Bloor

White Paper

White Paper by Bloor
Author **Fran Howarth**
Publish date **March 2016**

Selling unsecure websites is not an option

...why market dynamics are creating a new opportunity for hosting providers

Website security is too important to ignore, especially when an organisation depends on it for its trade. As a hosting provider, this new opportunity will help you not only to meet your goals of better servicing your customer, but will also provide a means to increase your revenues.

Author **Fran Howarth**

Executive summary

The market for online commerce and services is growing rapidly. Ironically, every new website or application creates a new opportunity for cybercrime, which is growing at the same – if not even greater – pace than legitimate business. That's because not every website owner has the capabilities required in-house to ensure that they are providing their customers with the levels of security required to counter such problems. At the same time, browsers and search technologies are starting to make it very obvious when a site has inadequate security in place.

As a result, growing numbers of website owners are turning to the services of hosting providers, who are increasingly being asked to provide the assurance that their web-based services can scale up as required, and that provide them with the means to ensure that the services they offer are secure and meet their regulatory compliance objectives. Hosting providers must offer their customers security as a service.

A baseline component of effective website security is the use of secure sockets layer (SSL) technology, which provides encryption for data in motion to help keep transactions secure and to ensure the privacy of personal data. SSL certificates attest to the security of a website and the authenticity of the website owner. They provide visitors to those websites with the confidence that they require that the web-based service is secure and can be trusted.

Hosting providers can help their customers to achieve the levels of security that they need by handling processes related to SSL certificates for them. However, this is an arduous task if done manually, often with the use of spreadsheets. Far better is to use the services of a trusted managed security platform provider, which can automate and manage the entire lifecycle of the certification process, from issuance of certificates to their renewal and revocation. All certificates have limited lifespans and need to be replaced when they have expired, or have been compromised in any way. By using such a service to handle all certification needs of their customers, hosting providers will not only engender their loyalty, helping to retain customers and attract new ones, but will provide them with the ability to gain further revenue through the provision of higher levels of security than just basic certificates, as well as other value-added security services.

This document discusses the role that SSL certificates play in achieving security and looks at how hosting providers can benefit from offering such services from a trusted security platform provider to their customers.

Fast facts

Organisations with web-based offerings are increasingly looking to service providers who can host their offerings for them. They are increasingly asking those hosting providers to help them tackle the web security issues that they face. The huge spike in security breaches and incidents being seen is raising the bar for the need to engender customer trust, requiring a rethink in security strategies.

New browser and search capabilities will make it obvious to visitors that a site or application is not seen as trustworthy or secure and will lead visitors to abandon the service in favour of a competitor.

A managed website security service will do much to ease the pain for hosting providers regarding the cost and complexity of providing their customers with the "understructure" that they need in a highly competitive, low margin market that is driven by customer demand. It removes the need to cobble together free or open source offerings, or standalone security tools from a variety of vendors, both of which require a great deal of manual work to manage, especially given vulnerabilities such as Heartbleed that require action to be taken fast.

The use of a comprehensive security platform – purpose-built for hosting providers – makes it feasible to integrate a complete security portfolio into their existing business process and infrastructure without friction, deliver security to their customers with ease, and will allow them to scale their offerings as far as required, all in an automated fashion.

Hosting providers that can help their customers to ease their security concerns in an efficient manner will not only be able to increase market share, but will see other revenue-generating opportunities appear on the back of these services.

The bottom line

The market for managed services in general is growing rapidly, appreciated by many organisations for the help that this gives them managing aspects of their business that are not core competencies for them. The introduction of managed security platform that is purpose-built for hosting providers will ease many of the management headaches that they face in managing SSL certificates for all of their customers, providing not just great efficiencies, but also ensuring that security is tight.

"This document discusses the role that SSL certificates play in achieving security and looks at how hosting providers can benefit from offering such services from a trusted security platform provider to their customers."

The growth of hosted cloud services

> **...according to Forrester, spend on ecommerce platforms will grow from US$1.5 billion today to US$2.1 billion by 2019 in the US alone, driven by the use of hosting providers.**

Uptake of hosted cloud services continues to grow rapidly. For example, according to Forrester, spend on ecommerce platforms will grow from US$1.5 billion today to US$2.1 billion by 2019 in the US alone. Much of this growth is being driven by the need to replace homegrown platforms with those managed by hosting providers that are more scalable, compliant and easier to maintain. The ***Cloud Industry Forum*** estimates that web hosting is the application that is most likely to be cloud-based, cited by 58% of respondents to a survey of organisations from the UK. Security is often cited as an inhibitor to the take up of cloud-based services, but the survey found that 99% of respondents had never experienced a breach of security when using cloud services.

