IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

SWIFT: Comply or No-Fly

Jason Steer

Jason Steer
EMEA CTO
Menlo Security

Biography

Jason Steer is the EMEA Chief Technology Office at Menlo Security (www.menlosecurity.com). Jason is an engineer at heart and has built and broken computer and networks since 1996. Jason has worked at a number of successful technology companies over the past 15 years, including IronPort, Veracode & FireEye.

Jason has worked as a cyber-expert with CNN, Al Jazeera & BBC and has worked with the EU and UK Government on Cyber Security Strategy. Jason has spoken at numerous industry events such as ENISE. You can follow Jason @verylongbloke on Twitter.

Keywords Isolation, Malware, Cybersecurity, Threat, Jason Steer
Paper type Research

Abstract

From Q2 2017, SWIFT customers will have to comply with new mandatory customer security requirements. A whole new segregated physical network might be needed – but as the author of this article claims, isolation technology is the quicker, cheaper and easier solution.

Introduction

More than ten thousand banks and financial institutions in over two hundred countries rely on a standard code to identify the correct destination for international wire transfers. The Society for Worldwide Interbank Financial Telecommunication was founded in 1973 to develop a system that was faster and more secure than existing TELEX mechanisms, and they created the SWIFT code that is used today.

Security is clearly a vital concern for SWIFT. Any ability to penetrate the system and manipulate the code might allow criminals to control the movement of bank transfers. The challenge for SWIFT lies in its extensive global attack surface: successful penetration of any customer's system might potentially provide a doorway into the SWIFT system itself. Security is not just an internal matter for SWIFT, it also relies critically upon the security of each individual user.

In September 2016 SWIFT announced a set of core security standards and an assurance framework against which all its customers would be required to demonstrate their compliance every year. SWIFT Chairman, Yawar Shah explained, "The growing cyber threat requires a concerted, community-wide response. This is also why the SWIFT board unanimously approved the framework and remains fully engaged in overseeing and driving the further development of SWIFT's Customer Security Programme."

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

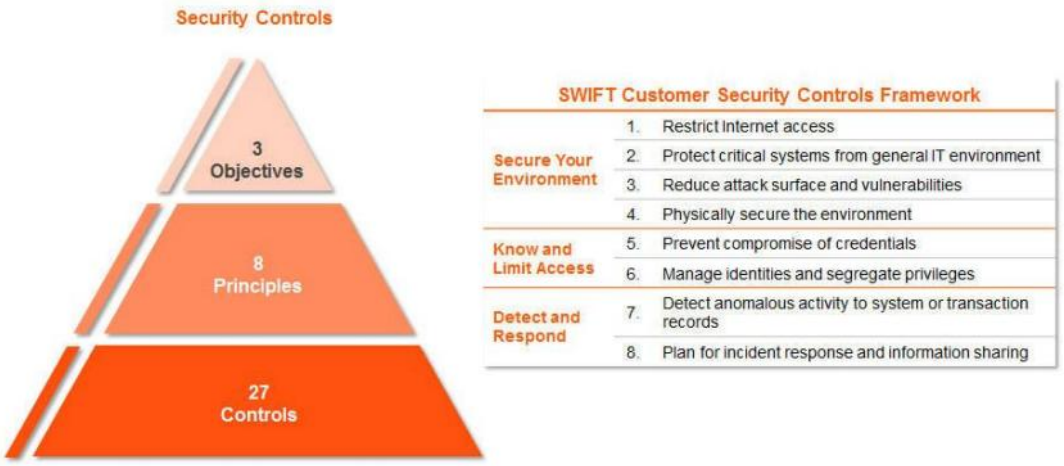
During the second quarter of 2017 the standards will be made applicable to all customers connected to SWIFT, including those connected through service bureaus. After that, SWIFT's customers will be required to provide self-attestation against 16 mandatory controls on an annual basis. Inspections and enforcement will begin on 1 January 2018, when customers' compliance status will be made available to their counterparts, ensuring transparency and allowing firms to assess risk of counterparts with whom they are doing business. SWIFT will then report non-compliant customers to their regulators, and randomly select customers for additional assurances, either from their internal or external auditors.

This process will not preclude customers from independently requesting additional assurance from their counterparts. Customers will also be able to announce their compliance with a further 11 advisory controls that will supplement the 16 mandatory controls. Yawar Shah admitted that: "We recognize that this will be a long-haul, and will require industry-wide effort and investment, as well as active engagement with regulators".

SWIFT's Customer Security Controls Framework

The SWIFT Security Controls Framework can be summarized in terms of its three objectives, eight core principles and twenty-seven requirements or controls, of which sixteen are compulsory and a further eleven are advisory – see *figure 1*.

Figure 1: SWIFT Customer Security Controls Framework



A full listing[1] of these controls can be found at www.swift.com/myswift/customer-security-programme-csp/securitycontrols. It is well worth looking at it as a guide to everything that should be considered when auditing security for any system, not just SWIFT. The controls cover not only IT measures – such as 2.1 Internal Data Flow Security and 2.3 System Hardening – and process measures such as 1.2 Operating System Privileged Account Control, but also the need for 7.2 Security Training and Awareness for employees.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

How is the customer going to comply with some of these requirements, such as 2.3 System Hardening (Reduce the cyberattack surface of SWIFT related components by performing system hardening) and 6.1 Malware Protection (Ensure that local SWIFT infrastructure is protected against malware)?

