FROST & SULLIVAN

50 Years of Growth, Innovation and Leadership

The Growing Hacking Threat to Websites: An Ongoing Commitment to Web Application Security

A Frost & Sullivan White Paper

Chris Rodriguez,
Senior Industry Analyst

Richard Martinez,
Research Analyst

www.frost.com

CONTENTS

ACKNOWLEDGEMENTS

Frost & Sullivan would like to thank Robert A. Martin of MITRE, Ilia Kolochenko of High-Tech Bridge and Craig Spiezle of OTA for their excellent support and insight in writing this white paper.

The MITRE Corporation is a not-for-profit organization that provides systems engineering, research and development, and information technology support to the government. It operates federally funded research and development centers for the Department of Defense, the Federal Aviation Administration, the Internal Revenue Service and Department of Veterans Affairs, the Department of Homeland Security, and the Administrative Office of the U.S. Courts, with principal locations in Bedford, Mass., and McLean, Va. http://cve.mitre.org/

High-Tech Bridge SA provides multinational companies, financial institutions and international organizations with edge-cutting information security solutions and services. In 2012, Frost & Sullivan has recognized High-Tech Bridge as one of the market leaders and best service providers in the ethical hacking industry. https://www.htbridge.com/

Formed as an industry working group in 2005 and approved as an Internal Revenue Service (IRS) 501c6 non-profit in September 2007, the Online Trust Alliance (OTA) is a non-profit with the mission to enhance online trust, while promoting innovation and the vitality of the internet. https://www.otalliance.org/

INTRODUCTION

"Web applications have become vital to almost any organisation, but these applications can be dangerously weak links in the network security perimeter."

The World Wide Web is the growth engine of our decade. Because the Web has the power to make everything available to anyone, anytime, where ever they are, through which ever device, even century-old businesses are adopting Web-centric business models. Government information systems are also becoming Web-centric because they, too, realise that technology allows them to meet and exceed the expectations of citizens with lower budgets. In essence, Web applications have become vital to almost any organisation, but these applications can be dangerously weak links in the network security perimeter.

Google and Amazon are well-known examples of companies that rely almost entirely on Web applications for their business; Netflix is showing the way in the home entertainment industry, and even grocery shopping is becoming Web-centric. Social networks, such as Facebook, have introduced gaming (e.g., Farmville), image sharing (e.g., Instagram), and other Web applications that give insight to users and their activities. Businesses are increasingly adopting social media into their marketing strategies. At the same time, services like ICQ or MSN Messenger (that are much more powerful, but require additional software to install) are losing popularity.

More and more hardware devices—from industry equipment to telephone systems—are supplied with administrative Web interfaces. Ceridian Payroll & HR and Salesforce CRM are examples of essential and highly sensitive systems built on Web applications.

Since the 90s, we have seen a steady proliferation of Web application vulnerabilities. As soon as system administrators and developers acknowledge one attack vector, a new attack vector is already being developed by hackers. Security research labs and vendors are implementing extensive testing methods to find and patch vulnerabilities.

For example, Frost & Sullivan found that in 2011, third-party researchers disclosed 98.3 percent of total vulnerabilities for the year, while application developers only disclosed 1.7 percent. This is further validated by security labs stating they have shifted their testing from being customer-driven to analyzing all applications, primarily those that are highly valuable to businesses, widely deployed, and have a reputation for being vulnerable.

This paper puts the threat to Web applications into its right business context. The reader is able to peak into the mysterious world of Web applications hacking, catching a glimpse of the workings of hackers and how they are able to attack unsuspecting organisations, powerful governments and even private persons. Finally, the paper gives an overview of the likely victims of Web application hacking and outlines what organisations should be doing to protect themselves.

The paper benefits from the insight and experience of leading security organizations and companies like MITRE, Online Trust Alliance (OTA), and High-Tech Bridge, which have provided excellent support to Frost & Sullivan during the editing and review of the paper.