One of the major trends seen in 2015 and continuing in 2016 is the growing use of managed cloud services that help organisations to embrace the opportunities that the cloud offers, but that lack the expertise to make the move to cloud unaided. Organisations providing ecommerce and other web-based services have extremely high uptime requirements, but hosting their own websites is not generally their main expertise. By using hosted services, they can benefit from enhanced security since the service provider provides security controls and is in the position to monitor security on a continuous 24x7 basis. A cloud hosting provider can also ensure that its customers have the bandwidth they require to handle all traffic, even during peak times, to ensure that they experience no downtime since they will have the computing resources required.

The Cloud Industry Forum found that 90% of respondents to its survey were satisfied with the results of using hosted and cloud-based services, with 56% having achieved greater competitive advantage through use of such services and a further 22% anticipating that they soon do so. Among the benefits of the use of such services are more flexible and faster access to technology, and improved customer service and engagement.

The need for security in the cloud and website trust

Visitors to websites that provide information or that offer goods or services need to be sure that any interaction with that site, especially where sensitive information is provided by them, is secure in order to engender their trust. Security breaches are everyday news and affect organisations of all sizes in any industry. According to ***PwC***, 90% of large organisations and 74% of small firms have had a security breach in the previous year. Organisations must do all that they can to prevent breaches occurring in order to maintain the trust of their customers.

Whilst many breaches are of internal systems, organisations offering goods and services via websites must pay particular attention to website security. However, according to ***Symantec***, three-quarters of websites that it has scanned for vulnerabilities contained security issues in 2014. Whilst that is roughly the same proportion as it found the previous year, the percentage of vulnerabilities that were classed as critical increased by 30% in 2014 over 2013. Critical vulnerabilities include those that could allow attackers to access sensitive data, alter the website's content or compromise the devices of visitors. In total, it estimates that 95% of websites do not even have basic security controls in place.

Digital certificates are one of the most important components of protecting websites by encrypting data and making transactions secure. They attest to a website's authenticity and integrity, showing visitors that data, communications and transactions are protected.

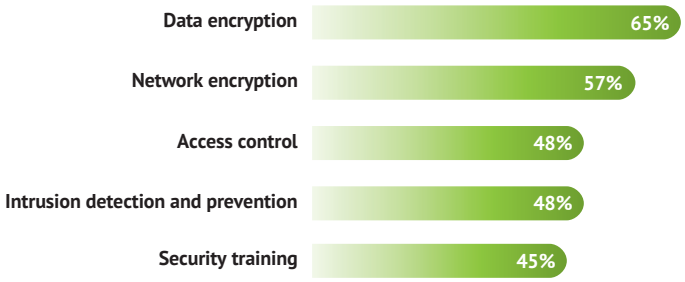
Among the most common of such certificates are secure sockets layer (SSL) certificates. A successor to SSL has been developed in the form of transport layer security (TLS). For convenience all mentions of SSL here refer to SSL/TLS. SSL, which is a transaction layer security protocol for securing communications and authenticating users, shows site visitors that the site is trustworthy and secure and that data provided to the site by them is secure because it is encrypted and cannot be intercepted by a third party. An SSL certificate shows that all data that is provided to a website by a visitor, including credit card number, personal details or account information such as passwords, has been encrypted.

According to Symantec, SSL certificates can be considered to be similar to passports because they have the following characteristics:

- They are secured artefacts that vouch for the identity of the holder.
- They are provided in a standardised form agreed upon by all issuers through the CA Browser Forum.
- The trustworthiness of the artefact depends on the issuer and the type of certificate.
- The artefact identifies the holder.
- The artefact is valid for a set period of time.
- The artefact is tamper resistant.

> **According to Symantec, SSL certificates can be considered to be similar to passports.**

Figure 1: Most effective controls for data protection



Source: ***Share the cloud security spotlight report***

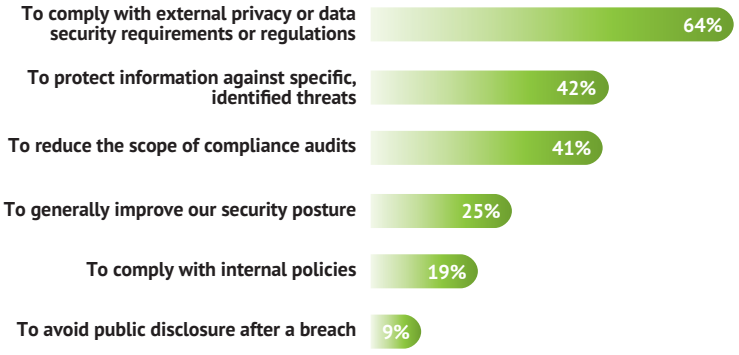
Website visitors associate SSL trust seals on websites, which indicate that the certificate is valid, as indicating that the website is trustworthy. According to ***Symantec***:

