clearswift | SCC We make IT work

Information Visibility: Reducing Business Risk

Application and web content inspection and protection with the unique Clearswift and F5® Partnership

Contents

1. Overview

Following the notorious hack of Sony's PlayStation Network, it came to light that "Sony failed to protect its networks and was using obsolete web applications, which made the company's sites inviting targets for hackers"[1]. As a result of this attack, the account information of up to 77 million users was stolen. In 2014 it was evident they had not learnt their lesson as terabytes of server information were hacked by 'The Guardians of Peace'[2], fundamentally proving the increasing need for organizations to better understand and manage their electronic information as it passes through internet gateways.

In 2014 there were further extreme examples of unauthorized information disclosure via internet and web traffic across even the largest corporates; still not recognizing that prevention is better than cure, to avoid malicious and innocent data breaches; **ANZ Bank**- mistakenly posted a template on their website to help analysts and investors with their forecasts that "inadvertently contained" numbers for the to-be-published annual earnings, resulting in suspension from trading[3] on the ASX and causing a 3.5% drop in share price; **NMBS** (Belgian Railway Service) was responsible for leaving a web server unprotected causing a breach of – an estimated 700,000 people – including names, addresses and email addresses. The data, which was open for consultation on an unsecured server, were later copied by the hacker and placed on another site.

Table 1 shows further examples of breaches published in 2014[4], additional examples can be found in Appendix 1.

Table 1 Example of Published Data Breaches in 2014

Name of Organization/ Individual	Sector	# of Records	What was compromised	Lost or Stolen	Target Country	Insider Abuse or Theft
UK's tax authority, HM Revenue and customs	Government	25,000,000	Personal data of UK citizens	Mismanagement	United Kingdom	Exposed Online
Individual	Commercial	1,460,000	PII, in some cases, home address and telephone numbers of customers	Mismanagement	Multiple	Exposed Online
Hyperion	Commercial	400,000	PII, bank account number, social security, password, balance accounts and internal information	Mismanagement	Poland	Exposed Online
Berliner Jobcenter Charlottenburg – Wilmersdorf	Government	163,000	Private addresses, mobile phone numbers, account data	Mismanagement	Germany	Exposed Online
CZ (health insurance company)	Medical	55,000	Individuals	Mismanagement	Netherlands	Exposed Online
Nederlandse Spoorwagen (Dutch Railways)	Government	50,000	Individuals	Mismanagement	Netherlands	Exposed Online

New legislation continues to be introduced both from a national, as well as an industry sector perspective with a view to protecting the information, and more importantly, the people that the information relates to. This began with credit card, bank and financial details and has subsequently spread to healthcare (PHI) and other personally identifiable information (PII) and is now looking to protect Intellectual Property (IP). On the face of it, the problem doesn't seem to be so great; understand the information of value, where it is located and then how to protect it. However, for all those who have been trying to do this, the challenge has never been greater.

Most organizations do not understand what information has the most value to them, why it has an associated value, where it is stored and who has access to it. The situation is made even more challenging due to changes in working practices with critical information being held on a variety of enablement devices, laptops, local servers, CYOD (CYOD – choose your own device) and BYOD (BYOD - bring your own device), 'in the cloud', social networking applications, file storage sites, amongst others. While it is a challenge for the CIO to understand information within their own focus of control, when it starts to travel outside of the organization, the challenges multiply exponentially.

[1] http://www.eweek.com/c/a/Security/Sony-Networks-Lacked-Firewall-Ran-Obsolete-Software-Testimony-103450

[2] https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

[3] http://www.bbc.co.uk/news/business-29782600

[4] cmds.ceu.hu/sites/cmcs.ceu.hu/.../databreachesineurope-publicdata

2. Why do organizations need to increase visibility of their information?

One of the biggest areas of opportunity for CIOs in the area of information visibility is the process of sharing critical data that is required to manage the flow of products, services, and information in real time between suppliers and customers. The greatest potential of the Internet has been to facilitate collaboration between supply-chain buyers and sellers to achieve better information visibility and facilitate better decision making. Information visibility between original equipment manufacturers or large service providers and their lower-tier suppliers holds the greatest potential for creating joint cost-savings opportunities.

Traditional supply chains are rapidly evolving into "dynamic trading networks" comprised of groups of independent business units sharing planning and execution information to satisfy demand with an immediate, coordinated response.

- The power of visibility can never be underestimated— especially the visibility of enterprise information—yet it's often overlooked because it's the most difficult problem to tackle among information managers.
- Proliferation of disparate information sources—on-premise and off-premise, paid and unpaid—create complex silos that clog the flow of information and make information seeking activities time-consuming and painful.
- Many knowledge workers simply adopt information seeking behaviours that align with whatever data resource is most visible and accessible at the time that they need information to accomplish their work, leaving deeply buried or hard-to-access information that could be quite useful in the context of their work—under-utilized.

The examples above are problematic for a number of reasons, but most notably, it's fostering lazy or partial thinking. By not leveraging all of the information that might be available to help a knowledge worker (especially directors and other middle managers) contextually reach a decision or take action creates a huge risk to the competitive advantage of the organization and slows the possibility of progress.

Aligned to visibility of information comes the desire to collaborate for organizations and individuals as the adoption of cloud, internet applications, social networks and mobile working increases the ease with which content can now be shared internally and externally, whilst significantly improving the efficiency of working practices within a business. However, many companies that wish to collaborate in this way are deterred by the security implications. Critical and sensitive information can become lost once the data leaves the organization and moves beyond the control afforded by the use of corporate devices, applications and collaboration tools.

From a security perspective, these new business practices have a potentially high negative impact yet it is the combination of these desires that gives today's businesses their agility and competitive edge. Not adopting or blocking the use of these new business practices is not an option as it portrays a lack of evolutionary practices. No longer does a consumer spend 10 minutes to enquire in a store about a product or ask the sales person for the best resolution to their concern, they have a vast resource at their fingertips online, 24 hours a day and according to a recent 2015 F5 survey of 2,000 consumers they expect the correct information to be visible within 5 seconds[5] or they switch to an alternative brand. 82% of consumers highlighted fast websites and mobile apps as important to them when engaging with brands, alongside irrelevant online content and security concerns that drive negativity to a brand. The result is substantially increased business risk, from loss of customer (consumer and business) confidence, emphasising the need to address information visibility, speed of access and protection of corporate and consumer information as a priority to remain competitive.

[5] http://www.theguardian.com/media-network/2015/feb/12/online-shoppers-five-seconds-website

3. Business Risks

All businesses run on risk, without risk there is no benefit. It is how organizations manage risk which helps give them a competitive advantage. As mentioned previously the fast, efficient, secure and relevant access to information creates a business advantage but accompanying it are multiple risks.