THE THREAT TO WEB APPLICATIONS

Today Web applications are becoming powerful and complex, providing a rapid and simple attack vector that continues to attract hackers. Increasing adoption of Web 2.0 functionality and powerful features of HTML5 have further enhanced the opportunity for hackers to exploit vulnerabilities. The more complex a technology is, the more potential vulnerabilities and weaknesses it contains. Web applications remain the third most common attack vector overall, and while the number of recorded breaches has decreased somewhat, the data theft with which they are associated is on the rise.

"Anything you use on your website can be and will be used against you."

— Craig Spiezle, Executive Director & President, OTA

Targeted and Untargeted Attacks

First of all, it is necessary to distinguish between targeted and untargeted attacks against websites. Untargeted attacks are launched simultaneously against as many websites as possible without prior knowledge of the possible outcome. Most of the attacks on websites are untargeted attacks.

The most common method to launch an untargeted attack against a website is to use a worm or crawler (similar to Google-bot) that surfs millions of random websites all over the world every day, looking for a number of known vulnerabilities in well-known Web applications, such as Content Management Systems (CMS), blogs or forums. As soon as vulnerability is discovered, the vulnerable Web application is compromised. In the majority of cases, hackers integrate malicious software (malware) into the HTML code of all pages of the website. The goal of the malware is to compromise as many website visitors as possible and to install Trojan applications on their machines, turning the machines into zombies. Zombies are used to launch a second wave of untargeted attacks against new websites. Later, compromised machines are sold on the black market to be used to perform DDoS attacks, send spam, hide source of other attacks, host illegal content and perform other criminal activities. Today, unsecured websites are some of the main sources of malware spreading in the Internet.

Targeted attacks address a specific organisation or individual with a specific purpose. In a targeted attack, hackers use all available means of hacking, including social engineering combined with other types of attacks.

"... Each day in June, Symantec Intelligence identified an average of 2,106 new websites containing malware."

Examples of How Targeted Attacks are Perpetrated

a. A hacker uses brute force, steals or simply guesses a password to an employee e-mail account. The hacker then sends an e-mail from the employee's account to the Web team or IT department demanding to give/restore access to the administrative interface of the corporate website (many variations of social engineering are possible here, depending on the structure of the victim organisation and hacker's goal).

b. The hacker pretends to be a dismayed customer and sends an e-mail to the Web help desk alleging problems using website, attaching a DOC or PDF document with "details of the problem" or "payment confirmation." The attachment contains sophisticated malware exploiting 0-day vulnerability in Microsoft Office Word or Adobe Acrobat Reader, giving hacker access to the help desk PCs, where he can usually find credentials to access the website of the company.

c. With help of automated software or Google-hacking techniques, the hacker discovers and uses SQL injection vulnerability on a vulnerable website to get access to the admin panel. Hacker tries to upload a Web shell (a script that allows command execution and various file and database-related operations) to compromise the entire Web server. Once the hacker can execute system commands with privileges of the Web server, he tries to escalate privileges and get root/administrator access to the server (viz. absolute control). As soon as the hacker controls the server he may launch attacks on the local network of the victim (if the Web server is hosted in DMZ) and potentially get inside of the entire local network of the victim.

According to Craig Spiezle, executive director, founder and president of OTA, websites need to employ multiple tools to ensure there are no vulnerabilities and malware on the site from multiple sources (e.g., certificate authorities and anti-virus/security providers). For example, client-based solutions from Secunia look for plug-ins and applications on a site that are not patched or current. An endpoint solution, such as Symantec Norton, looks for exploits already on a machine. The combination of the two provides an end-to-end approach and should be employed on a server.

Malware Exposes New Targets to the Hacking Threat

The vast proliferation of malware has facilitated a much broader probing of the Internet, leading criminals to realise that there is an immense number of interesting targets that might have been ignored five years ago.