- 80% of consumers are aware that the padlock symbol signifies the use of SSL encryption.
- 81% know that HTTPS means that the internet connection is secure.
- 75% state that they would abandon an online transaction if they had doubts over a website's security.
- 55% know that the green address bar indicates that an extended validation SSL certificate is being used.

- One in three state that they would be deterred from completing a transaction if the website does not display a trust seal.

Data protection controls are necessary for ensuring consumer trust in services over the internet, which will protect organisations' brands and reputations. As can be seen in **Figure 1**, encryption is one of the most essential controls for ensuring data protection. Through use of SSL certificates, web-based services providers are indicating to site visitors that the site can not only be trusted, but has the strong encryption mechanisms in place for securing and protecting customer data. SSL encryption is a key component of website security.

Figure 2: Main drivers for use of encryption



Source: ***Ponemon Institute***

However, attackers have shown that SSL certificates themselves can be vulnerable and, in recent years, there has been a steep rise in attacks that look to gain possession of and use SSL, VPN and SSH cryptographic keys and certificates to steal data. In this way, the attackers are able to decrypt communications or use encrypted communications to mask their actions. When the ***Heartbleed*** vulnerability was discovered, it was estimated that half a million, or 17% of all secure web servers that have been provided with certificates by trusted certification authorities were believed to be vulnerable, allowing attackers to retrieve the associated private keys. Roughly three-quarters of Global 2000 organisations with public-facing systems were still vulnerable in 2015. Heartbleed allows an attacker to extract data, including SSL keys from digital certificates without being detected. Rather than applying a patch, it is recommended that all SSL certificates should be considered to be compromised and should therefore be revoked and reissued using a version of OpenSSL that doesn't have the Heartbleed vulnerability, since this vulnerability enables websites to be spoofed, as well as data decrypted. By using a managed security platform service, those organisations could easily have been issued with replacement certificates in a timely manner.

Gartner estimates that the use of encryption to mask the activity by attackers will constitute more than 50% of network attacks by 2017. Organisations must do all they can to avoid their private keys being compromised and, in the event that they are, all SSL keys and certificates must be replaced.

There has also been a rise in ***malware that uses stolen certificates*** to propagate. In 2014, 27% of Android malware was using stolen certificates, up from 0% in 2012, and 99% of certificates are vulnerable to attack. When Stuxnet was discovered, it signalled to attackers the advantages of using stolen certificates, many of which were of well-known companies. By 2013, some ***800 trojans*** were known to steal certificates and the number has swelled since then. According to ***Gartner***, there was a 700% increase in certificate-enabled malware from 2012 to 2015.

According to the ***Ponemon Institute***, every single organisation that responded to its recent survey of trust-based attacks has had to respond to multiple attacks that misuse keys and certificates over the past two years. It estimates the cost of such attacks over the coming two years will be US$53 million. Failure to adequately implement SSL encryption has already led to some organisations being fined by the Federal Trade Commission on the basis that those organisations had disabled their certificate validation process.

In order to be able to mitigate trust-based attacks, organisations need a way to replace all keys and certificates that have been compromised. However, spreadsheets remain a common method used by security teams for tracking all of their certificates.

Business requirements for and benefits of deploying SSL certificates

The three key business requirements for adopting SSL are to maintain compliance with regulatory requirements, user trust and system availability.

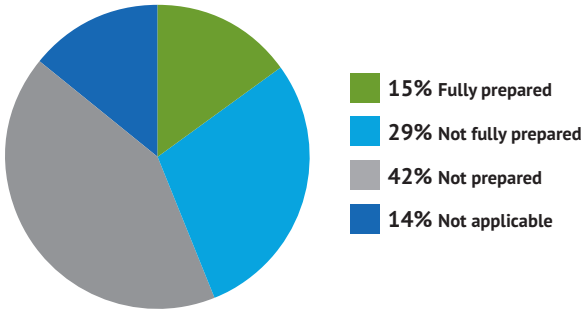
There are a wide range of regulations and industry standards that place an emphasis on data and privacy protection. Some of these impact particular industries; others are more general in nature. SSL technologies are a core component of establishing the foundation of compliant IT systems.