- **Fast:** Impatience, stress, multi-tasking, location, time-bound, etc. are all reasons that a consumer see as irrelevant when they are interacting with a computer, so none can be an excuse for lack of speed to gain access to information
- **Efficient:** Changing form factors, how I want to consume information, provide consistent data flows, always be available, intelligence to remember me; any of these or others not provided will tolerated as the consumer expects the 'computer' to address all these challenges
- **Secure:** I may provide an organization with personal information, credit cards, health status, social security number, tax returns, likes and dislikes, hobbies, family tree, etc. but it is **my** information so ensure that it is secure for access, visibility and use internally and externally
- **Relevant:** Content is king, but relevant content maintains loyalty. Your content needs to be up to date, resolves the 'unknown' questions to be asked and be easy to digest (form factor)

The risks associated above are all associated with the needs of the consumer, so to an extent can be addressed from feedback and trends obtained with the 'User Experience'. But what about those risks that are invisible to the organization; the cyber, malicious or internal risks.

4. The challenges of the information delivery chain

From the moment when Marketing proposes a new value added service for customers until it is actually functional and can be utilized by clients, there are a big number of steps.

From a user perspective, they will probably end up pointing the browser to a web page or running an app in the mobile phone to access the service.

However, the underlying technology that supports the service is much more complex than just a simple webserver or mobile application. These are just the very last steps where the information is presented to the client and they can interact with it.

But this information is only relevant if it has been correctly processed and somehow associated with a specific customer for their interest. This means that corporate critical business systems, like the Enterprise Resource Planning (ERP) or Customer Relationship Management system (CRM), will feed information to the service. This will also probably mean that the business logic that interprets the requests from clients and interrelates it with the existing information on the corporate systems will also interact with other business applications' logic.

Because of the complexity of some of these interactions, in many occasions a middleware layer needs to be added, which acts as a logic communication flow between different applications, databases and defines also a common information model.

As part of the logical evolution of systems, applications evolve and deliver new versions. But not all the interactions are always upgraded to connect with the new version of the application. This leads to even more complexity, as apart from the interactions between different applications, also the version of each of them needs to be taken into account.

The resulting information systems result in a mix of up to date systems, legacy systems, and different versions running altogether as part of the corporate environment. If we could trace how information is moving throughout the different subsystems, it will look very similar to a plate of spaghetti.

So there it is, a new service is finally deployed making use of new and legacy technology, and interacting with corporate information to provide value to customers.

It is usually in the last layer, the presentation one, where all the attention to security is focused. Firewalls are configured to block network access to the webservers different from the ones required to provide their service. Web application firewalls are sometimes deployed to protect from errors in both the presentation and the business logic layer.

But what is protecting the inner layer in this infrastructure, the most valuable one and the ultimate objective of any attack? This layer, by the way, is your information. The answer is almost nothing.

It is commonly known that human error is the final cause of most of the security problems. Actually, some studies[6] point out that 95% percent of all security incidents involve human error. That is not different for services exposed to the Internet. Misconfigurations or default ones, poor patch management policies and the use of default user names and passwords are still commonly found in systems in the information delivery chain.

Looking back at the number of sub-systems and departments involved in the delivery of a service, we can give ourselves an idea of the number of people entailed as a whole. In big organizations this number goes up to three digit numbers. Can we assure that none of them has made a mistake therefore putting information at risk? Can it be guaranteed that there is no forgotten development directory, no default configuration, no weak password or no unpatched system? What about the application? Are you 100% certain that all the interactions with other systems are under control, that there are no security problems at any level of the service and that all access to the information is controlled? Of course not.

Any of these can lead to a security breach, to information being exposed and to a substantial fine from the data protection authorities. So be prepared, you know where your gold is. Are you ready to protect your goldmine?

5. Why every organization is a potential victim from 'Team Attacker'!

Ask the majority of organizations if they have been attacked via a cyber-activity and the response would systematically be 'no', 'not us', 'they couldn't get through our security', 'probably, but it hasn't hurt us', 'no, we don't have anything of value', 'definitely not, I'd know if we had been breached'. Considering that the average awareness of a date of intrusion of breach discovery is approximately 300 days[7], making the immediacy of breach awareness about as rare as a finding a 'mint perfect' Honus Wagner baseball card[8] or realizing your copy of 'A Midsummer Night's Dream' was actually signed by Shakespeare[9]. In a targeted attack, your organization is singled out because the attacker has a specific interest in your business, or has been paid to target you. The groundwork for the attack could take months so that they can find the best route to deliver their exploit directly to your systems (or users). A targeted attack is often more damaging than an un-targeted one because it has been specifically tailored to attack your web servers, applications, processes or personnel, in the office and sometimes at home. The independent attacker or 'Lone-Wolf' still exists, primarily to gain a reputation or make a statement, but the attackers who spend weeks and months surveying your organization as a potential honey pot of valued information will come from the 'Premier League' of black hatters. Under a matrix operational model, actors (black hatters) sign up and transfer from one cause or objective to another under the simplicity of anonymization, credentials and belief.

Who might 'Team Attacker' comprise?

- Cyber criminals interested in making money through fraud or from the sale of valuable information stored on your web servers or executed within your applications; Industrial competitors and foreign intelligence services, interested in gaining an economic advantage for their companies or countries;
- Hackers who breach your organization's [apparently secure] collaboration channels as an enjoyable challenge; Hacktivists who wish to attack companies to gain insights of their political or ideological preferences, also sabotaging your website with inappropriate material or installing diversionary links to take the user away to a fabricated site
- Script Kiddies (a derogative term, by the more sophisticated crackers), the apprentices and interns of the 'Team' who have yet to earn their stripes, but unfortunately are often just as dangerous for exploiting back door and patch flaw security lapses on application web servers or sending Phishing attacks
- And finally the 'wild card' of the team; your employees, or those who have legitimate access to use, develop, test, integrate and maintain the web experience of your organization. Who either by accident, misguided intentions, or indeed with malicious intent, leave an open door for all to enter, or fail to apply appropriate security layers underpinning the web lifecycle framework.

[6] IBM 2014 Cyber Security Intelligence Index

[7] Don Ulsch, Managing Director, Price Waterhouse Coopers, 2014

[8] aT206 Honus Wagner, made by the American Tobacco Company, 1909. Sold for $2.8 million in 2012. It has been called the "Mona Lisa of baseball cards."

[9] William Shakespeare' s signature is one of the rarest of all, with only 6 of them in existence and valued somewhere around $3 million dollars

6. Data loss

The biggest information risk facing businesses today is data loss. Not only does data loss frequently result in regulatory fines, but it can also incur substantial additional costs associated with reputation damage, the possibility of losing intellectual property to competitors and the unbudgeted costs for strengthening an organizations security posture following a data loss/breach. While it's crucial for an organization's success to allow their employees to communicate in a free and collaborative manner, the intensified use of the internet (web) as a commercial and social platform has increased the risk of data loss, where applications such as social-networking tools pose an enhanced risk to organizations that don't protect themselves fully.

Whilst opinion believes that the majority of breaches are externally driven, the overwhelming majority of data loss comes from inadvertent or accidental incidents. According to IBM Cyber Security Intelligence Index[10], 95% of all security incidents involve human error. That is no different for services exposed to the Internet. Misconfigurations or default ones, poor patch management policies and the use of default user names and passwords are still commonly found in systems in the information delivery chain.

