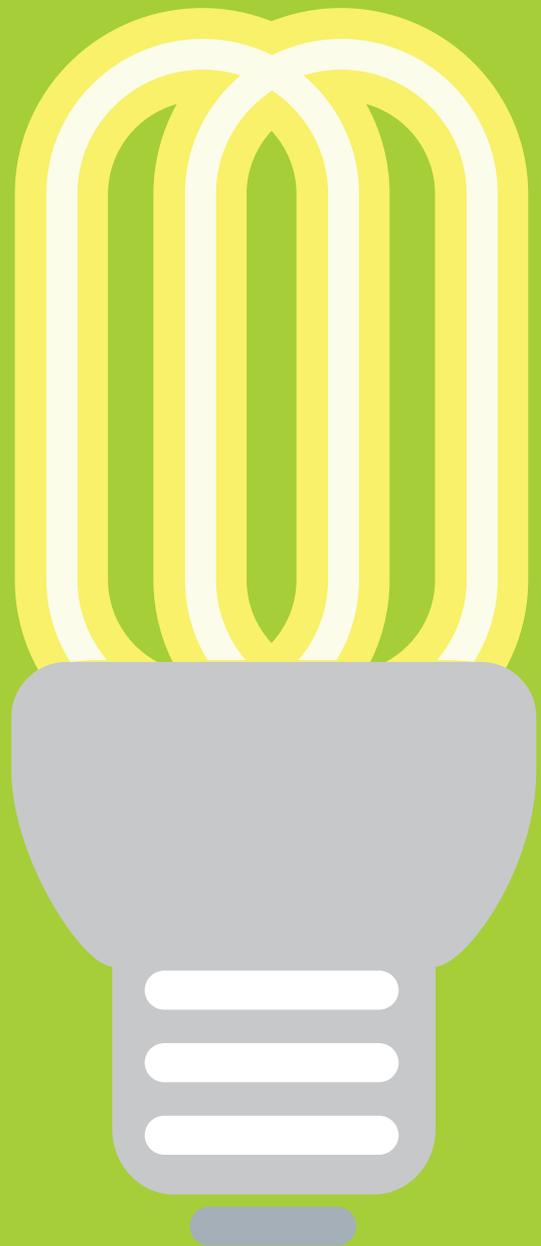


Securing Vital Infrastructure

Keeping the lights on



Securing vital infrastructure

It's not that long since anyone looking for news of international cyber criminals hacking into essential infrastructure had to be content with a Bruce Willis movie. Then Stuxnet hit the headlines.

While the exact motives behind Stuxnet are still the subject of intense speculation, the recent arrival of a 'Son of Stuxnet' Trojan called DuQu has served to further sharpen minds when it comes to securing the IT assets of essential service providers.

Although the concept of an Armageddon-style attack taking down entire infrastructures remains more of a preoccupation of government intelligence agencies than it does for those at the coalface of essential service provision, these high-profile attacks serve the purpose of placing information security front of mind for a sector that, as will be seen, isn't always noted for it.

The tip of the iceberg

Stuxnet and DuQu may be grabbing the headlines, but the day-to-day threat landscape for critical infrastructure providers is a lot less glamorous. Too bad the same can't be said of the consequences. Even the smaller, often less sophisticated players are increasingly aware of the vulnerabilities of IP-based infrastructures and the humans who use them, exploiting flaws in common productivity software or human carelessness to access sensitive data or launch malware than can cripple an organisation's ability to keep systems running.

Utilities organisations in particular are undergoing a sea-change in the way their IT systems and sub-systems interact. Once upon a time, SCADA and Industrial Control Systems (ICS) were based on proprietary standards and existed largely in isolation from the corporate applications and communications layer. As critical service providers move towards smart grid systems and web-based applications for in-the-field or end-user access, SCADA systems are increasingly converging with corporate and public networks, making them more vulnerable to breaches than before. The UK's Parliamentary Office of Science and Technology (POST) has pointed to an increasing trend towards connecting SCADA devices to wider networks as necessitating a renewed focus on IT security.¹

According to POST, approximately one third of water companies in the UK are upgrading SCADA infrastructure to allow control of remote sites from a central location, adding that 'Future smart grid infrastructure, which will provide more control over distribution of gas and electricity, will also require a significant increase in the use of ICT infrastructure for monitoring and control.' As much as these developments will enhance and enable productivity, they can also increase the risk profile of any organisation that fails to address security.

