hackers and used against them.

"It is about putting it in words and context that makes sense to them, but that is a very difficult thing to do as a mass broadcast."

Leeming says this is easier to do in small groups, spending time with people to talk them through the risks.

"Unless someone is really interested in what security means to them, it is not going to click in their heads no matter how much passive content you expose them to, such as posters, because they are not engaged. So far, the only way I have seen to do that is to have small groups and do it on a one-to-one basis."

Goverment heading in 'right direction'

Although Leeming believes there are currently few really effective security technologies that are accessible to smaller companies, which lack the money and expertise of larger organisations to buy and run state-of-the-art security systems, the message is clear for all companies of all sizes.

In this e-guide

Leeming and Martyn say it is almost pointless worrying about advanced cyber security attacks before taking care of all the basic things that attackers will look to first to get easy access to corporate networks.

On a positive note, they recognise that the UK National Cyber Security Centre (NCSC) is doing good work in engaging with businesses and providing useful guidelines on how to improve cyber security.

"We are not there yet, but from the results they have shown from the small amount of time they have been operating, I have high hopes. The government is finally going in the right direction," says Leeming.

From the perspective of two former hackers who are now practising those same skills on the right side of the law, the message is clear: not every organisation will be hit by the lastest, most sophisticated targeted attacks, but most are leaving the door wide open to the simple hacking techniques used by the majority of attacks that could hit any business to steal money and data.

Quick security wins

- Leeming and Martyn say following simple guidelines will enable enterprises to greatly increase security and avoid the majority of fairly low-level attacks.
- Educate employees on using a password manager and mandate their use in the security policy.

- Introduce a robust password policy to ensure passwords are strong, unique and changed frequently.
- Introduce two-factor authentication to stop attackers using stolen credentials.
- Educate employees not to open untrusted attachments or download untrusted software.
- Ensure computers are password protected and locked when not in use.
- Ensure Wi-Fi is secure using the WPA2 security standard.
- Mandate encryption for essential files.
- Block advertising at the network edge to eliminate malvertising campaigns.
- Disable Flash, Java and macros across the enterprise wherever they are not needed.
- Apply software security updates regularly.

Next article

In this e-guide

Data breaches strip tens of millions off UK firms' market value, study shows

Warwick Ashford, security editor

Cyber attacks on top UK companies are leading to losses of 1.8% of share price or £120m on average, according to a study on the effects of data breaches on share prices.

This has doubled in the past 18 months, according to the report released by global advisory firm Oxford Economics and IT and business process services firm CGI.

The report is based on a study of 65 severe or catastrophic breaches at FTSE 100 companies in the past four years and indicates that investors are now punishing companies more harshly for cyber attacks.

The *cyber value connection* report, which is aimed at helping senior business people understand the impact of cyber breaches on company market value, reveals that investors have lost at least £42bn since 2013 due to the severe public domain cyber security incidents used for the study.

However, the report notes that this figure includes only 65 publicly known severe breaches, which means the true amount of company value lost due to cyber attacks is likely to be far higher.

The report examines factors such as how new regulations for mishandling data will also strongly impact the public visibility of future breaches and therefore how organisations will plan for, manage and report cyber crime as incidents continue to rise.

"Cyber security is a still a top priority for businesses, but business leaders, policy makers and investors still have work to do to take cyber security risk far more seriously," said Andrew Rogoyski, vice-president of cyber security at CGI in the UK.

"We are beginning to see city analysts, venture capital firms and credit ratings agencies factor cyber security readiness into the way they assess firms. This is positive and should encourage boards across the world to treat cyber security as an enterprise-wide risk."

A good example of the effects of data breaches on company value is Yahoo, which was forced to discount by $350m the sale price of its core business to Verizon after revelations of data breaches in 2013 and 2014 affecting one billion and 500 million accounts, and of hackers forging cookies to gain access to customer accounts.

The cost of cyber attacks to investors is likely to skyrocket in the near future, said Rogoyski, as the General Data Protection Regulation (GDPR) and Network Information Security (NIS) directive mean that firms dealing with European citizens' data must disclose all breaches of that data.

He estimates that only around 10% to 20% of the major breaches companies suffer in Europe are currently made public, so lost shareholder value across European markets could rise by as much as a factor of 10 when the new regulations take effect in May 2018.

"We are likely to see a rapid spike in publicly reported incidents in Europe and financial markets will respond accordingly. Company boards should be considering cyber security prevention and preparation as a critical way of protecting the interests of shareholders," said Rogoyski.

Cyber breaches affect share prices

Ian Mulheirn, director of consulting at Oxford Economics, said the study shows a significant connection between a severe cyber breach and a company's share price performance.

