clearswift

Has the enforcer become the enabler?

What the next evolution of Data Loss Prevention technology means for business collaboration and productivity

Dr. Guy Bunker

Contents

Into the eye of a perfect information security storm

Barely a week goes by without reference to the loss of sensitive data. Remember those stories of government laptops being left on trains from yesteryear, has much changed today? How about all those successful attempts to steal commercially valuable or potentially embarrassing information? Think Target, eBay and even the Sony Pictures hacked by Guardians of the Peace, which exposed private corporate emails and damaged Sony's reputation in a blink of an eye.

Consequently, the topic of information security is white hot. But what is driving the information security agenda that you need to be aware of? And can you really enable collaboration and drive productivity using security technologies that have traditionally been seen to do the opposite by locking down business?

Today, three major factors are whipping together to create a perfect information security storm: technology, user behavior and the law.

What do you know about SMAC, or Social, Mobile, Analytics and Cloud? This group is stimulating and enabling new and more agile ways of working, driving communication and collaboration across the enterprise, into partners and customers.

The volume of data flowing through, residing in, and being disseminated across organizations' networks, storage and devices continues to rise dramatically. Unfortunately this also means that would-be cyber attackers have more points within the information flow at which they can attack to exfiltrate data, and organizations have more points of vulnerability. Think BYOD, cloud storage, remote access and hardware-enabled file transfer, such as USB devices and others.

The human factor

Yet, it is the people who use these technologies and their innate human fallibility that poses the most significant threat to information security. Whether malicious or accidental, the damage caused by an information breach can take many forms from denting an organization's reputation to hitting its bottom line. How big that hit ends up being is, in no small part, down to the local and industrial regulatory environment.

Regulators are getting serious

Data protection, specifically information security is something the EU takes very seriously. In fact, new regulations mean that a breach of sensitive or confidential data could result in hefty fines of between 2-5% of global turnover, or up to €100 million when they come into force over the next 12 months or so.[1] Let's face it, no matter if you are big or small, this is an amount you cannot ignore!

In the US, data protection legislation is imposed at both a local and industrial level, with federal about to impose standards across all the states. For example, in healthcare, regulations such as the Health Insurance Portability and Accountability Act (HIPAA) govern access to, and use of, personally identifiable information. In California, operators of commercial websites that keep information about State residents must comply with the California Online Privacy Protection Act, a local data privacy policy.

But it's not just the US and the EU, 2014 saw the Privacy Amendment (Enhancing Privacy Protection) Act 2012 for Australian Companies come into effect. It's an amendment to the Privacy Act 1998 and impacts them – and their international subsidiaries – who store personal customer data either inside or outside of Australia. Should any organization breach the Act, it also provides the Office of the Australian Information Commissioner (OAIC) with the power to impose fines of up to $1.7 million.

How to quieten the storm

So if the way we work has changed thanks to new technology, and new laws are forcing organizations of all types and sizes to take data security more seriously, how can we all prevent the loss of our critical information?

1. Information Age, EU Regulation: Time to Act on EU Regulation, 21st August 2014.

The problem with data loss prevention is...

...Data Loss Prevention

Like many a technology before it, Data Loss Prevention (DLP) has suffered the hype-bust cycle of so many others – think CRM pre-Salesforce.com – and the faltering start of cloud, the most revolutionary technology to never really take off until 10 years after its inception (... but look at it now).

When it first came on the scene many years ago, DLP was touted as the way to ensure critical information wouldn't be stolen, misplaced or misused. But it has struggled. Because it relies so heavily on rules regarding who can and cannot access, send and receive certain types of sensitive information, it was thought complex and taxing for customers to set up and keep up-to-date. The operational costs are often seen as being prohibitive, so much so, that the solution gets switched off or turned down – putting the organization and its information at risk.

In addition, early forms of the technology often yielded too many 'false positives' – in other words, too many of the data breach alerts were found to be wrong, and not a breach at all, but the communication was stopped and blocked. It's clearly evident then, why DLP rapidly earned the reputation as something of a business inhibitor.

Because a 'stopped business' is no good for anyone, DLP was often turned down, but even with refined policies business would still be stopped. Productivity dipped and frustrations with the technology escalated. The commercial imperative of business relies on being able to connect and share information and that wins over security concerns – even at the cost of information security.

In its recent report, Rethinking DLP: Introducing the Forrester DLP Maturity Grid, Forrester gathered qualitative research from US and European businesses. As we can see from the following quotes taken from the report, businesses of all kinds are experiencing challenges with DLP, particularly around value for money:

"We are not getting our bang for the buck... problems happen all the time, and we constantly have tickets open. [DLP] running globally, but mostly used for investigation purposes."

– CISO at an industrial processing company.

"Ours [DLP] is not worth it. I'm not sure if even a great system is worth it."

– VP of technology services at a financial services company.