You are the weakest link

A remarkable feature of many high-profile attacks on IT infrastructure is the simplicity of the mode of access. While the attacks themselves may be very sophisticated, the reality is that the route into the organisation is anything but. Whether it's executables like Flash buried in harmless-looking Excel files, malware embedded in Word documents or dodgy Web sites, the weakest link in the IT security chain is the tendency of people to click without thinking.

In 2010, the Idaho National Laboratory in the US ran a number of tests to assess security practices in high-security organisations. Researchers left infected USB sticks and CDs, some of them company-branded, in car parks and other communal areas around the workplace. They then counted how many of the devices called 'home' when people used them on their work devices. In addition, a phishing mail was created, with researchers monitoring how many people clicked an infected URL. Finally, a woman pretending to be from tech support phoned people at random and asked for passwords.

"ICT security, along with computing system reliability, safety and maintainability are critical attributes for smart grid implementation and operation and need to be considered as part of overall management for this Critical National Infrastructure."

Energy Networks Association, UK²

1 Parliamentary Office of Science and Technology: Cyber Security in the UK POSTNOTE No. 389 September 2011
2 Energy Networks Association: UK Smart Grid Cyber Security, 2011.

The results were revealing: 40 per cent of people gave their passwords, 22 per cent clicked the infected URL and 20 per cent plugged the infected USB stick into their work device. The really surprising thing was that while security training reduced the number of USB device offenders to 2 per cent, many argued that this finding had more to do with updates to Windows that disabled the automatic launch of executable files than it had to do with the training. That argument appears to have some substance when you consider that the numbers clicking the infected URL or giving their passwords away remained more or less the same following training.

The reality is that, for many vital infrastructure providers, the most probable security breach vector by far is not a targeted, terrorist one. It's in-house. A key vulnerability for vital infrastructure providers is the seemingly innocuous threat from the kind of inadvertent, non-malicious human behaviours that compromise network security.

Beyond physical security

Good security technology, combined with education and awareness training can go a long way towards mitigating these risks, yet too many organisations overlook this vital aspect of security. Even as infrastructure and utilities providers integrate systems more closely with smart grid strategies, there's a continued emphasis on physical over information security. Ponemon Institute's recent research into IT security in the sector found that while 29 per cent of utility/energy companies spend \$20-40m on physical security every year, 21 per cent had less than \$1m to invest in IT security in any given year; 32 per cent had up to \$2m.³

While no one would dispute the importance of securing physical infrastructure, it seems remarkable that, given the potential fall-out of a data breach or attack, many service providers continue to view IT security purely as a box-checking exercise, with an emphasis on surviving compliance audits.⁴ PikeResearch has found that, while many organisations are becoming more thoughtful in their security approach to maturing technologies, such as smart meters, the security attitude towards newer technology such as control system automation is characterised by a desire to simply 'make it work', with cyber security 'an after-thought; or a never-thought.'

The problem with this train of thought is that the more intelligence and data that's added to grid assets - whether that's customer credit card details or the kind of sensitive information valued in industrial espionage circles - the greater the attack surface and broader the appeal. And with attackers increasingly aware of the role human error plays in exploiting vulnerabilities, organisations need to adopt a unified approach to information security that allows users to communicate and share information in a way that makes it easy for them to do their job without compromising on security.

Unifying information security

The UK's Energy Networks Association has pointed to a tendency towards fragmentation in the approach to cyber security, calling for a more integrated approach. Clearswift's Unified Information Security (UIS) approach allows information to flow freely and securely into and out of organisational networks, allowing staff to use IT in line with evolving security policies while enabling them to make full use of online collaboration technologies. A unified, integrated approach allows organisations to reduce complexity and administrative burdens without compromising on information security, striking a balance between business continuity requirements and the need to keep pace with a rapidly evolving threat landscape.