"It was found that, on average, a firm's share price was 1.8% lower in the wake of a breach than it would otherwise have been in the week following an attack. However, in some cases the relative share price fall for affected

companies was much higher, with one attack lowering the company's valuation by 15%."

Mulheirn said such underperformance should be viewed as a permanent impact on the firm's overall performance.

"That's because a firm's share price reflects market participants' expectations of future profitability as markets 'price-in' such incidents. Therefore the reaction of a company's share price in the immediate aftermath of a cyber breach should be viewed as representing the permanent effect of the attack on the firm's future profits."

Raj Samani, chief scientist at McAfee said: "This latest research revealing the detrimental impact cybercrime can have on an organisation's market value should serve as a warning to corporations across the globe. Data breaches damage far more than a company's reputation, often hitting the bottom line hard.

"Corporations cannot afford to dismiss cyber security as a problem which just belongs to the IT department. The financial future of a corporation – and often that of its customers – can hinge upon the security of its business and user information.

"As a result, it is crucial for executives, including the chief financial officer and CEO, to take an active role in understanding the level of cyber risk

they're exposed to in order to implement an appropriate, effective cyber security strategy. This process should include assessing the value of the company's data assets and implementing mitigation strategies appropriately proportioned to the level of risk involved."

Making cyber security a priority

Alex Guillen-Estudillo, go-to-market marketing manager at Insight UK, said: "Today's news will hopefully be the wake-up call businesses need to bring cyber security to the top of the boardroom agenda.

"Recent advances in technology mean that businesses now have access to a wealth of data and with that comes a risk they cannot ignore. The research proves that taking a backseat approach not only affects a business's reputation, but it has potentially crippling financial consequences if they do incur a data breach," he said.

Simon Moffatt, senior product manager at ForgeRock, said all organisations should have fully documented data breach plans in place that both minimise risk and enable them to respond quickly and effectively to any issues.

"As more and more services are delivered through digital channels, implementing strong device and person-based identity and access management practices will also be critical," he said.

CGI's recommends eight steps to achieve effective cyber security governance:

1. Appoint someone at board level to be responsible for cyber security with the authority and know-how to address the risks and demonstrate leadership during times of crisis.

2. Include cyber security on every board agenda, reporting on: risk to the business, nature of sensitive data and mitigation progress at a minimum.

3. Treat cyber security as a company-wide business risk and assess as you would with other key business risks such as major safety issues, environmental disasters and accounting scandals,

4. Ensure that the company understands the rapidly developing legal landscape that applies to cyber risk – in particular, begin preparing for the GDPR and NIS directive now.

5. Get specialist expertise to advise and inform the board, whether from internal teams or external advisors.

6. Set a programme of work to manage cyber risk, allowing a realistic time and budget.

7. Encourage discussion about risk appetite, risk avoidance, risk mitigation and cyber security insurance.

8. Assume you have already been breached but you might not yet know about it. Take action to reassure yourself no such attack has taken place, but plan on the assumption that they have.

Next article

In this e-guide

European data protection law to give consumers more control

Warwick Ashford, security editor

The European Union (EU) General Data Protection Regulation (GDPR) will require organisations to make the personal privacy rights of consumers a top priority, said the UK privacy watchdog.

The GDPR, which becomes enforceable by law in May 2018, will give people stronger rights to be informed about how their personal information is used, said UK information commissioner Elizabeth Denham.

The GDPR will bring "a more 21st century approach" to how personal data is processed and that organisations should seize the opportunity to set out a culture of data confidence in the UK, she told the ICO's annual Data Protection Practitioners' Conference in Manchester.

"The GDPR provides more protections for consumers and more privacy obligations for organisations. It aligns with people's expectations for strong safeguards, and recognises the advance of digital services in the public and private sector," she said.

In this e-guide

While the GDPR gives specific obligations for organisations – for example, around reporting data breaches and transferring data across borders – Denham emphasised that the real change for organisations will be understanding the new rights for consumers.

"I want to see comprehensive data programs as the norm, organisations better protecting the data of citizens and consumers, and a change of culture that makes broader and deeper data protection accountability a focus for organisations across the UK," said Denham.

The Information Commissioner's Office (ICO) has the power to impose monetary penalties of up to £500,000, but the GDPR provides for fines up to €20m or 4% of annual worldwide turnover, whichever is greater.

Denham said while the GDPR gives regulators greater enforcement powers, there is a carrot as well as a stick.

"As regulators we prefer the carrot. Get data protection right, and you can see a real business benefit," she said.

"I believe there is a real opportunity for organisations to present themselves on the basis of how they respect the privacy of individuals. Over time, this can play a real role in consumer choice."