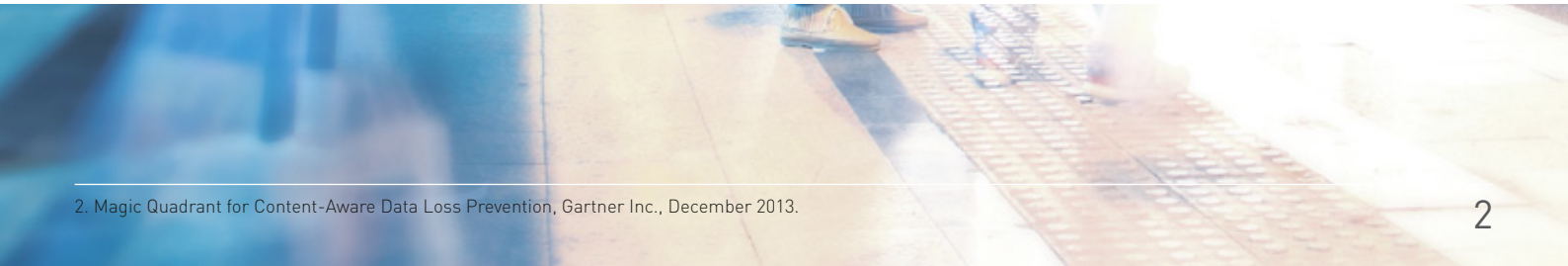
As a result, DLP was put on the back burner by many organizations, consigned to be shelfware, and very expensive shelfware at that.

DLP exuded such promise, yet became a business disabler when it should have been a business enabler. Roll forward several years and the very way in which information is required to be used has driven some incredible advances in technology.

DLP has grown more 'intelligent' thanks to its ability to perform deep content inspection and combine it with the context that the information is being used. Who is sending what to whom and how. This relatively new breed of content-aware DLP is growing in popularity but is it enough? Figures from Gartner show that the market has grown from $369 million in 2010 to $710 million in 2013, with closing figures for 2014 estimated at $830 million.[2]

Yet this content-awareness is not the end of DLP's evolution because, as our perfect information security storm continues to blow, and the value of information increases, information security is no longer purely an IT risk, it is now regarded as a critical business risk. As a consequence, DLP must take into consideration the context in which information is being accessed, shared, uploaded and stored. In short, it needs to adapt in line with changing user behaviors, business priorities and regulatory frameworks.

So can DLP be 'adaptive'?



2. Magic Quadrant for Content-Aware Data Loss Prevention, Gartner Inc., December 2013.

Critical information: IT risk or business risk?

With increased access to information, it's more difficult to evaluate exactly what constitutes critical information, where it goes and how to keep it safe as it flows in, through and out of an organization – not to mention the storage issues that come with cloud. (Exactly who is responsible for information security when it resides in 'a cloud' overseas?)

One thing is for certain, as the critical asset of any organization, information has shifted from being purely an IT risk to a major business risk. Furthermore, with the rise of SMAC technologies and increasingly stringent regulations to obey information security is certainly giving many Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) sleepless nights.

The old days of using DLP as a means to acquire a tick on the compliance box are gone. Today and in future, lines of business leaders across departments such as finance, HR, supply chain, product development, sales and legal must be empowered to create their own definition of critical information, together with policies and processes that determine how it can be used and by whom.

As a result, DLP solutions need to gain an element of proactivity. They can no longer lock down data, instead they must adapt to become the enabler of continuous collaboration, so that organizations can connect and compete. And the best way to do this is with a DLP solution that gives organizations 100% visibility of their critical information 100% of the time – wherever it goes, however it is used.

With a better understanding of what critical information actually is, how it can be used and what business risk it presents should a data breach occur, organizations can retain more effective and appropriate control. Better control in turn reduces risk – and that can only lead to one thing: a better night's sleep for the CIO, the CISO, the CFO... and the CEO.

DLP gets proactive: A new breed of content and context-aware DLP

What's driving the market for DLP – one that Gartner believes is the fastest growing segment of information security, at 18.9%?[3]

Well, recent research undertaken by Loudhouse on behalf of Clearswift provides some solid indicators. Certainly, a rise in the awareness that attacks can come from inside as well as from outside organizations are growing and is stimulating a growing appetite for the next evolution of DLP. However other factors are also at play, including awareness of regulatory change, awareness around risks and consequences, uncertainty about what constitutes critical information and where it lives, an increase in the adoption of cloud and a fear of being vulnerable because organizations know they don't have any form of effective DLP in place.

Factors driving the rise of the new adaptive breed of DLP

A summary of findings from December 2014 Loudhouse market research undertaken with individuals responsible for data security.