Lack of understanding as to the value of different types of information, and where the sensitive or confidential information is, coupled with how it flows through an organization, ensures that data loss has to be recognized as a board-level issue for organizations large and small. Without this understanding, it is difficult for organizations to put in place the appropriate security measures.

Data loss catalysts could be:

- **Web servers:** Are just like a 'dumb user' that is not asked to validate 'should I do this?' for every daily action, they assume all directives are true and valid and will perform them according to their ability.
- **Phishing links:** These open the user to download malware during their session that installs malware onto the user's device for immediate or future exploitation.
- **Patch inefficiency:** You can't afford to ignore third-party patching, but it can be an overwhelming challenge. Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data it contains.
- **Insecure cryptographic storage:** Insecure cryptographic storage is a common vulnerability that occurs when sensitive data is not stored securely. Insecure Cryptographic Storage isn't a single vulnerability, but a collection of vulnerabilities.
- **Insufficient transport layer protection:** Is a security weakness caused by applications not taking any measures to protect network traffic. During authentication applications may use SSL/TLS, but they often fail to make use of it elsewhere in the application, thereby leaving data and session ID's exposed.
- **Cross-site request forgery:** Is a malicious attack that tricks the user's web browser to perform undesired actions so that they appear as if an authorized user is performing these actions
- **Directory traversal:** Is a type of HTTP exploit that is used by attackers to gain unauthorized access to restricted directories and files
- **Malicious code:** Analysis tools are designed to uncover any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system
- **SQL injection:** Is a type of web application security vulnerability in which an attacker is able to submit a database SQL command, which is executed by a web application, exposing a back-end database

[10] http://www.ibm.com/services/uk/en/it-services/security-services/2014-cyber-security-intelligence-index-infographic/

7. Advanced Persistent Threats

The next generation of malware is the APT or Advanced Persistent Threat. This is the 'replacement killer' for computer viruses of old, and while viruses are still a threat, these threats target specific companies and individuals with the aim of damaging infrastructure, stealing information, including intellectual property, to sell for profit or disrupt commercial operations for political and competitive reasons. Viruses are usually detected using statistical analysis based on the fact they have been observed thousands or millions of times. The APT is most often a 'one-off' and so statistical analysis based on observation is not applicable.

Phishing and spear-phishing are the weapons of choice to begin the attack, and small to medium-sized companies (those that tend to have less robust security policies in place) are particularly vulnerable. The delivery mechanism is often an innocuous looking document or a link to a [believable] website, both of which have embedded targeted active malware hidden for execution.

All information has a value to someone; not understanding where the business critical information is stored, makes it very difficult to adequately protect it. The rise of the APT has moved the focus for security away from systems, to the people and the information they hold. Keeping the information secure, which leads to the reduction in risk, and the ability to track and trace its progress inside and across the organizational boundary, is critical for good governance and compliance.

8. What is Adaptive Redaction?

Redacting sensitive information from documents where 'your eyes are not permitted to view' has been available in the broadest of forms such as 'blacking' out the content with a marker pen or digital overlay; obscure (fade) the content into the background of a document making it unreadable to the naked eye; converting the document into a new form factor, whilst omitting the sensitive content, since the marker pen was introduced. But these and other obfuscation processes rely too heavily on human intervention, have no context of the sensitive content being targeted and cannot adjust to the innovation of the malicious cyber attacker.

Clearswift introduced a response to the traditional methods of redaction with a unique and automated software layer, available for Clearswift and non-Clearswift email and web technologies.

Adaptive Redaction is the removal or transformation of data according to policy (rules), to ensure that information complies with corporate information security policies before it is sent or received by the recipient (person, application or system). By employing adaptive redaction, organizations can enable safer, more effective collaboration – in the cloud, in the office and external to the organization. Traditional Data Loss Prevention solutions are a simple 'yes' or 'no' to sending information, as they lack the architectural design to inspect, disassemble and apply recursive assembly to the content 'in its original format'. Adaptive Redaction removes this barrier by modifying the information according to policy to ensure only the acceptable levels of information is shared, and that critical information remains secure at all times.

Adaptive Redaction consists of three approaches:

Text Redaction

- The automatic removal of keywords or phrases. For example, the removal of sensitive project references in a document attachment sent within an email or via cloud storage outside of the organization. Or the removal of expletives from social network pages that enter the user's browser.
- Specific pieces of information, tokens, can be detected and removed via text redaction, such as credit card numbers / social security numbers. For example, sharing an order with a supplier becomes a seamless process when the content aware policy removes an overlooked credit card number from the original purchase form.
- Information from databases such as phone numbers, social security numbers or any other data stored can also be detected and redacted. This highly reduces the false positives rate for information with a common pattern.

Document Sanitization

- For many organizations, the existence of meta-data and history information in documents is a potential source of data leaks. The content aware policy detects and removes or modifies meta-data, revision history and selected properties associated with multiple document types.

Structural Sanitization

- The automated removal of active content that could contain malware, targeted attacks or critical information including objects such as macros, scripts, embedded executables and other active content items.

9. Direction Agnostic

Information flow in business, 'The Information Supply Chain' cuts through and across organizations via multiple communication channels. Traditional data loss protection architectures continue to lack the intelligence that 'outsiders' may send inappropriate and sensitive data that should not be accepted into an organization, continuing to focus only on 'outbound' data movement. Clearswift recognized these threats over a decade ago, ensuring that content inspection and subsequent remediation actions are bi-directional (direction agnostic), so data protection policies are able to apply the same levels of protection and information tracking of content flowing into and around an organization as well as information flowing to external stakeholders. While the policies associated with the direction flow may be different, any content inspection technology needs to apply a high degree of contextualization using a deep content inspection (DCI) technology and analysis engine to assess the data and apply appropriate policies.

For many organizations these days, having a blanket policy to remove active content (executables, malware, macro's etc.) from incoming documents is crucial to preventing infection by APT's. Similarly, a blanket policy to remove document meta-data and revision history on all documents leaving the organization is also frequently used to prevent inadvertent data leaks and embarrassing comments from reaching the wrong person.

Enabling a collaboration agnostic content inspection solution should not be focused on only one [busy] communication channel such as email. Protection for the organization from information sent or received through the internet/Web is being utilized in greater measures, including access of information on web application services or via social networking and cloud collaboration sites. So your content inspection technology should have the breadth to secure across all your channels and directions of communication that encompass the overall information supply chain.

10. Do I still need anti-virus, firewalls, Data masking, SPAM filtering?

The IT security market can confuse even the most competent professional or user. It is sometimes easy just to accept that a certain technology will resolve your current issue and also assume that it has the capability to evolve to resolve new and more formidable challenges and operating challenges.

Deep Content Inspection (DCI) is a form of filtering that examines an entire file or object as it passes an inspection point, searching for viruses, spam, data loss, key words or other content level criteria.