Strong UIS brings multi-layered, flexible IT security technologies together in one easy-to-manage place, allowing you to apply common, consistent policies across both web and email, giving complete control over the information entering and leaving your networks. Let's take a look at some of the key technologies and features:

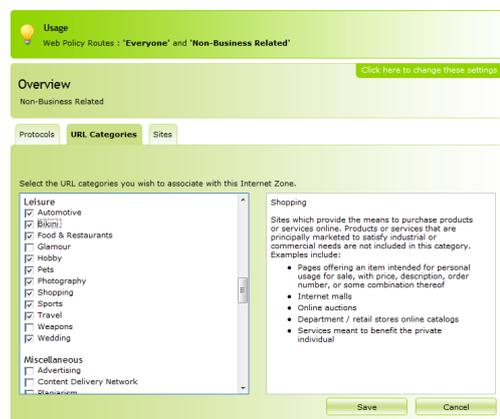
³ Ponemon Institute: State of IT Security: Study of Utilities and Energy Companies, 2011.

⁴ PikeResearch: Smart Grid Cyber Security, 2011

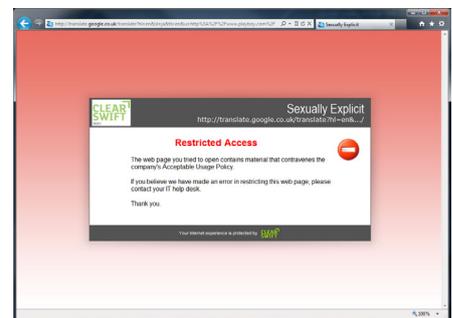
Flexible policy

The best IT security starts with policy. Context is everything when it comes to deciding what information needs to be blocked or controlled, and when. Flexible policy means organisations don't have to sacrifice security for agility and collaboration. Policies should reflect the way you do business: You might need to block music downloads but enable the easy exchange of CAD files or instant messaging for emergency situations. Policy should dictate technology, not the other way around. Traditional stop and block technologies are neither flexible nor intelligent enough to understand the nature of the content being exchanged and, crucially, how and where it can legitimately be used. The UK's Energy Networks Association has said that this capacity to apply different controls to different types of data improves data privacy by differentiating between consumer and technical data.

Clearswift's SECURE Web and Email Gateways allow IT staff to work with the business to set flexible parameters within which communications technologies can be securely used, whether it's placing limits on the amount of time employees can spend on personal browsing or applying policy-based deep content inspection to automate the decision to encrypt content sent over the organisational email network, block the exchange of sensitive data or flag potentially dangerous content.



Comprehensive URL filtering capabilities



Flexible policy moves beyond simple URL filtering to allow organisations the freedom to enable productive use of web applications or social media without exposing the organisation to data loss, intellectual property theft or malware attacks. Real-time scanning blocks malware that can be buried in Flash or Java script applications on sites normally deemed acceptable, e.g. Facebook games, allowing you to continue using social media applications without worrying about them becoming a back door for attacks. Scanning within URLs to detect sites using obfuscation techniques to hide malware, phishing or spear-phishing offers further protection.

Context is king

Real-time categorising means filters are constantly updating and learning; remote proxies are detected and embedded URL detection in cached items prevents users from working around policies. Context-aware controls mean that sensitive data exchange can be blocked or allowed depending on the nature of the application and the user's permissions; for example, uploading product information to LinkedIn may be blocked, but context-awareness and flexible policies mean data can be safely shared on business applications such as Salesforce.com.

This granularity can be extended right down to the individual user level, where different employees with different access requirements are granted appropriate permissions. Clearswift's technology enables IT teams to work with end users to set up structures that recognise the importance of different types of data, ensuring that protocols are in place that prevent certain categories of information from being transmitted or copied. Sensitive information may only be shared between approved users with a pre-recognised need to receive the information. At the very highest level, this can prevent data from leaving the organisation; at the lowest risk level, warnings for staff can be triggered, requiring them to check that they are not inadvertently attaching or copying sensitive data, or accessing potentially harmful material.