Given the abundance of Web application vulnerabilities and untargeted attacks described in the previous sections, it is hardly surprising that, each day in June, Symantec Intelligence identified an average of 2,106 new websites containing malware. Symantec Intelligence also reports an extreme fluctuation (in May, 4,359 sites were detected; in April, it was fewer than a thousand), making it very difficult to draw any conclusions about the development trend. *Source: Symantec Intelligence Report, June 2012*

When victims ignore the presence of malware on their systems, they unwittingly push valuable information out to hackers. Initially, keyloggers were a function of malware designed to capture all user typing. Modern keyloggers can intercept microphone and Web-camera inputs/outputs as well, and can take screenshots of user desktops at regular intervals defined by the hackers. Many other industry-specific functions may exist in malware. For example, malware that target banking and financial websites usually contain special algorithms to steal and/or intercept e-banking sessions of popular online banking systems.

Frost & Sullivan research shows that, in 2011, four applications commonly associated with websites—Adobe Shockwave Player, Adobe Acrobat, Apple QuickTime, and Microsoft Internet Explorer—were all on the top five list of applications with the most vulnerabilities overall. Vulnerabilities present in these applications—especially in older versions of the applications—are targeted by various exploit packs, such as BlackHole, Eleonore or Phoenix Exploit kits, hosted on compromised websites to perform drive-by attacks against website visitors.

Four out of Five Sites are Vulnerable

The Web Application Security Consortium (WASC) identifies almost 50 unique classes of website vulnerabilities, and 83 percent of websites have at least one serious vulnerability. Given these findings, the attack vectors and potential damage we have already described are, by no means, horror scenarios, but they are serious, looming threats facing most of us.

> *The details provided by several websites attest to the seriousness of the situation. XSS Attack Archive demonstrates that there is hardly a financial institution whose website has not been vulnerable to XSS attacks. Even more harrowing statistics come from the Zone-H site. Zone-H is popular with hackers wanting to make a "mirror" of a hacked website to prove later that the hack occurred. Currently, almost 7.5 million mirrors are available there, many of which belong to the financial industry, governments and law enforcement agencies.*

We also need to consider the possibility of human error and the security of system administrators and other privileged users' machines. Web masters, editors and all other people who have administrative access to the Web application are potential targets. In addition, the security of the server where the application is hosted must also be taken into consideration. In many cases, a perfectly secured Web application hosted on a vulnerable Web server (or on a server with other Web applications that contain vulnerabilities) can be compromised in just a couple of hours.

When evaluating Web application vulnerabilities caused by poor programming practices we must distinguish not only between various vulnerability types, described by MITRE's Common Weaknesses Enumeration (CWE), but also between various details and exploitation conditions of the vulnerability. For example, an SQL injection (CWE-89) that can be exploited by any unauthenticated user in default configuration is many times more dangerous than an SQL injection exploitable only via the CSRF (CWE-352) vector, because it needs to be

"The Web Application Security Consortium (WASC) identifies almost 50 unique classes of website vulnerabilities, and 83 percent of websites have at least one serious vulnerability."

The most reactive vendor in 2012 was the Serendipity team, which fixed a high-risk vulnerability (HTB23092) in 23 minutes!

authenticated as an administrator on the vulnerable system.

The Common Vulnerability Scoring System v2.0 (CVSSv2) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSSv2 scores consist of three groups: Base, Temporal and Environmental. Each group produces a numeric score ranging from 0 to 10 and a vector, a compressed textual representation that reflects the values used to derive the score. CVSSv2 enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit from a common language for scoring IT vulnerabilities.