So you would assume that a technology that has a DCI engine will perform all of the above functionality? **Incorrect.**

Specialist anti-virus providers such as Kaspersky and Sophos (amongst other)s develop this technology and have a plethora of engineers and technology focused on the identification and removal of these malicious programs. In the same way Palo-Alto, Check Point and others have their roots deep in firewalls, network security systems that control the incoming and outgoing network traffic based on an applied rule set, by establishing a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted. Data masking is a proven technology to secure requests of data from a source database to a 'load' database, where the processor may not have the require authorization to utilize the data in its native form.

So there is a place for everything, but everything needs to be in its place.

Clearswift has its roots heavily entrenched in DCI having developed its own inspection engine over the past 20 years. But our expertise is in data loss, information search or other content and context level criteria. Clearswifts' Email and Web Gateways and all their derivatives such as the SECURE ICAP Gateway primary purpose is to ensure that organizations can inspect [to over 200 layers] content and then apply Adaptive Data Loss Prevention (A-DLP) policies to ensure sensitive information cannot enter or leave an organization, whilst also ensuring active content under the label of APT's do not enter an organization to inflict damage or exfiltrate content to an unauthorized 3rd party.

Clearswift complement [if required] all our SECURE Gateways with anti-virus engines from Kaspersky and/or Sophos, so our users can be assured that the experts in virus detection technology are providing this much needs additional security layer to your web application protection strategy.

So yes, you do need to ensure that you have the required levels of anti-virus, firewall, IPS, IDS, Data masking (SDM, DDM), data loss prevention, application security, amongst many other technologies. Never assume that marketing literature implies a service, always ask the vendors.

11. Clearswift and F5 Partnership provides innovation from innovators

Clearswift technology provides the ability to dissect communication flows and inspect content to identify critical information and perform the appropriate mitigation actions as defined by the organizations corporate compliance policies. The Clearswift SECURE ICAP Gateway technology has been developed to utilize the industry ICAP protocol interface, enabling advanced content inspection and adaptive redaction therefore identifying and applying the necessary remediation action across the F5® BIG-IP® Local Traffic Manager™ (LTM®) architecture.

F5 ensures application delivery and security in data centres, hybrid cloud environments, and future software-defined networks; the key to success in today's highly demanding ecosystem. BIG-IP LTM provides full proxy architecture with the ability to interact as an ICAP client to make use of available external adaptation services provided by the Clearswift SECURE ICAP Gateway.

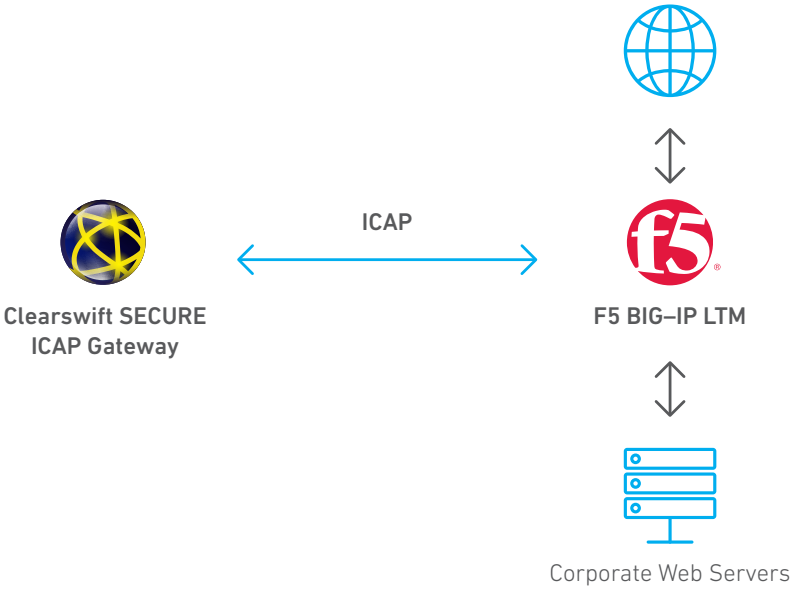
By combining the solutions, clients can benefit from high performance and optimized application delivery while ensuring the appropriate corporate information compliance policies are applied on both incoming and outgoing traffic.

F5 and Clearswift can also provide a smart window to your services where data is only seen if it is compliant with your information security policy and information security breaches are solved on the fly.

Just like electrochromic glass works in smart windows, becoming dark based on the environment and the light that goes through them, Clearswift can selectively filter the data that is presented to external users, becoming opaque to hide sensitive information and keeping transparent for the rest of the time. And this is done in an automated way, enforcing your information security policies and in real time.

The architecture of the solution that can achieve this magic is very simple. Just complementing BIG-IP LTM with the Clearswift SECURE ICAP Gateway is enough to start protecting your most valuable asset: your information.

Figure 1: Simple architecture for effective data protection



Just as F5 BIG-IP LTM can be used to optimize application delivery in the cloud, Clearswift can similarly complement its technology to protect organizations' critical information for cloud services.

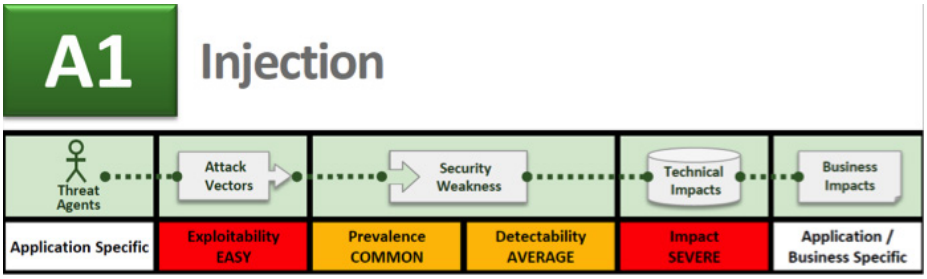
So check the windows to your services and upgrade them to smart windows where no critical information can be seen from outside. At the end of the day, nobody likes being stalked through a visible window!

12. Use cases

Application vulnerabilities

Every piece of software is prone to have errors and some of them can lead to a security breach. The use of strict coding standards and both static and dynamic security audits minimize the probability of them occurring. However, new security problems are discovered every day and don't forget that commercial software is also supporting your applications, which is not under your full control.

According to Open Web Application Security Project (OWASP – http://www.owasp.org) in their latest report on the top ten most critical web application security risks[11], Injection vulnerabilities are at the top of the list. These vulnerabilities exploit text entry boxes or application parameters to abuse the targeted interpreter to access data that shouldn't be shown by the application.



The impact is high, as it usually results in data losses by dumping information of the database that supports the web application. But regardless of which the existing vulnerability is, the final aim of exploiting it is to get access to critical information, in most cases being gently served by the abused web application.

The Clearswift SECURE ICAP Gateway can analyze the responses from web applications and identify any potential data loss, regardless of whether it is caused by a poorly implemented application, a vulnerability being exploited or access to a system gained.

Your information is protected, the impact of the attack neutralized and your business processes can keep their usual activity.