The EU general data protection regulation, that builds on and updates the data protection directive of 1995, applies to all cloud services and hosting providers that hold and process data on EU citizens, no matter where they are based. By encrypting data, the need to inform data subjects whose personal data could potentially have been compromised is removed if the data was encrypted, as long as the encryption was properly implemented. Where a certificate is invalid, because it has been compromised, revoked or has expired, will mean that the encryption is not properly implemented. With the general data protection regulation, fines for violations are being increased dramatically. For a serious breach, organisations can be fined up to 20 million euros or 4% of global turnover, whichever is higher. As **Figure 3** shows, very few organisations believe that they are fully prepared to meet the challenges of this new regulation.

Whilst maintaining trust involves the use of many security controls, the comprehensive use of SSL to encrypt all data in motion will help the customers of hosting providers to maintain user trust. However, it is important that this be adequately conveyed to users so that they trust the websites with which they are interacting. Different levels of certificates display to users that SSL has been implemented and that certificates are valid.

The need for engendering customer trust by ensuring that personal information is protected has been growing recently, not just owing to the growing number of breaches being seen, but also over fears regarding surveillance. Whilst estimates show that around 95% of websites still don't have basic security in the form of authentication, encryption and validation via trust seals, recent *research* shows that the use of SSL is increasing, with a quadruple rise seen in SSL traffic in Europe in the past couple of years. Much of this growing interest in the use of SSL has been driven by the revelations regarding widespread surveillance made by Edward Snowden in the documents that he leaked showing the extent of this. It is expected that the growth in the use of SSL will accelerate.

Figure 3: Organisational preparedness to comply with the general data protection regulation



Source: ***Cloud Security Alliance***

The use of valid SSL certificates will also help ecommerce and other web-based service providers to maintain their service availability by ensuring that the website has not been spoofed.

Another reason why hosting providers should offer their customers a security as a service is that it will help their ecommerce customers to ensure that they are well ranked by search engines. Google announced in 2014 that the fact that websites are protected by SSL certificates will be a growing factor in its search rankings and will likely grow further in importance over time. Hosting providers that offer their customers a managed SSL service will therefore be helping their customers to better reach their own clients for their web-based services.

The need for a managed security platform

Certificates are valid for defined periods of time and need to be managed throughout their lifecycle. That lifecycle involves issuing certificates, managing the inventory in terms of how many there are, what type they are, where they are deployed and their expiration dates, replacing certificates when they expire, and revoking certificates that are no longer valid or that have been compromised. Managing all certificates throughout their lifecycle is a daunting task for any organisation without the process being fully automated, but is especially so for hosting providers that need to manage certificates for a large number of customers.

A managed security platform simplifies all stages of the certificate lifecycle process, from certificate issue to renewal and revocation. A certificate that is no longer valid means that the site is no longer protected, leaving visitors vulnerable to phishing schemes or to theft of their personal and financial information. When visitors see that a website's certificate is no longer valid, they are likely to not trust that site and may take their business elsewhere.

Through a managed security platform, the entire lifecycle process is the responsibility of the service provider, which vastly simplifies the processes involved for hosting providers. Hosting providers enable their customers to use the certificates provided by the service to authenticate themselves, validate and secure their offerings, including transactions, and to enable their customers to fight off malware threats and cyber attacks.

By using such a service, hosting providers are provided with a centralised view into all the certificates that they are managing, as well as full automation over certificate lifecycle processes. This should be provided via a portal that provides full end-to-end automation capabilities, as well as APIs that make it easy for developers to integrate the service with other tools.

Through the use of such a service from one trusted vendor, hosting providers can take advantage of complementary security features and controls such as managed firewalls, vulnerability assessments and malware scanning, without the need to purchase and implement all such controls separately.

“When visitors see that a website's certificate is no longer valid, they are likely to not trust that site and may take their business elsewhere.”

Benefits for hosting providers

Hosting providers are finding themselves under increasing pressure to offer their customers a full portfolio of services that integrate with their existing infrastructure such as DNS servers and a variety of control panels that include WHMCS automation, cPanel and more, as well as existing processes. To do this, they need to partner with a trusted provider that can offer the support processes that are required to ensure that the needs of their customers are fully catered for. At present, some rely on the use of free products, but those are likely to incur costs in their implementation and management, which is also not an easy undertaking. With a managed security platform service, the guesswork is taken out of making appropriate security decisions as the service provider can map the required controls to web-based service providers in the context of their existing environment and their business needs. Such a platform will simplify the entire security lifecycle and is highly scalable, allowing hosting providers to onboard thousands of customers and rapidly issue high volumes of certificates. They can place orders via bulk or transactional APIs for issuing certificates, and partners will be able to rapidly revoke and reissue certificates in the case of vulnerabilities such as Heartbleed.