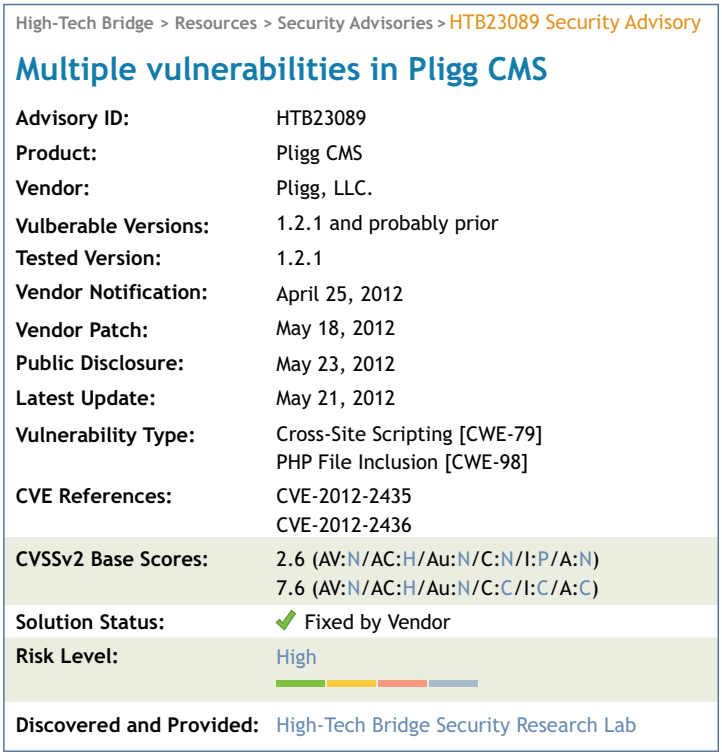
The higher the CVSSv2 base score, the more serious the vulnerability. Two CVSS scoring examples from High-Tech Bridge Security Advisories are provided below:

High-Tech Bridge > Resources > Security Advisories > HTB23084 Security Advisory

Multiple vulnerabilities in Pligg CMS

Advisory ID:	HTB23084
Product:	Newscoop
Vendor:	Sourcefabric o.p.s.
Vulberable Versions:	3.5.3 and probably prior, partially 4.0 RC3
Tested Version:	3.5.3
Vendor Notification:	March 28, 2012
Vendor Patch:	April 5, 2012
Public Disclosure:	April 18, 2012
Latest Update:	April 23, 2012
Vulnerability Type:	PHP File Inclusion [CWE-98] SQL Injection [CWE-89] Cross-Site Scripting [CWE-79]
CVE References:	CVE-2012-1933 CVE-2012-1934 CVE-2012-1935
CVSSv2 Base Scores:	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C) 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P) 2.6 (AV:N/AC:H/Au:N/C:N/I:P/A:N)
Solution Status:	✓ Fixed by Vendor
Risk Level:	High
Discovered and Provided:	High-Tech Bridge Security Research Lab

https://www.htbridge.com/advisory/HTB23084



High-Tech Bridge > Resources > Security Advisories > HTB23089 Security Advisory

Multiple vulnerabilities in Pligg CMS

Advisory ID:	HTB23089
Product:	Pligg CMS
Vendor:	Pligg, LLC.
Vulberable Versions:	1.2.1 and probably prior
Tested Version:	1.2.1
Vendor Notification:	April 25, 2012
Vendor Patch:	May 18, 2012
Public Disclosure:	May 23, 2012
Latest Update:	May 21, 2012
Vulnerability Type:	Cross-Site Scripting [CWE-79] PHP File Inclusion [CWE-98]
CVE References:	CVE-2012-2435 CVE-2012-2436
CVSSv2 Base Scores:	2.6 (AV:N/AC:H/Au:N/C:N/I:P/A:N) 7.6 (AV:N/AC:H/Au:N/C:C/I:C/A:C)
Solution Status:	✓ Fixed by Vendor
Risk Level:	High
Discovered and Provided:	High-Tech Bridge Security Research Lab

https://www.htbridge.com/advisory/HTB23089

High-Tech Bridge Security Advisories are provided on a non-profit base, with the aim of helping various software vendors improve their products' security and reliability. High-Tech Bridge is CVE Compatible and uses CVE Identifiers in its security advisories, alongside its own HTB advisories IDs. More than 180 different software vendors have released security patches and improved security of their products thanks to High-Tech Bridge Security Research Lab. High-Tech Bridge makes every effort to help vendors eliminate discovered vulnerabilities in a reasonable time. According to HTB Research Lab statistics, 88 percent of vendors fixed discovered vulnerabilities in 2012 Q1 and 90 percent in 2012 Q2.