GDPR increases consumer control

Strengthened rules around consent will give consumers choice and ongoing control over how organisations use their data, as well as ensuring an organisation is transparent and accountable.

The GDPR will also introduce a duty on all organisations to report serious data breaches to the regulator and, in some cases, to the individuals affected.

Under GDPR, UK citizens will benefit from new or stronger rights, such as being informed about how their data is used; around data portability across service providers; the ability to erase or delete their personal information; access to the personal data an organisation holds about them; the ability to correct inaccurate or incomplete information; and over automated decisions and profiling.

Post-Brexit, Denham said the UK government will need to answer questions about how the UK's digital economy's need for data to flow across borders will be met and how the UK can continue to foster economic growth while still respecting citizen's rights.

"When the government comes to answer those questions beyond the implementation of GDPR in 2018, we expect to be at the centre of many conversations, speaking up for continued protection and rights for

consumers, and clear laws for organisations. [We will also be] addressing the strong data protection laws we'd need if we want to keep the UK's approach at an equivalent standard to the EU," she said.

Giving evidence to the House of Lords EU Home Affairs Sub-Committee on 1 March 2017, Stewart Room, head of legal data protection and cyber security at PricewaterhouseCoopers (PwC), said the GDPR essentially provides a code for good business practices in handling personal data.

"Stripping out the legal components and enforcement mechanisms, we find in the GDPR a framework that most businesses would agree as being necessary for data handling.

"As far as consumers are concerned, the GDPR gives more rights over personal data, such as greater right to transparency and a greater right to intervene in the operation of business if they have concerns [about their personal data]," he said.

The GDPR also includes mandatory breach disclosure that will help consumers to understand serious incident concerning confidentiality and security, and it acts as a transparency mechanism as well as a mechanism to help those affected mitigate any harm.
Room said in the light of the fact that certainty is important for business, having a "GDPR Act" post-Brexit where the legislation is transposed verbatim is going to be a "significant advantage".

This view is consistent with the UK government view expressed by digital minister Matt Hancock, who faced questions from the same sub-committee in February 2017 on how best to ensure there are unhindered flows of data between the UK and the EU after Brexit.

He told the same sub-committee that the UK will replace the 1988 Data Protection Act with legislation that mirrors the GDPR, saying he was confident that this strategy would ensure the UK achieves its goal of free data flows with the EU post-Brexit.

In addition to GDPR-like legislation, Room said it is also important for the ICO as the UK privacy regulator to remain relevant and penetrative as well as being able to lead.

"We need to ensure that our regulator is sufficiently resourced in terms of skill and capability so that no-one can levy the charge that the [UK] data protection regulation is not working in operations," he said.

Next article

In this e-guide

Danish consumer council refers Google to Data Protection Agency

Karl Flinders, Emea content editor

A consumer protection organisation in Denmark has alleged that Google has broken privacy laws by not limiting how long it stores personal data, and has asked the government agency responsible to investigate.

Watchdog Taenk (Think) has asked Denmark's Data Protection Agency (DPA) to check whether Google's data collection adheres to privacy laws.

A document from Taenk, that has been seen by Reuters, said: "The consumer council Taenk would like the Data Protection Agency to assess whether Google's indefinite data collection complies with consumer's basic right to privacy. We have become aware of the fact that Google today has nine to 10 years of data on users with a Google account."

"We believe that Google generally try to be transparent with respect to the data they collect and, among other things, allow consumers to delete their own data," said Taenk chairman Anja Philip.

"However, in our view, Google collects and stores the information for much longer than necessary in relation to the trades that they can deliver services

and target ads to their customers, and we look forward to getting DPA's assessment of the case.

"What words you search for, and where you are saying, is very personal information so it is not [right] that Google stores indefinite. Besides the obviously uncomfortable [idea] that one's comings and goings in the smallest details are recorded and stored for years, there is a risk that information can be misused by unauthorised persons that gain access to a Google account," added Philip.

In a recent study of 2,022 consumers in Denmark, Taenk said they perceive data about their whereabouts location Google records and stores as "very private".

Next article

In this e-guide

Your enterprise data protection strategy should include cloud and tape

Jason Buffington, guest contributor

There are lots of reasons to embrace cloud services as part of your enterprise data protection strategy. But unless you are an SMB in a nonregulated industry, eliminating your use of tape shouldn't be one of them.

In ESG's recent Data Protection Cloud Strategies report, although most respondents cited an intention to store data in a cloud for one to three years, they had to meet data retention mandates for five or more years. For most organisations, the longer they have to retain data, the more likely tape will continue to play a role in long-term data retention.