At a basic level, hosting providers will be able to provide their customers with free domain validation certificates. These are basic certificates that offer encryption, but provide only basic authentication in the form of verifying that the organisation applying to use the certificate has the right to use a specific domain. For those organisations that wish to apply certificates to further domains, the hosting provider has the opportunity to derive further revenue from those customers by upselling to domain validated wildcard certificates, which provide protection for multiple subdomains. They would also have the opportunity to upsell extended validated certificates, which verify that a particular organisation owns a particular domain and that the organisation's validity has been verified. These certificates provide visitors to a website with visual clues that the site is secure, including a padlock icon and by turning part of the browser address bar green.

Hosting providers will also be able to generate further revenues by offering premium services to their customers such as a regular scanning service to identify malware or vulnerabilities on a customer website. Search engines such as Google blacklists websites known to contain malware, removing them from its search listings. This, along with ongoing management of certificates, enables their customers to better achieve higher levels of security and meet their regulatory compliance obligations, along with protecting their SEO investments.

By offering security services to their customers, hosting providers will have the opportunity to increase their market share. According to ***analysts***, the web hosting market is seeing annual growth rates of 17%, with one or two new websites being created every minute of the day. Visitors to and customers of those websites are requesting that higher levels of security be provided and website owners are increasingly asking their hosting providers to help them to meet those needs. By providing their customers with the ability to more easily implement security measures, hosting providers will appeal to more customers, allowing them to benefit from the high levels of growth being seen in the market.

As **Figure 4** shows, by providing their customers with security services, hosting providers will be able to help them engender trust in their own customers, which will allow them not only to retain their own customers, but to attract new ones.

As well as being able to engender loyalty among their customers, the use of a managed security platform will provide benefits to the hosting providers themselves in terms of lower costs and complexity in offering their services. Hosting providers will be able to lower their costs by having access to a set of fully automated, integrated services from one trusted vendor, reducing both the costs and effort of manual processes, administration and integration.

Figure 4: Trust issues with online visitors

Source: ***YouGov***

Summary

Web security is a serious issue and one that can derail operators of web-based services if they suffer an incident that destroys the trust that their customers have in them. With many providers of such services turning to hosting providers to help them operate their businesses, there is a growing opportunity for those hosting providers to help them to ensure that their web-based offerings are secure. Since SSL certificates are an important part of web security, validating that a website is secure and authenticating the owner, a security platform aimed at hosting providers will help those that use them to differentiate them from the competition and to engender loyalty and trust among their own customers.

“...a security platform aimed at hosting providers will help those that use them to differentiate them from the competition and to engender loyalty and trust among their own customers.”

FURTHER INFORMATION
Further information is available from
www.BloorResearch.com/update/2282

About the author

FRAN HOWARTH
Senior Analyst, Security

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including Silicon, Computer Weekly, Computer Reseller News, IT-Analysis and Computing Magazine. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of InfoToday.

Bloor overview

Bloor Research is one of Europe's leading IT research, analysis and consultancy organisations, and in 2014 celebrated its 25th anniversary. We explain how to bring greater Agility to corporate IT systems through the effective governance, management and leverage of Information. We have built a reputation for 'telling the right story' with independent, intelligent, well-articulated communications content and publications on all aspects of the ICT industry. We believe the objective of telling the right story is to:

- Describe the technology in context to its business value and the other systems and processes it interacts with.
- Understand how new and innovative technologies fit in with existing ICT investments.
- Look at the whole market and explain all the solutions available and how they can be more effectively evaluated.
- Filter 'noise' and make it easier to find the additional information or news that supports both investment and implementation.
- Ensure all our content is available through the most appropriate channels.

Founded in 1989, we have spent 25 years distributing research and analysis to IT user and vendor organisations throughout the world via online subscriptions, tailored research services, events and consultancy projects. We are committed to turning our knowledge into business value for you.

Copyright and disclaimer

2nd Floor
145–157 St John Street
LONDON EC1V 4PY
United Kingdom

Tel: **+44 (0)207 043 9750**
Web: **www.BloorResearch.com**
email: **info@BloorResearch.com**