CVSSv2 scores are valuable starting points to assess the seriousness of a vulnerability, but organizations must evaluate vulnerabilities in the context of their own network architecture and unique sets of security requirements. CVSSv2 scores are calculated from 14 separate intuitive inputs provided by software providers or security companies.

Three out of Four Network Intrusions Start with an Unsecured Web Application

The real problem with unsecured Web applications is the threat they pose to an organization's network and intellectual property, not the potential damage to the website itself. However, sometimes just a damaged website may cost millions in direct losses and much more in terms of tarnished reputation.

"More than 180 different software vendors have released security patches and improved security of their products thanks to High-Tech Bridge Security Research Lab."

The best known example of an APT is the Stuxnet attack. The Stuxnet worm spread through and targeted sensitive Iranian nuclear production facilities. The malware was designed to remain hidden, and the malware's authors were then able to subtly sabotage the facilities over the course of many years while also extracting data.

All security companies base statistics on their individual case loads, so the statistics may vary. According to High-Tech Bridge, as many as three out of four successful network intrusions start and/or involve an unsecured Web application. There are several reasons that Web applications are prime starting points for network intrusions. First, Web application vulnerabilities are much easier and faster to exploit than a buffer overflow vulnerability in a network service. Today, various buffer and heap overflow vulnerabilities in network services are becoming rare and quite difficult to exploit in comparison to Web vulnerabilities. However, in many cases a successful intrusion into a corporate website gives almost exactly the same outcomes as intrusion into a corporate network. In any case, control over the victim's website provides additional launch points for follow-up attacks.

By "network intrusion" we mean attacks where the goal is to achieve ongoing access. To maintain access without discovery, the hacker must continuously rewrite code and employ sophisticated evasion techniques. The attack becomes categorised as an advanced persistent threat (APT). The purpose of an APT is always to steal data, rather than to cause damage. APTs target organisations in sectors with high-value information, such as defence, manufacturing and financial organizations.

Once inside, a hacker moves laterally across the network, installing more back doors. The back doors allow the attacker to install bogus utilities and create a "ghost infrastructure" for distributing malware that remains invisible to the naked eye. Or the hackers stay hidden and come back to collect data, depending on their motives. System administrators may discover the APT due to anomalies in outbound data, but before that happens, the damage may already be severe.

A Simple Web Vulnerability can Compromise an Entire Organisation

The complexity of an attack and the victim's internal architecture will determine how much damage a hacker can do. However, today even a simple XSS on a website combined with social engineering and designed to infect the network administrator's PC with a Trojan could result in the total compromise of the entire local network of an organization. If a Web application has access to the organisation's database with all customers and orders (a common situation for many online businesses), then even a tiny Web application vulnerability can result in the entire organization being compromised.

The database structure behind a website is much more important than the structure of the website itself. In almost every case, a compromised Web application gives unlimited access to all the resources that the Web application uses (including the databases). When hackers have achieved read/write access to the Web application, any information submitted by website visitors can be intercepted, redirected and abused. Private portals (e.g., for partners or employees) could be completely separate from an organisation's public-facing website, but if the private portals share the same database with the public site, then it may represent a catastrophic risk, as any vulnerability in the public website will give full access to the confidential information in the private portals.

As explored in the Frost & Sullivan white paper "The Importance of Ethical Hacking—Emerging Threats Emphasise the Need for Holistic Assessments," hackers frequently attack the trusted partners of their real victims. Web developers usually consider partners to be trusted parties and often take insufficient security measures while implementing security of Web portals and applications designed to be used by trusted third-parties only. Organizations must be vigilant that their partners ensure the protection of their accounts against breaches and misuse.

The threat landscape has changed to compromise users upstream rather than downstream. This means that rather than attack the user directly, attackers are targeting the trusted supply chain (e.g., partners, suppliers, legal advisors, and even Certificate Authorities).

—Ilia Kolochenko, CEO High Tech Bridge SA

WEB SECURITY IS AN ONGOING COMMITMENT

It would be easy to blame Web developers for the vulnerabilities in Web applications, but laying blame is neither fair nor constructive. Websites develop over time. No development team has time and resources to review all existing code for vulnerabilities when new code is written, and QA and third-party auditing of Web application code is rare. Web security is an ongoing commitment that organisations must make themselves.