- **78%** of organizations believe the forthcoming EU Data Protection regulations will encourage them to re-think a DLP solution
- **67%** say a key driver for DLP adoption is to protect against malicious internal breaches
- **52%** of organizations don't yet have a DLP solution in place
- **88%** of those without a DLP solution intend to deploy one within the next 12 months
- **50%** of organizations have no idea where their critical information resides
- The proportion of data stored in the cloud will rise by **25%** within the next two years
- **50%** of Australian, Brazilian, Canadian, Chinese, French, German, Indian, British and American respondents in a Forrester survey admit they deliberately circumvented security policies because it is the most efficient way to get things done[4]

Business leaders are readily aware of new data loss incidents over and above the well-rehearsed credit card/bank detail leaks. It is these kinds of incidents that DLP should help to prevent, as they are still worryingly commonplace, so what should organizations now consider:

1. Intellectual property theft
2. Insider threats – both from malicious and inadvertent actions of their personnel
3. Information stored in cloud environments and then compromised en masse
4. Embedded malware in documents and resulting Advanced Persistent Threat (APT) infections
5. Sensitive email leaks which damage reputation
6. Classified information 'hidden' in documents which are released to the public

All these scenarios require an Adaptive DLP solution

This new variant of DLP acts with increased accuracy, which requires the technology not just to understand the content, but also the context – who was sending what, why and how. Imagine a solution that can recognise information at risk and remove it, while leaving the rest of the information to continue unhindered. The result is not just reduced business risk but also improved information governance and productivity. This is an environment where collaboration thrives – and one that every business leader would wish to create, because this is the route to greater competitive advantage, efficiency, customer satisfaction and profitability.

So how do we get to Adaptive DLP?

3. Magic Quadrant for Content-Aware Data Loss Prevention, Gartner Inc., December 2013.
4. Rethinking DLP: Introducing the Forrester DLP Maturity Grid, Forrester, 2015, using Forrester's Business Technographics® Global Security Survey, 2014.

What to expect from the next evolution of DLP

Clearly no CISO, CIO or line of business manager wants to diminish the positive collaboration benefits that SMAC technologies deliver. No organization can be responsive, competitive or even remain static these days without using some or all of them.

So in an ideal world, and taking into consideration the perfect information security storm we're all whirling through, can DLP ever really make the shift from security enforcer to business enabler?

Where there's a will, there is a way

When traditional DLP kicks in, it is usually over a simple piece of information that has broken policy. For example the credit card in an order that's forwarded to a supplier – the communication is then blocked, stops the risk, but also slows the business. So if we could remove the offending content we'd be good to go? Correct. And that's precisely what the new technology in an Adaptive DLP solution, Adaptive Redaction, was designed to do – find the information that breaks policy and remove it. Perhaps the order was a PDF document, no problem, Adaptive Redaction recreates the document without the offending information – and sends that on. However, the brilliant part is that Adaptive Redaction not only deletes the obvious visible information, it also removes the less obvious 'invisible' information (hiding in document properties, revision histories and fast save data). It is also designed to work on both incoming and outgoing information, Direction Agnostic, and can also remove embedded active content (eliminating things like Advanced Persistent Threats before they have the time to act).

Adaptive Redaction is intelligent; it can decide that secure email is fine for a particular document, but when it gets pushed into the cloud or copied onto a USB stick critical information is redacted (or even blocked – sometimes, blocking is the only sensible option!) Of course the actions can also differ depending on who you are, the CEO can send different types of information to a person in HR or someone in finance. Adaptive DLP is just that... Adaptive.

In summary, the traditional approach of 'stop and block' is still there, and the ability to alert on policy violations is also present – enabling the CIO to remain in control. But there is a new alternative – remove the information that breaks the policy and send the rest on. It might be a word from an email, or a credit card number in a report – remove it, but keep the business moving.

This adaptability is the cornerstone of what constitutes the next evolution of DLP – information always flows in, through and out of an organization, but specific information that breaks a policy is automatically and consistently removed.

This creates the perfect balance between:

- Collaboration and control
- Information access and security
- Liberating businesses today and future-proofing them for tomorrow

In essence, the new era of Adaptive DLP has been purposely designed to drive productivity to the max, secure in the knowledge that only the right information is seen by the right people at the right time. Discover how, with Clearswift's technology, you can enjoy 100% visibility of critical information, 100% of the time.

If you'd like to learn more about how Adaptive DLP can help your organization drive productivity while staying secure, please contact us:

Tel:
+44 (0) 118 903 8903

Email:
info@clearswift.com

Web:
www.clearswift.com/solutions/data-loss-prevention

Twitter:
For more insights on data loss prevention follow Dr. Guy Bunker:
@guybunker

clearswift

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations to have 100% visibility of their critical information 100% of the time.

As a global organization, Clearswift has headquarters in the United States, Europe, Australia and Japan, with an extensive partner network of more than 900 resellers across the globe.

United Kingdom
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale
Reading
Berkshire, RG7 4SA
UK

Germany
Clearswift GmbH
Landsberger Straße 302
D-80 687 Munich
GERMANY

United States
Clearswift Corporation
309 Fellowship Road
Suite 200
Mount Laurel, NJ 08054
UNITED STATES

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
JAPAN

Australia
Clearswift (Asia/Pacific) Pty Ltd
5th Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIA

www.clearswift.com