Protecting published content

As mentioned before, up to 95% of security breaches are caused by human errors. The stress to deliver, the need to keep a quick information delivery chain and the demand for instant collaboration with customers are part of the problem. That makes overzealous employees become a risk if proper controls are not set in place.

Part of this interaction is done by sharing information with customers or partners by publishing documents or content in a specific webserver accessible from the Internet.

Any piece of information that is published on a website, regardless of whether it is done in a password protected area only for certain partners or as publicly available content, is a potential egress point. This means that information should be analyzed and the corporate security policy applied. Human errors, like publishing the wrong file, can easily lead to data losses.

Also hidden information in the form of metadata is hardly ever removed before content is published which means that usernames, internal servers and even allegedly removed information can be accessed by externals.

12

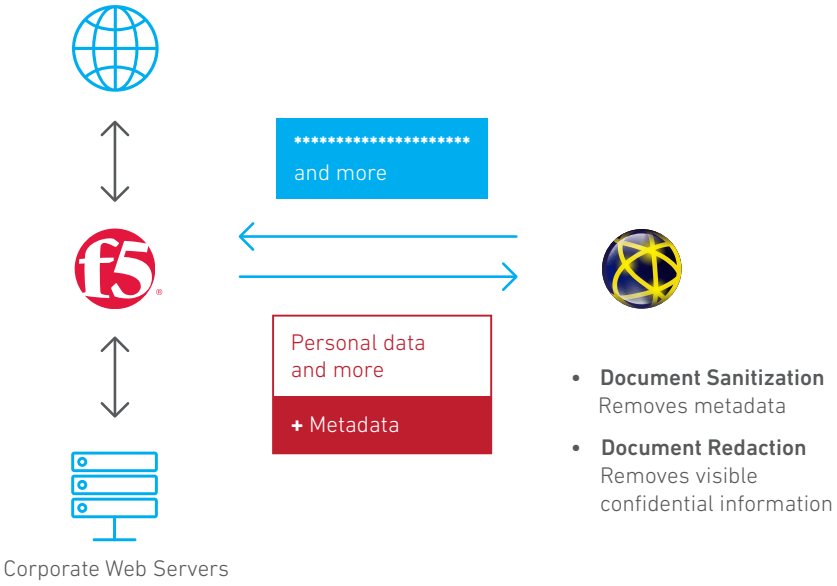
13

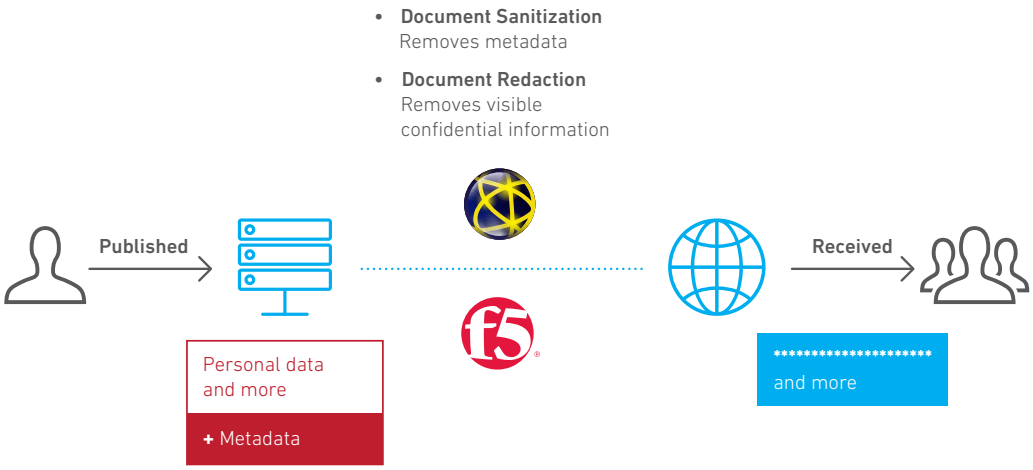
[11] Reference: OWASP Top Ten Project report - http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf

[12] Source: Sputniknews.com – http://sputniknews.com/europe/20150306/1019170728.html

[13] Source: The Guardian – http://www.theguardian.com/world/2014/aug/28/federal-police-mistakenly-publish-metadata-from-criminal-investigations

BIG-IP LTM optimizes the delivery of applications. When deployed together with the Clearswift SECURE ICAP Gateway and its Adaptive Redaction technology, it can modify the content as it is delivered to remove confidential information and hidden metadata.



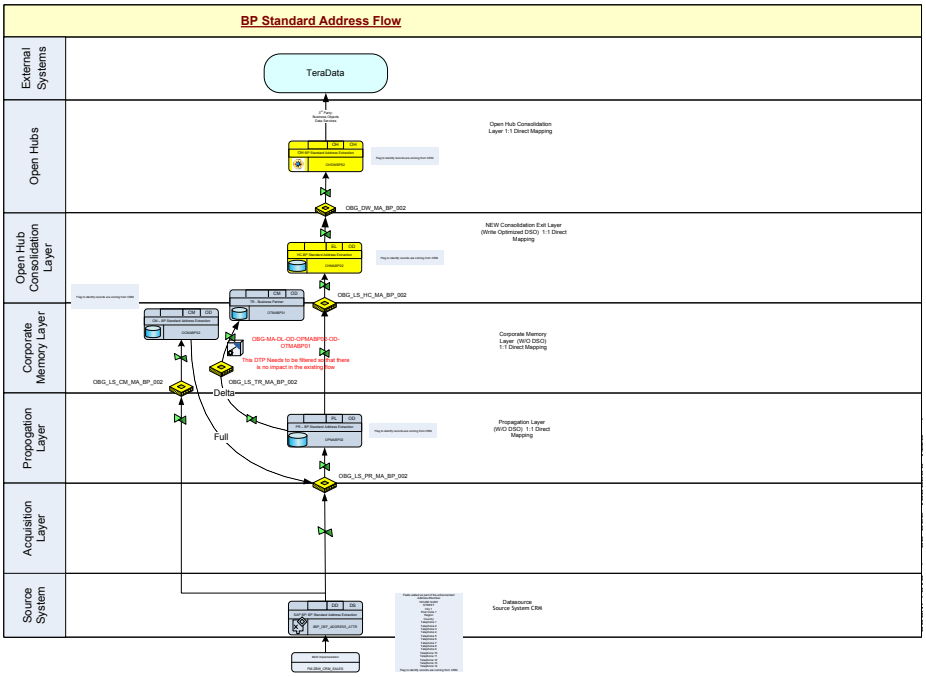


By automating the process, confidential information is kept protected even from human errors.

Web services delivery

The stress to deliver new services quickly can cause organizations to move services from development to production environments without following the appropriate security procedures.

Human error is amplified by the high number of people involved in the delivery of a service. Each layer and every subcomponent is prone to have some sort of misconfiguration, such as components installed by default, or data used for development available in the final production environment.