In essence, an organisation can never be certain to have a zero-vulnerability website even if the utmost care is taken during development. Even if that were the case, there is no way that we could future-proof out code. Developers can only take vulnerabilities into account that are known at the time of development. A Web application can be safe today and vulnerable tomorrow.

As part of the ongoing commitment to security, it is important to document applications, plug-ins and legacy items on a server; determine what risks they imply; and then make an informed decision about what is allowed to reside on the server. Another major issue arises when organisations migrate their systems to new servers. Many organisations will also move legacy applications onto the new server, even if the legacy applications are no longer being used. They may be kept for backward compatibility, or they are just plain forgotten. This creates an opportunity for hackers, as most of these applications will not have been patched or updated. OTA's recommendation is usually to remove or isolate legacy applications from the production server.

Finally—and this is particularly relevant to organisations that outsource Web development—Web developers will not take responsibility of the overall security of a website, unless they are specifically asked to do so and paid to do so and, most importantly, have the necessary skills to do so. Web development is a competitive business, and many sites are developed on a shoestring. Organisations will receive the service they pay for, for better or worse.

Network Firewalls, Secure Socket Layer (SSL) Encryption and Back-Up Fall Short

SSL encryption and network firewalls are important measures to implement on a network, but they do not stave off the Web hacking threat. SQL injection (SQLi) and Cross-Site Scripting (XSS)—the two most common Web vulnerabilities—pass straight through Web server ports that are open on any Web server by design. Traditional network firewalls are simply not designed to perform any filtration on the seventh level of the OSI model—the application level, where Web application vulnerabilities are present.

"The role of SSL today is to encrypt data exchange and identify the website owners in a trustable and reliable manner."

SSL protocol only encrypts data in transit, making it difficult for hackers to use or falsify any intercepted data. SSL protocol was only designed to protect transaction security and does not protect against Web application attacks. The second important function of SSL protocol is identification of two parties who exchange information. An SSL certificate issued by reputable and trustworthy Certificate Authorities (e.g., VeriSign) can clearly identify the website owner and prove that the website is legitimate. SSL EV certificate (the famous "green bar") goes even further in identity verification, assuring that the website behind the certificate belongs to an existing and clean legal entity. The role of SSL today is to encrypt data exchange and identify the website owners in a trustable and reliable manner. However, even the Certificates Authorities cannot be safe from hackers today, especially if they do not care about security of their own Web applications. In 2011, various Certificate Authorities were hacked, permitting hackers to issue fake SSL certificates, and thus exposing SSL traffic to risk. Symantec's 2012 Internet Security Threat Report states that Certificate Authority websites saw an unprecedented number of attacks in 2011.

The DigiNotar Case

The worst case took place from July 2011 to August 2011, involving DigiNotar, the primary certificate authority used by the Dutch government. A single attacker hacked into DigiNotar's network and issued more than 500 false certificates. When the breach became public knowledge, DigiNotar's customers abandoned it in droves. Within one month, DigiNotar filed for bankruptcy. The network intrusion was the result of unpatched Web server software, weak passwords, a lack of Web server anti-virus, and poor network segmentation on the part of DigiNotar. According to the official report, "all CA servers were members of one Windows domain, which made it possible to access them all using one obtained user/password combination." The investigation showed that the hacker had been in the system undetected from June 17 to July 22. This is a good example of how a compromised Web server can have potentially catastrophic consequences.

Industry pundits speculate that the same hacker was responsible for the March 2011 attack against Comodo. The hacker obtained the access credentials of a Comodo Trusted Partner in Southern Europe and was able to issue nine false SSL certificates to sites in seven domains. In this case, the breach was detected within hours and the false certificates revoked.

An interesting perspective offered by OTA is that, although websites are hardening their infrastructures, content and ad-sharing sites are being targeted and compromised. The danger in this is that phishing filters become ineffective. Website owners lack visibility into ads from trusted third-parties serving content to the first-party site. Examples of this situation include Major League Baseball and the New York Times website. The sites did not do anything wrong, but their contractually provided third-party ad content providers were attacked. Site owners must make sure their sites and third-party provided content is secure.