Nonetheless, even if you don't reduce your usage of tape, that doesn't make the cloud any less compelling for an enterprise data protection strategy. The power of the cloud lies in *agility*, not the race to bottom dollar per gigabyte stored.

When it comes to data protection and retention, the benefits of cloud-powered agility fall into a few camps, including lowering the potential amount of data that might be lost and being able to do more with secondary data copies. Let's delve into these a bit.

Reduced data loss

While organisations often struggle with "cost of downtime," it's arguably easier to appreciate "cost of lost data" as a simpler and more compelling measurement of effort lost or repeated when data must be recreated. That's because the time needed by workers to recreate their earlier efforts takes time away from new work they should be doing.

IT professionals, meanwhile, often cite recovery point objective (RPO) as a metric for data protection. This can be simplified by presuming "predictable data loss" is one half of the frequency of data protection.

For example, say an organisation performs a daily data protection event (backup, snapshot, replication and so on) at midnight each evening. A server failure early in the morning would result in very little data loss, while a failure at 6 p.m. would result in a full business day's worth of lost data (i.e., eight hours). So, to determine predictable data loss in this scenario, split the difference by assuming all failures happen at noon (midday). The result is a half-business day of predictable data loss when backup occurs on a nightly basis.

According to ESG research, 17% of organisations send data to a cloud on a daily, or nightly, basis as part of their enterprise data protection strategy. While typical of a tape backup process, it's not the most effective way to take advantage of the agility of the cloud for data protection. Fortunately,

users of cloud-based data protection send data to the cloud every two hours on average. For them, predictable data loss decreases from a half day to one hour, decreasing RPO from eight hours -- a business day -- to two hours in the process. That is real ROI!

Data agility

Many can simplify the topic of copy data management down to the rhetorical question: "What else can I do with the secondary and tertiary copies of my data?" After all, it's not unreasonable to presume 10 or even more copies of secondary data exist, resulting from snapshots; replicas created for disaster recovery; and multiple backups across daily, weekly and monthly iterations. And while most of those copies and partial versions may be legitimised for the assured recovery or preservation of business data, they can also be cumbersome and expensive to store and maintain. As such, many organisations need to gain new "value" out of their enterprise data protection strategy beyond crisis preparation.

Some want to run reports or conduct analytics from secondary, otherwise dormant, data, for instance, while others will do patch testing or similar test/dev activities. You can often accomplish these efforts by simply harnessing secondary data storage through orchestration workflows, combined with noninvasive representation data-access methods that do not malign pristine copies that may still be required for data restoration.

While you can accomplish some of these goals through on-premises secondary storage, combining cloud-based compute (on-demand access) with cloud-based protection storage provides an economical and scalable (from instant-on to entirely dormant) set of business outcomes. Essentially, organisations that do the latter recognise the incremental business value of "warm" data within a cloud, something not typically attainable from the "cold" copies of data within tape cartridges.

This is the primary reason why businesses store data in clouds for the short term (one to three years), while still embracing tape for long-term (10 years-plus) retention. The warmer the data, the more agile it is and, therefore, the more useful that data is for purposes other than retention and protection objectives.

Now that we have a clearer understanding of why cloud(s) make sense as part of an enterprise data protection strategy, my next Hot Spots column will explore the key determinants between cloud storage, cloud backup services and disaster recovery services. It'll also explain how those different approaches apply to both on-premises servers and cloud-based production data.

Next article

In this e-guide

How the cloud fits in an enterprise data protection strategy

Jason Buffington, guest contributor

If you've decided to use the cloud as part of your enterprise data protection strategy, but aren't sure what you should do next, I have some questions for you. But first, keep reading.

In my last *Hot Spots* column, I talked about *why* cloud services should be part of your enterprise data protection strategy, alongside (not replacing) disk and tape media. The two most compelling parts of that discussion related to the following:

- Reducing data loss through more frequent replication streams to cloud versus nightly tape jobs.
- Data agility, whereby you can often do more with your "warm" data in a cloud than you can with the "cold" copy of data within a tape cartridge. So, use cloud services for unlocking dormant value within your short-term data, while leveraging the economics and portability of tape for truly long-term retention.

This month, as promised, I want to talk about which cloud services to use for your enterprise data protection strategy by posing four sequential questions.

1. Are you satisfied with your existing backup software platform(s)?

If yes, then you are likely looking to the cloud to add data survivability (without tape couriers) or looking for more economic storage capacity than simple disk arrays. In either case, cloud storage is probably the right place to start. Most modern backup software products provide, or will soon provide, cloud connectors, so they can use cloud-based storage similarly to how they utilise local disk or tapes today. For organsations simply seeking to get data out of the building, cloud storage as another repository within the backup UI makes sense. A huge note of caution, though: Not all backup software uses the cloud effectively. Many products are very cumbersome with their cloud APIs, causing horrific amounts of extraneous data transfers that will blow up your budget.