It is also very common to find vulnerabilities in services related with deficient or inexistent application lifecycle management. This problem can get augmented in organizations following a poorly implemented Continuous Delivery methodology.

As a result, confidential information can be made accessible from the Internet. By deploying BIG-IP LTM and Clearswift SECURE ICAP Gateway, information can be inspected to avoid data leaks through services facing external users.

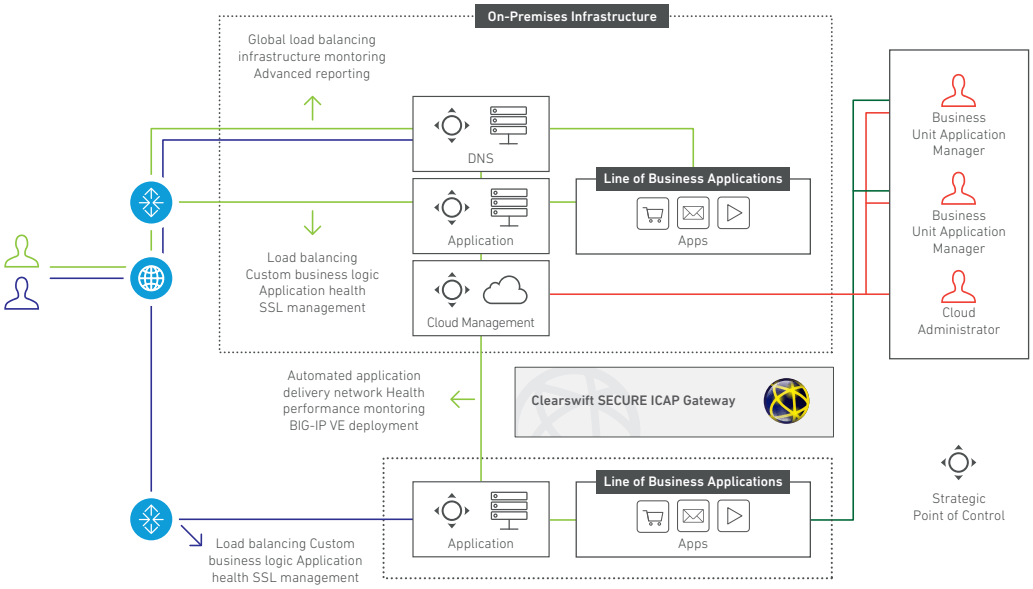
Cloud connectivity

While IaaS providers are promising faster build and deployment times, a quicker ROI, and more flexible payment terms—and thus outcompeting services within private data centers—inherent dangers lie in the new infrastructure silos that are created as a result. Enterprises are looking for a single, seamless, self-service IT infrastructure that will ensure secure access and collaboration of content, minimizing the threat of inbound malware intended to disable the efficient delivery of public, private and hybrid cloud operations.

Integrating the management tools and connectivity between public and private environments creates a seamless experience across the two, delivering a transparent extension to the data center environment and avoiding technology silos. The F5 Cloud Migration architecture combined with Clearswift Adaptive Redaction technology within the SECURE ICAP Gateway delivers strategic points of control that enable IT departments to meet expectations for delivery, security, access, functionality, configurability, and performance—wherever the workload is hosted.

The combined F5/Clearswift solution provides critical information protection for integrated and automated application delivery capabilities into the cloud, rapidly reducing the provisioning and deployment times for application networking services, whilst ensuring that data flows are clean, authorized and align to relevant regulatory standards. It accomplishes this through:

- Integration into third-party cloud management tools.
- Automation of the provisioning of application networking services across public and privately hosted F5 BIG-IP® products.
- Integration with Clearswift SECURE ICAP Gateway with Adaptive Redaction technology.
- Orchestration that expedites deployment times.
- Extensibility and unparalleled flexibility using APIs.



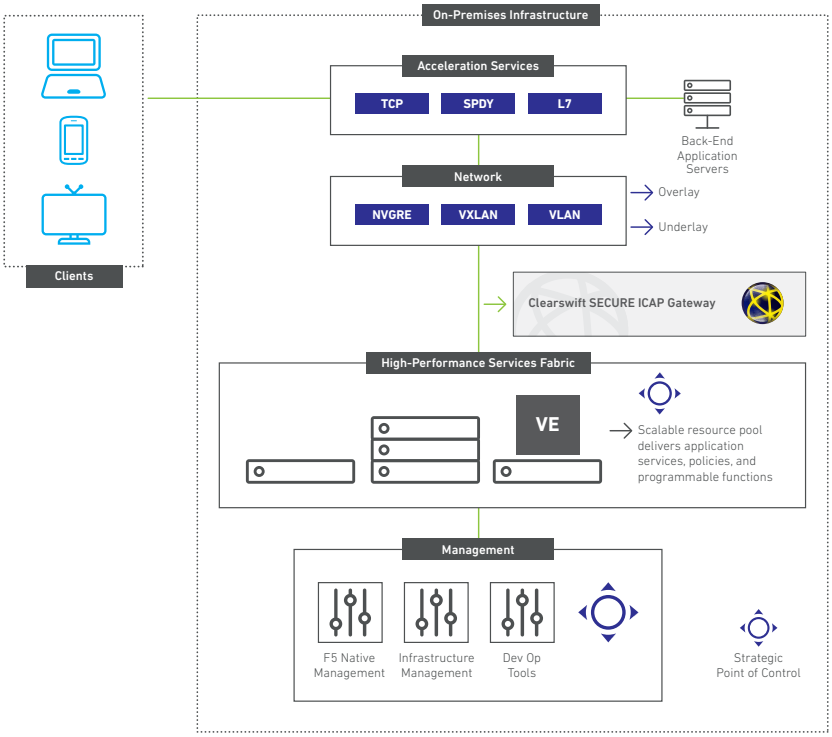
Integrating the Clearswift Adaptive Redaction technology with the F5 Cloud Migration solution provides critical information protection whilst you automate and orchestrate the deployment of application delivery services across both traditional and cloud infrastructures. Whether an organization is adopting a public, private, or hybrid cloud, Clearswift and F5 simplifies the optimization and authorized information collaboration and accessibility of business applications, ensuring that they're fast, secure, and available—wherever they are.

- **Save time:** Reduce deployment and provisioning timelines otherwise extended by management silos.
- **Critical and Sensitive Information Protection:** Automate the content inspection and redaction of data that breach policy violations for content passing across BIG-IP solutions
- **Minimize the introduction of hidden APTs:** Automate the redaction of 'active content' used to deploy malware entering the 'Cloud' environment.
- **Increase efficiency:** Automate the provisioning of application networking services across public and private data centers.
- **Simplify provisioning:** Coordinate with third-party cloud orchestration solutions to unify application and network services provisioning.
- **Gain flexibility:** Ensure extensibility using F5 iControl™ and REST APIs.