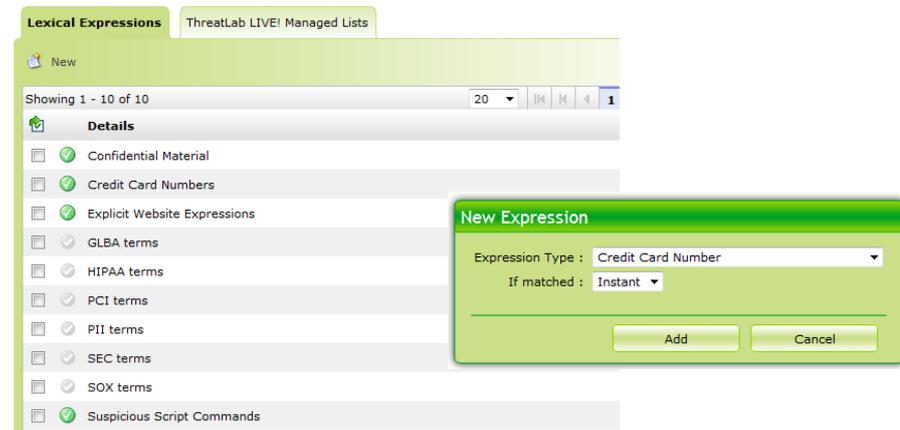
Deep content inspection

Most of the successful high profile breaches of recent years were phishing attacks launched via targeted emails carrying malware hidden deep within attachments. The attack on RSA in March 2011, for example, is now known to have been delivered via an infected Flash file embedded in an attached Excel spreadsheet entitled '2011 Recruitment Plan.' The mail was sent to only four employees and the one person who opened the attachment retrieved it from their junk mail folder.

It's all too easy for these things to happen; presentations carrying spyware payloads, zip files within zip files concealing viruses or other malware or even well-intentioned employees attaching sensitive data to an email by mistake or clicking 'reply to all'. In the utilities and infrastructure sectors, field engineers and other mobile workers bring an added element of risk: Laptops and other engineering devices are increasingly loaded with software and applications over which the field worker has sole control. Such equipment offers a potential entry point to networks and other systems, either through the malicious use of legitimate software or the introduction of malware through seemingly-innocent applications or portable storage devices.

Manage Lexical Expression Lists

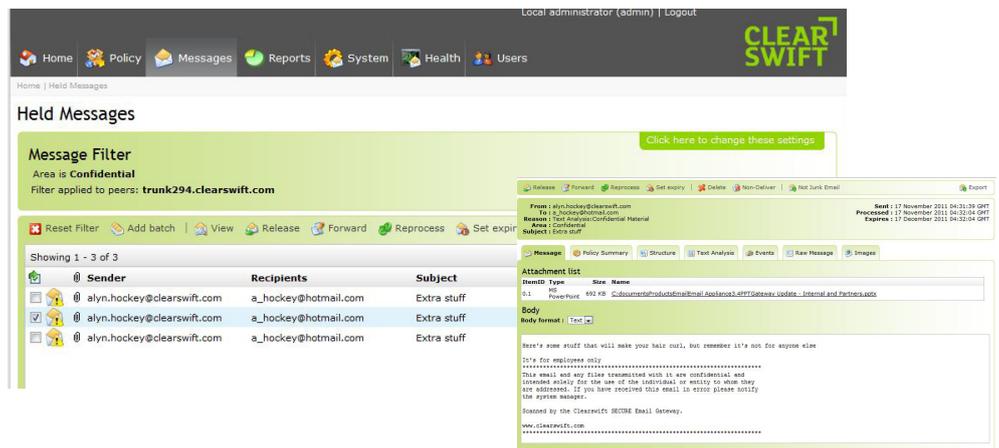
Using this page you may create lexical expression lists that can then be used by your content rules.



The screenshot shows the 'Lexical Expressions' management interface. The main panel displays a list of expressions with checkboxes and status icons. A 'New Expression' dialog box is open, showing 'Expression Type' set to 'Credit Card Number' and 'If matched' set to 'Instant'. The dialog has 'Add' and 'Cancel' buttons.

Deep inspection and intuitive scanning options are at the heart of the policy engine.