Even if stored data were protected by a strong encryption algorithm and an organisation had servers mirroring each other for real-time back-ups, data poisoning can still alter the files on the primary server and the back-up.

Deep Packet Inspection (DPI), Intrusion Prevention Systems, and Web Application Firewalls (WAF) are Essential Basics

No modern application can be made 100 percent secure and still be 100 percent functional and user-friendly. Layered security is a sensible approach to optimising security by deploying IPS at different points of the network, even inside the corporate firewall (to mitigate the threat from insiders). In very simplified terms, IPS analyses all traffic, trying to distinguish "bad" traffic from normal traffic, but few of them can effectively monitor the behaviour of Web applications. DPI is a relatively new and quite efficient approach to network traffic inspection and filtration, as it represents a combination of IPS and firewall that is able to perform filtration on all OSI levels, except the physical one.

A common solution to monitor and filter malicious traffic to Web applications is a WAF. The OWASP definition of WAF is that it is an appliance, server plug-in, or filter that applies a set of rules to a HTTP conversation. WAFs are deployed in front of the Web application, and they analyse inputs to Web applications (e.g., queries or keywords typed into a search box on a Web page). Typically, an attack against a Web application has identifiable patterns that would trigger the WAF. Because a correctly configured and tested WAF does provide efficient protection against common attack vectors (such as XSS and SQLi, as well as various code and command injections) for a very specific Web application, many people think that WAF is a universal solution, moreover that "one configuration fits all" applications, which is wrong. A properly configured WAF can protect a very precise and limited scope of a Web application, but the WAF cannot assure proper protection following any modification or update of the application. Moreover, modern WAF cannot protect against application logic errors, or some other types of new attacks that are appearing because of new features of HTML5.

"... WAF can protect a very precise and limited scope of a Web application, but the WAF cannot assure proper protection following any modification or update of the application."

Efficient WAF configurations can't block any legitimate users and at the same time must not miss any malicious HTTP requests. Constant WAF updates and monitoring are required to achieve this balance. Consequently, many organisations use wrongly or sub-optimally configured WAFs that don't provide total protection from hackers, or will prevent legitimate users and customers from working with their website. Moreover, even minor modifications to the Web application could create new, critical vulnerabilities—much like a zero-day vulnerability—unless the WAF is correctly reconfigured in parallel. Whereas that may sound simple in theory, the reality is that the programmers who write the Web application code will rarely be completely co-ordinated with the security professionals who reconfigure the WAF. They might even work in completely different companies.

This is why regular penetration testing of Web applications remains vitally important, even in organisations that have deployed DPI/WAF solutions.

THE PERPETRATORS OF WEB HACKS

According to Frost & Sullivan's research, for 2011, 92 percent of data breaches stemmed from external agents (a 22 percent increase from 2010); 17 percent implicated insiders; less than 1 percent resulted from business partners; and 9 percent involved multiple parties. Verizon DBIS 2011 reports that an even higher number (98 percent) of perpetrators were external agents.

"Black Hats are the invisible hand of the market. [...] They remain undetectable in most of the cases."

According to High-Tech Bridge, the picture is different if we look at targeted attacks in isolation. High-Tech Bridge believes that in roughly half the targeted attacks, there will be an accomplice inside the victim organisation. What is hugely important to understand, however, is that insiders will often not realise that they are helping hackers. Via social engineering, they may be tricked into unwittingly handing over credentials and other information to hackers. There are even situations in which employees are threatened by hackers to become accomplices against their will.

Essentially, there are three types of perpetrators: organised criminals (or "Black Hats"), vandals ("or Script Kiddies"), and activist groups (or "Hacktivists"). The types are not completely distinct, but we shall make an attempt at defining them.