In view of the growing complexity of most organizations' systems, and their porosity in terms of wireless access, mobile working and Internet connectivity, how can these conditions possibly be met without the costly task of building and maintaining an extra dedicated and physically segregated system? Isolation technology could be the answer.

Isolation technology – a better solution

Today's most sophisticated form of isolation technology was developed for the critical needs of the finance industry, to address the problems of Internet usage. Few financial institutions could operate successfully without the immediacy and responsiveness of e-mail, e-chatting and Internet access – and this poses significant risks.

The problem is that the Internet's success today lies in its rich, responsive multimedia experience; a far cry from the static pages of its early years. What makes this possible is the hidden "active content" that lies behind surface appearance – the Flash and Java and other interactive elements. Even a PDF or Word document includes a lot more hidden complexity than you see on the surface and that is why we are continually warned against opening attachments in suspicious e-mails.

It is these files and active content that can be infiltrated with exploits, even on generally "trusted" sites. A recent report[1] by Menlo Security showed that visiting top any of the top 50 websites in UK resulted in your browser downloading an average 1.40MB of active code and executing 40 scripts per website; the "winner" was the website that executed 132 scripts from 48 background domains.

The solution to solving some of these requirements is to find a way to provide the user with a replica of the webpage, document or email that has all the hidden content removed. This is what happens when you can safely read and print a copy of a document, even if the original PDF contains an exploit. One simple technique has been to reproduce the pixels on the page – like printing a copy of the page onto the user's screen. This "one-size-fits-all" approach makes no allowance for the actual content – whether text, image or video – whereas the hidden active content is specifically designed to improve the user experience by adapting the rendering to suit the content. As result, pixel mirroring tends to slow down page loading, reduce responsiveness and makes common operations, such as printing and copy-paste almost impossible for the normal end-user.

A better, Document Object Model (DOM), approach allows for the actual content type and the dynamic manner it is represented in the browser. DOM Mirroring means that the isolating process actively monitors the currently loaded page tab for changes, translates those changes into DOM commands (without the underlying active content) and sends those commands to the end user's device, so the user's

"safe" page automatically updates in sync with the original. For example: instead of sending a Flash video to the endpoint, the same movie will be sent as crisp, suitable quality HTML5, while non-active safe elements are simply transmitted as they are. All the natively available fonts can be reproduced at the end point, so the whole page looks, feels and behaves just as it should.

When it comes to printing, this DOM Mirroring approach allows the document to reflow to suit the local printer – unlike the pixel mirroring approach that freezes the page as a rigid array of pixels. The reason why Internet isolation need not require installing special hardware, browsers or other software on the users' devices is that it can be delivered as a Cloud based service via your desktop browser. It replaces the actual web page with a "clean" page image that is then solidly encrypted and transmitted via a secure web proxy to the user's screen.

The advantages of isolation

Much of traditional IT security is based on experience of cyberattacks that have already happened, a knowledge of their characteristics (IOC's), what to look for and how to resist future attacks. With today's rapid malware evolution this becomes an extremely complex and demanding approach.

SWIFT's requirements include the need for user education and training. This includes much more than just an understanding of the technology, because successful cyberattacks rely heavily on social engineering via Phishing; users need to be trained to recognize the many signs of a dodgy e-mail, and to think twice before clicking on the handy short-cut buttons offered.

Today's Spear Phishing is even more invidious because it works its way into the users' confidence via subtle steps. For example, one is much more inclined to trust an e-mail that uses your proper name and refers to personal details such as "Hi John, we hear that you are a keen chess player and wonder if you would like to join the company's chess club – click here". But all such data could be harvested by trawling employees' Facebook and LinkedIn profiles. The link provided might even take John to a realistic looking chess club page with real people's names on it and a chance to join by providing personal details. In this way the attackers gain knowledge of the user's credentials and their first foot into the corporate system.

The simple instruction 7.2 Security Training and Awareness could require endless training and on-going updates with each new escalation of Spear Phishing exploits. This cannot ever be totally avoided, but e-mail and web isolation that strips all e-mails of hidden content and warns if the link leads to an infected site will not only make training simpler but also free the users to spend more time on actual work.

SWIFT and secure

The DOM mirroring isolation platform was developed in collaboration with JPMorgan Chase & Co. Its features and capabilities were developed from square one with financial services in mind and it was deployed with zero impact to users. It was claimed to deliver a seamless user experience.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

In fact, it was so popular as a solution that in just two years, the same technology has been successfully adopted by other critical sectors, including government, technology, healthcare, oil and gas companies in many countries worldwide. The user response has been overwhelmingly positive, and the reduction in risk serves to increase both morale and productivity. Of course, this requires caution: one should not encourage a too complacent sense of security, but rather to build as much caution into the system itself so that users do not get bogged down in detail.

Remember, the essence of isolation is to sterilize all communications on the assumption that anything might contain malware rather than to rely on a huge databank of potential risks. How can this technology be used to help SWIFT compliance? This clearly depends upon the individual organization, its systems and business processes, so there is no simple answer. But it would surely make sense to ask for advice from specialists in isolation technology before committing to any drastic fork-lift overhaul of the corporate system.

Reference

1 www.swift.com/myswift/customer-security-programme-csp/securitycontrols

2 www.menlosecurity.com/uk-vs-germany-top50report