Clearswift uses a process called recursive disassembly to examine complex data formats and analyse content for potential threats. The Gateways use true binary-file type identification with full recursive decomposition analysis to ensure that nothing untoward can be hidden within files. Message and file content can be identified by byte signature, deconstructing nested or compressed files and extracting all the useful parts of any piece of data before inspecting them. The data decomposition is highly granular, allowing documents such as Microsoft Office, archiving, streaming media and hundreds of other common file types to be analysed by source, type and bandwidth consumption. Documents can be deconstructed into their individual parts, meaning that finding keywords like 'Confidential' in the footer of a document is more important than finding it in the main body. Similarly, Clearswift's content inspection engines will detect executables embedded within documents or other file formats, preventing users from unwittingly unleashing spyware or other malware onto organisational networks.



The screenshot shows the Clearswift web interface. The top navigation bar includes 'Home', 'Policy', 'Messages', 'Reports', 'System', 'Health', and 'Users'. The main content area shows a 'Held Messages' section with a 'Message Filter' applied to a message. The message is marked as 'Confidential' and the filter is 'trunk294.clearswift.com'. The message content is visible, showing a warning about sensitive information.

Deep content inspection detects sensitive content and applies policy accordingly.

Keyword search is a very powerful mechanism capable of detecting information leakage, abuse or insider trading activity. Using single and complex expressions, regular expressions and operators, you can look for these and block them accordingly. Powerful expression lists allow users to build up search patterns for detecting content leaks; the regular expression engine combined by Boolean and positional operators allows constructs such as:

- Reference Number FOLLOWEDBY =1 Part Number
- Credit card numbers NEAR expiry dates
- Employee ID AND postal code

Users can easily define the security policy that will be applied to the data, choosing to execute specific security rules for the sender and recipient, all based on the extracted data. Unrecognised file types can be blocked by default, quarantined and/or deleted.

Further granularity allows the policy management engine to configure rules and thresholds by department, location, user group, sender, recipient, file type, file size, time of day or individual user. Once set, the content-aware policies will automatically invoke the prescribed response to any threat or potential breach, including block/delete/quarantine - and alerting relevant managers and generating tailored reports.

Inbound threats detection and protection

Bi-directional scanning is at the heart of Clearswift's solutions. Just as the Web and Email Gateways monitor and handle everything entering your networks, leading anti-virus, anti-spyware and anti-spam technologies work alongside the powerful content inspection engines to prevent suspicious content and spyware from getting a toehold on the network. Zero hour anti-malware filters offer early detection, allowing for proactive defence against new, undiscovered malware based on 'honey pot' activity. The anti-virus software is updated automatically every 15 minutes.

Spam is detected and dealt with on a 99.6 per cent accuracy basis; the global reputation network is able to detect and reject 80-90 per cent of all spam traffic before it reaches the gateway, saving time, bandwidth and administration costs. Clearswift's TRUSTManager technology contains over 50 million IP addresses and has a dynamic feedback mechanism that constantly monitors behaviour and adjusts settings accordingly. Anti-spoofing controls mean that only mail servers can use the organisation's email domain, protecting the business from fraudulent email activity by criminals seeking to dupe users into revealing sensitive information by sending fake messages purporting to come from the company. Sender policy framework (SPF) controls help prevent phishing attacks by allowing senders to publish the server they used to send out mail, which recipients can then check against and validate before opening any attachments or clicking on links.

Encryption made easy

Vital infrastructure provision doesn't just involve the maintenance of services 24/7; with the overwhelming majority of critical services infrastructure in the UK, US and Australia privately operated⁵, customer data protection and privacy needs to be safeguarded alongside other highly-sensitive information. As email continues to be the communications channel of choice across industry sectors, most economies now call for proactive data protection policies, positive enforcement and risk reviews. In many jurisdictions, personal data is required by law to be encrypted. In the UK, for example, the Information Commissioner (ICO) has said that data loss occurring 'where encryption software has not been used to protect the data' are likely to result in regulatory action.

Flexible policy can be used to control not only the flow of information through the organisation, but also to decide whether (and when) messages and their attachments should be encrypted using industry standard protocols. Clearswift's SECURE Email Gateway with integrated encryption technology enables free communications without the risk of sensitive data loss. Encryption and decryption are performed automatically and centrally, within flexible policy parameters and without the need for user interaction, meaning that accidental encounters with the 'reply to all' button don't have to end with a hefty fine.

⁵ UK = 80%, according to Parliamentary Office of Science and Technology; USA = approx 85%, according to the Office of Homeland Security; Australia's Attorney General's Office says a 'significant portion' of the country's critical infrastructure is private-owned or operated on a commercial basis.