A simplified SECURE application acceleration architecture

Third-party web application acceleration software or appliances can provide a huge range of tools and techniques to accelerate web applications whilst protecting critical and sensitive information. A rich feature set of protocol and application manipulation tools enables organizations to control multiple aspects of application delivery and may extend down into TCP optimization layers. These tools can apply different acceleration techniques to sites, URIs, and objects to achieve fine-grained control of application behavior.

BIG-IP LTM modules and the Clearswift SECURE ICAP Gateway Adaptive Redaction options, for instance, contain a comprehensive feature set of tools, all of which can be further configured and customized to provide highly granular and highly effective application acceleration policies and deep content inspection for adaptive data loss prevention.



Accelerating websites and associated applications provide three essential principles; send data as efficiently as possible; send data as infrequently as possible and send as little data as possible. Integrating the Clearswift functionality provides a missing essential principle:

Send and receive data as securely as possible

- The combination of acceleration techniques, which manipulate HTTP traffic with the goal of reducing page-load times and increasing security (SSL/TLS encryption is required to use the protocol), the use of Adaptive Redaction will ensure that in times of stress and pressure only authorized content will be loaded, unlike the experience suffered where financial results were posted to the production web server prior to official disclosure.

- Without the ability to cache objects for an extended time, you may open the door for a hacker to transfer invalid data from the server in order to compromise your web application. Adaptive redaction will ensure that any active content not acceptable to the application comes from an authorized source and is permissible.

- Removing unnecessary data from server responses can be done by removing whitespace or comments from text files, such as JavaScript or CSS, or by transforming images into a more efficient file format and stripping image metadata. While the gains in removing whitespace from individual files might be only small, the incremental impact is measurable, given the number of objects commonly required to load a page. But content modification is not only down to optimization. Clearswift's ability to strip out metadata information, clean up confidential information from the communication and even remove active content applies content adaptation to safeguard you most precious secret: your critical information.

13. Summary

Clearswift has over 20 years expertise in adaptive - data loss prevention, information analysis and other content and context level inspection technology. This allows organizations to have visibility over communication data flows to identify and enforce policies over the information being exchanged. F5 ensures application delivery and security in data centres, hybrid cloud environments, and future software-defined networks.

The integration of F5 and Clearswift technologies brings information visibility to a new level by allowing inspection of incoming and outgoing traffic for corporate web servers. Enforcing adaptive information policies reduces business risk and proactive information loss scenarios, even in cases where information is stopped from leaving the organization under the control of malware that was loaded on a web server from an attack, prior to implementation of the SECURE ICAP Gateway.

14. Appendix 1 – Example of Breaches 2014

Name of Organization/ Individual	Sector	# of Records	What was compromised	Lost or Stolen	Target Country	Insider Abuse or Theft
Veronica Magazin / Dutch Lottery	Commercial	1,000,000	Individuals	Mismanagement	Netherlands	Missing or Stolen Hardware
Deutsche Bahn employees	Commercial	173,000	Personal data	Mismanagement	Germany	Missing or Stolen Hardware
University of Pittsburgh Medical center	Medical	1,300	PII, PHI, etc.	Mismanagement	United Kingdom	Missing or Stolen Hardware
National Liberal Party	Government	3,000	Personal data of teachers	Mismanagement	Romania	Insider Abuse of Theft
Metropolitan police	Government	1,136	Email Addresses	Mismanagement	United Kingdom	Insider Abuse of Theft
Ministry of Transportation	Government	168,000	Individuals	Mismanagement	Netherlands	Exposed Online??
ARD	Commercial	50,000	PII and email addresses	Mismanagement	Germany	Exposed Online??
Komercni Banka	Commercial	45,645	PII	Mismanagement	Czech Republic	Exposed Online??
UK's Tax authority, HM Revenue and Customs	Government	25,000,000	Personal data of UK citizens	Mismanagement	United Kingdom	Exposed Online
Individual	Commercial	1,460,000	PII, in some cases, home address and telephone numbers of customers	Mismanagement	Multiple	Exposed Online
Hyperion	Commercial	400,000	PII, bank account number, social security, password, balance accounts and internal information)	Mismanagement	Poland	Exposed Online
Berliner Jobcenter Charlottenburg-Wilmersdorf	Government	163,000	Private addresses, mobile phone numbers, account data	Mismanagement	Germany	Exposed Online
CZ (health insurance company)	Medical	55,000	Individuals	Mismanagement	Netherlands	Exposed Online
Nederlandse Spoorwagen (Dutch Railways)	Government	50,000	Individuals	Mismanagement	Netherlands	Exposed Online
HM Revenue and customs (HMRC)	Government	50,000	Financial details: bank details, National Insurance numbers and earnings of other claimants, in addition to their own annual award notice	Mismanagement	United Kingdom	Exposed Online
Bundesinstitut fur Bildungsforschung	Educational	37,000	Tests, 37000 individuals, 1.8 GB	Mismanagement	Austria	Exposed Online
Department of Health (UK)	Government	34,250	Applicants' PII, criminal convictions and sexual orientation and religion	Mismanagement	United Kingdom	Exposed Online
Het Dagblad van het Noorden (Dutch newspaper)	Commercial	32,781	Email addresses of individuals	Mismanagement	Netherlands	Exposed Online

Name of Organization/ Individual	Sector	# of Records	What was compromised	Lost or Stolen	Target Country	Insider Abuse or Theft
Indonesian Embassy in the Netherlands	Government	25,000	Individuals	Mismanagement	Netherlands	Exposed Online
CEC Bank	Commercial	17,000	VISA credit cards	Mismanagement	Romania, Multiple	Exposed Online
Standard Life Bank	Commercial	15,000	Personal and financial details	Mismanagement	United Kingdom	Exposed Online
BT	Commercial	13,500	Personal details, IP addresses	Mismanagement	United Kingdom	Exposed Online
Breekijzer (TV program)	Commercial	13,000	Complaints	Mismanagement	Netherlands	Exposed Online
GratisCondoom.com	Non-profit	10,000	Individuals	Mismanagement	Netherlands	Exposed Online
Ministry of Defense	Government	3,000	Individuals (several thousands)	Mismanagement	Netherlands	Exposed Online
Axel Springer	Commercial	3,000	Names, Addresses, cellphone numbers, bank account details	Mismanagement	Germany	Exposed Online
Rabobank	Commercial	3,000	Clients	Mismanagement	Netherlands	Exposed Online
Individual/ NHS Survey	Medical	3,000	Personal Records	Mismanagement	United Kingdom	Exposed Online
France Info	Commercial	3,000	Personal records (IP, time of connection, browser software, emails)	Mismanagement	France	Exposed Online
GPD (Press Agency)	Commercial	2,000	Individuals (Thousands)	Mismanagement	United Kingdom	Exposed Online
Individual/ Home Office	Government	1,598	Names, dates of birth and immigration status	Mismanagement	United Kingdom	Exposed Online
Torbay Care Trust	Educational	1,373	PII, Salary, etc.	Mismanagement	United Kingdom	Exposed Online
Individual/HMP Cardiff	Government	1,182	PII of inmates and sentence length, release dates and coded details of the offenses carried out	Mismanagement	United Kingdom	Exposed Online
UWV Werkbedrijf (Public Employment Service)	Government	1,151	Email addresses of Individuals	Mismanagement	Netherlands	Exposed Online
Ministry of Education	Government	893	Personal records of Roma students receiving funding	Mismanagement	Czech Republic	Exposed Online
City of Olfen	Government	800	Names, account information, financial information, miscellaneous	Mismanagement	Germany	Exposed Online
PvDA (political party)	Government	300	Individuals (several hundreds)	Mismanagement	Netherlands	Exposed Online
Veilingnotaris.nl	Commercial	300	Individuals (hundreds)	Mismanagement	Netherlands	Exposed Online
Zaandam and Lith Municipalities	Government	300	Personal records (several hundreds)	Mismanagement	Netherlands	Exposed Online
Marseille Constituents	Government	300	Personal records (identity, addresses, phone numbers, emails, ages and messages sent to their mayor)	Mismanagement	France	Exposed Online
EU-US Summit Delegates	Government	200	Personal records	Mismanagement	Multiple	Exposed Online
Bright (Magazine)	Commercial	80	Individuals	Mismanagement	Netherlands	Exposed Online
ResUrgences	Medical	50	Hospital Data (logins, passwords, access to servers, IP, VPN access)	Mismanagement	France	Exposed Online
Aberdeen City Council	Government	39	PII of several vulnerable children and their families, including alleged criminal offenses, minutes of meetings and detailed reports relating to the care of children	Mismanagement	United Kingdom	Exposed Online