Speaking of which: If you want more economical storage capacity for your existing backup software, then a local deduplication storage platform that efficiently leverages cloud storage behind the scenes may make sense. Deduplication storage platforms are particularly appropriate when you have multiple backup and archive applications deployed, because the multiple backup software products each talk to the local protection storage disk,

which typically retains the most recent data on site and transparently handles cloud storage behind the scenes. This approach deduplicates data locally, keeps a local copy for fast restores and only depends on one vendor's (the dedupe array) cloud connector for optimal transmission and cloud storage efficiency.

On the flipside, if you are not satisfied with your current backup software, adding cloud storage is unlikely to make it much better. Either buy new backup software and reconsider question number one, or move on to question number two.

2. Are you seeking revolution instead of evolution?

Adding cloud storage to an existing backup environment is evolutionary. Replacing an on-premises and self-managed backup product with a remotely managed product or turnkey backup as a service (BaaS) is revolutionary. And the real difference it can bring relates to expertise, specifically in two areas:

- **Turnkey services** can supplement your backup expertise with that of a service provider's staff -- people who are likely better trained and who focus exclusively on robust data protection. They operate their backup infrastructure at a scale and with a level of reliability only the largest and most sophisticated enterprises can boast. They possess valuable experience accumulated by integrating and supporting many subscriber organisations each year. So, that anomaly that broke your

backups last month but you've never seen before, they've likely worked through it before from helping so many other environments. As such, you should get a better result in the form of more reliable backups and recoveries.

- Alternatively, some service providers and partners will take the backup software you currently run (or a newer version if you are behind) and **co-manage it with you**. This is especially true of providers offering cloud storage, but you get integrator-level expertise alongside the storage capacity itself.
- If you're looking for "better" data protection than what your team is able to manage, budget and skills notwithstanding, look for a provider that believes "service" matters as much as a "data protection" feature set.

3. Where would you like to recover?

Both earlier questions result in a hybrid data protection architecture, with production servers running in your environment, combined with local recovery capabilities (to minimise workload downtime as much as possible and remote copies in a cloud service. Each, meanwhile, presume your desired recovery target is on-premises as well.

Many organisations are asking "Why BaaS when you can DRaaS (i.e., implement disaster recovery as a service)?" suggesting that if you have secondary data in a cloud, could you just power it up in the cloud instead of restoring the data back to an on-premises server? Unfortunately, that

depends on how the data was transmitted and stored within the cloud service.

Technologies that back up data tend to transform data chunks for most efficient retention of multiple previous versions over time. That requires the data to be "de-transformed" (restored) to be usable again, which is often harder to do within many cloud frameworks. Other technologies replicate the data, meaning that it's retained in a relatively untransformed manner, thereby making it easier to simply boot up or otherwise leverage in the cloud.

There are other considerations as well, which you can check out in this ESG video blog, aptly titled "Why BaaS when you can DRaaS?"

4. Will production systems be moving to the cloud?

Although everything changes when production systems move to a cloud service, enterprise data protection strategy options remain surprisingly similar.

When running virtual machines within a cloud-hosting environment, you need to back up those servers with the same rigor that you backed up physical or VMs in your own environment. Perhaps you'll run a virtualised backup server among the other hosted VMs. In that case, you'll want to consider cloud storage (question one) in the same hosted environment or intentionally with

another cloud provider to ensure that your data survives a crisis at the primary provider. You might even run "hybrid in reverse" and replicate your cloud-hosted data back to your own facility for data assurance and preservation.

Alternatively, a backup service (BaaS, as described in question two) can protect data within hosted VMs in the same way it protects your physical and virtual on-premises servers, while providing the same out-of-network retention that bringing data back home might yield. In short, hosted VMs have the same essential cloud options as on-premises servers do.

If you go all in with cloud-based services for production (e.g., Office365 or Salesforce), it will appreciably change your enterprise data protection strategy, because those platforms have fewer protection capabilities across the traditional backup vendors or backup services. But make no mistake, most of those software-as-a-service products do *not* back up your data as part of their service. That is still your job, regardless of it being more difficult.

There you have it, four simple questions with a very wide range of recovery outcomes and ramifications. Perhaps these questions won't yield a definitive answer for you, but they should spark new conversations among your team.

In this e-guide

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 120+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively – and faster – than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; Fotalia