Encryption options

Best practice calls for encryption to be part of an automatically enforced email security policy. A flexible system is context and content aware, subjecting data to deep analysis before making the decision to encrypt whether or not the end user selects that option. The SECURE Email Gateway contains built-in routines allowing organisations to define automated parameters that will trigger encryption based on any of the following elements of a message:

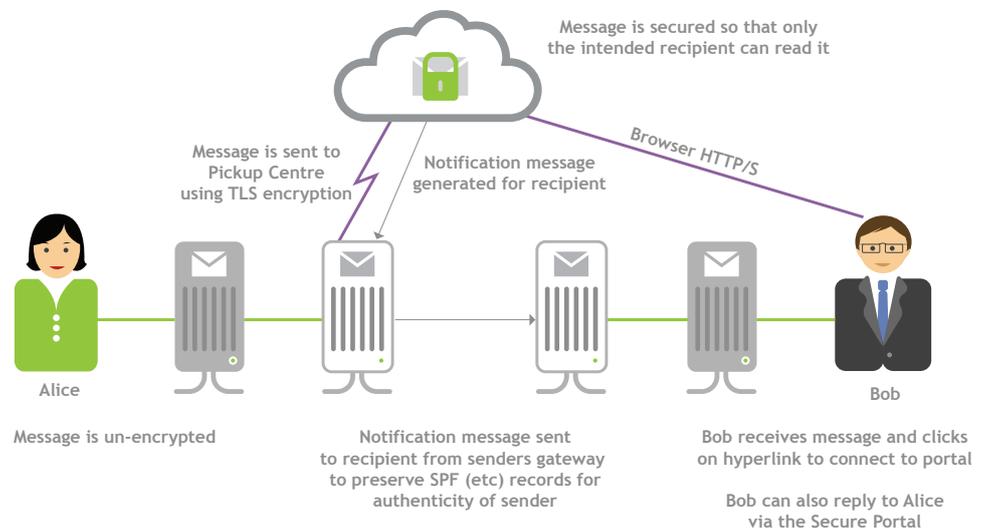
- The sender or destination of the message
- The content of the message:
 - In the subject
 - Message body
 - Message attachments
 - In message headers

Recognition of important tokens such as HIPAA, PCI DSS or IBAN numbers ensures that sensitive data is sent in an encrypted format, as do the built-in dictionaries for compliance such as GLBA and SOX. For added security, senders can force the encryption of any message simply by tagging messages with key words on the subject line or through the use of client plug-in options.

In addition to industry-standard formats such as S/MIME, PGP, ad hoc password protection and TLS, Clearswift also offers Portal Based Encryption (PBE), an infrastructure as a service (IaaS) option that provides a fully featured, policy based solution used with the SECURE Email Gateway. Hosting centres in the UK, US and Canada ensure that data is processed and stored in accordance with regional privacy directives.

Using PBE, when a policy engine determines that a message contains information requiring encryption, it is automatically sent to a secure host where it is encrypted and stored. A notification message containing a hyperlink to a HTTP/S site is then generated and sent to the recipient, who simply clicks the link and is taken to a secure portal, where they can read and respond to the content through their browser on a laptop, desktop or mobile device.

Secure Encryption Portal



Keeping the lights on

Securing IT for modern utilities and infrastructure providers calls for striking a balance between business continuity requirements and a rapidly evolving threat landscape. Today's plants, satellite sites and substations are increasingly linked through wired or wireless connections; advances in smart grid technologies are combining with economic and business imperatives to variously centralise or outsource network management. In-the-field workers, government environmental monitors, engineering and corporate staff all add to a heady mix that creates multiple points of vulnerability as corporate and plant systems increasingly overlap.

A unified approach to information security can help modern vital infrastructure providers deal with evolving IT threats without compromising on communications or the demands of an increasingly mobile workforce. Flexible policies, combined with quality inbound threat detection, deep content inspection and encryption capabilities can help organisations to mitigate the risks - not just from outside the organisation, but also within it.

Get in Touch
**CLEAR
SWIFT**

Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale
Reading
Berkshire
RG7 4SA

Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com