Name of Organization/ Individual	Sector	# of Records	What was compromised	Lost or Stolen	Target Country	Insider Abuse or Theft
Hackney Council	Government	35	Names of the residents who had expressed views on license applications, in many cases with the resident's home addresses; ten email addresses; four mobile phone numbers, one Twitter handle	Mismanagement	United Kingdom	Exposed Online
UK Identity and Passport Service (IPS)	Government	21	Passport renewal applications	Mismanagement	United Kingdom	Exposed Online
Individual (competition entrants)/Toshiba Information Systems	Commercial	20	Personal data (name, date of birth, contact details)	Mismanagement	United Kingdom	Exposed Online
Kenpo Studio Denmark	Non-profit	18	Accounts with usernames, email addresses and encrypted passwords	Mismanagement	Denmark	Exposed Online
Ambulance service of Giessen	Medical	15	Individuals	Mismanagement	Netherlands	Exposed Online
Technical university of Denmark (DTU)	Educational	10	HIV Patients' personal identification (CPR) numbers and medical information	Mismanagement	Denmark	Exposed Online
Royal Veterinary College	Educational	6	Passport images of six job applicants	Mismanagement	United Kingdom	Exposed Online
Stoke – on- Trent city council	Government	5	People affected; sensitive information relating to the care of a child and further information about the health of two adults and two other children	Mismanagement	United Kingdom	Exposed Online
Individual	Commercial	3	Personal data (housing needs, mental health, cases of domestic violence)	Mismanagement	United Kingdom	Exposed Online
Department of Justice	Government	2	Individuals	Mismanagement	Netherlands	Exposed Online
Cambridgeshire, Bedfordshire and Hertfordshire police forces	Military	1,000	Personal data	Mismanagement	United Kingdom	Administrative error??
Individual/Telford and Wrekin Council	Educational	4	Personal records	Mismanagement	United Kingdom	Administrative error??
Norway National Tax Office	Government	4,000,000	Individuals' tax returns records	Mismanagement	Norway	Administrative error
KPN (Dutch ISP)	Commercial	2,500,000	Personal records	Mismanagement	Netherlands	Administrative error
Royal Bank of Scotland, NatWest, American Express	Commercial	1,000,000	Bank customers' details	Mismanagement	United Kingdom	Administrative error
KwizdoO	Commercial	500,000	Emails	Mismanagement	France	Administrative error
Bulgarian Ministry of Foreign Affairs	Government	37,000	Individual residence addresses	Mismanagement	Bulgaria	Administrative error
Chartered Accountants Ireland	Non-profit	17,000	Members' date of birth, contact details, and membership numbers	Mismanagement	Ireland	Administrative error
Gynecology Clinic in Bilbao	Medical	11,300	Patient Records	Mismanagement	Spain	Administrative error
Belfius Bank	Commercial	3,700	Bank's customers' data	Mismanagement	Belgium	Administrative error
Department of Internal Affairs	Government	2,800	Individuals	Mismanagement	Netherlands	Administrative error

Name of Organization/ Individual	Sector	# of Records	What was compromised	Lost or Stolen	Target Country	Insider Abuse or Theft
Penta	Commercial	2,200	CVs of job seekers	Mismanagement	Solvakia	Administrative error
Municipality of Delft	Government	650	Email addresses of Individuals	Mismanagement	Netherlands	Administrative error
Tilburg Municipality	Government	500	Email addresses of Individuals	Mismanagement	Netherlands	Administrative error
NLKabel	Commercial	375	Email addresses of Individuals	Mismanagement	Netherlands	Administrative error
Ireland Department of Social and Family Affairs	Government	40	Social welfare details, personal details	Mismanagement	Ireland	Administrative error
N Digital TV	Commercial	30	Personally identifiable information	Mismanagement	Poland	Administrative error
T-Mobile	Commercial	20	Email addresses of Individuals	Mismanagement	Netherlands	Administrative error
AIVD (Dutch Secret Service)	Government	4	Email addresses of employees	Mismanagement	Netherlands	Administrative error
Nets	Commercial	3	Credit information records	Mismanagement	Denmark	Administrative error
Individual	Commercial	2	Individual retirement's funds	Mismanagement	United Kingdom	Administrative error
Regional Court Banska Bystrica	Government	1	Court electronic database composing password, electronic division of cases for judges, e-mails	Mismanagement	Solvakia	Administrative error
Skat (Tax Authority)	Government	1	Individual tax documents	Mismanagement	Denmark	Administrative error
Individual/ Aneurin Bevan Health Board (ABHB)	Medical	1	Personal record over 6 months	Mismanagement	United Kingdom	Administrative error

clearswift | SCC We make IT work

Clearswift and SCC

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

The partnership between Clearswift and F5 is a significant development that will help SCC customers to maintain visibility of, and control access to, their web application critical information. It will provide a tangible benefit that SCC can pass on directly to customers as we work with them as they transition to a phase of consuming more web services and applications.

SCC's relationship and Gold Partner status with both Clearswift and F5, combined with our deep technical skills, experience and capabilities across a broad range of sectors, vendors and partners, ensures we can provide customers with a complete end-to-end solution. We have the ability to design, supply, install, support and maintain integrated Clearswift and F5 solutions and also have a wealth of experience working with government and defence organisations to whom we supply products and services through a number of purchasing frameworks, including: Technology Products; Technology Services; and G-Cloud.

United Kingdom
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale
Reading, 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
Level 17
40 Mount Street
North Sydney
New South Wales, 2060
AUSTRALIA