Black Hats, Organised Criminals

Black Hats are the invisible hand of the market. They work for profit only, the cost of their operations running into hundreds of thousands of dollars. They steal information that they or their "clients" can turn into cash. They remain undetectable in most of the cases. According to Verizon DBIS, organised criminal groups were behind 83 percent of all breaches.

Although, arguably, hacking is a criminal offence, we do not include hacktivists into our definition of "organised criminals." Organised criminals are only motivated by profit, and they perpetrate the most complicated, costly and critical attacks.

The typical average website has limited value. It will be resold on the black market for about $10 to be used for spamming, phishing, scamming, gathering botnets, etc. However, banking, e-commerce, corporations and celebrity websites have enormous value. Typically, hackers sell these sites to black market resellers who have connections with governments, other criminals, private investigators, paparazzi journalists and businesses willing to pay staggering amounts for confidential information on their rivals. On such websites, the criminals usually try to install hidden and powerful backdoors to be able to come back and sell "updates" to their clients.

A UK government intelligence report estimates that, globally, there are up to 40,000 trades of financial data and personal information made every day and an estimated 13.2 million trades per year. In June 2012, the head of MI5, Jonathan Evans, said in an interview that, "Vulnerabilities in the Internet are being exploited aggressively not just by criminals but also by states. The extent of what is going on is astonishing." MI5 itself is working on countering "industrial-scale processes involving many thousands of people lying behind both state-sponsored cyber espionage and organised cyber crime," Evans added.

According to a NCC Group report, the U.S. and China together account for 38 percent of all hacking attempts worldwide, costing the global economy more than $43 billion a year. Russia comes in at number three. Verizon research suggests that the majority of perpetrators behind attacks against SMEs are from Eastern Europe. Attacks against larger organisations originate from all over the world.

High-Tech Bridge confirms this view. However, High-Tech Bridge also points out that, once detected, it can be difficult to establish the real geographic origin of an attack because the sources are almost always falsified and hidden behind multiple proxies. Hackers prefer to use proxies in countries with weak or inefficient e-crimes juridical systems.

In Frost & Sullivan's opinion, the biggest problem is that hacking is inherently done globally, but governments and police forces fail to collaborate due to legislation that is outdated and misaligned. The European Union Arrest Warrant explicitly removes the double criminality feature in cases of computer-related crime, but most other jurisdictions base their mutual legal assistance regime on dual criminality. Harmonising legislation and improving the investigative possibilities would help bring more hackers to trial.

Anonymous was accused of the biggest single data theft in history, against Sony's PlayStation Network in April 2011, affecting 77 million accounts. Anonymous denied any involvement, and later a group of Black Hats claimed to have 2.2 million credit card numbers from PSN users for sale.

Script Kiddies

Script kiddies are beginner hackers who hack mainly for fun and glory. The majority of arrested Web hackers are script kiddies because they lack the skill to completely cover their tracks, or because they boast too much about their exploits. Usually they try to take all the "glory" of the hack and spread this glory as much as they can. Although script kiddies are amateurs, they are immensely dangerous and often disregard the damage they cause.

Script kiddies use effective, easily downloadable hacking programs and sometimes even commercial software intended for legitimate security auditing. Even Google can be an effective tool for script kiddies. Google-hacking techniques can be used to identify potential Web vulnerabilities, as well as versions of installed software, which is very useful to select appropriate exploits.

Occasionally, script kiddies will deface websites to protest against something or charge their friends small amounts of money to accomplish a simple hacking task. However, that does not make them either hacktivists or Black Hats.

Hacktivists

Most security companies report an increase in the activities of the activist groups commonly known as "hacktivists." Verizon even talks about "reinvigorated conducts of activist groups" in 2011. Its caseload suggests that although hacktivists accounted for a small proportion of the 2011 attacks, they stole more than 100 million records. That is almost twice as many as the records stolen by Black Hats.

Taking down a website (e.g., using DDoS attacks) is easier than compromising it; indeed, DDoS utilities are fairly readily available and many hacktivists stop at that point. DDoS attacks can be bad enough, and the consequences can be much worse than simple annoyance and loss of business. The loosely associated hacktivist group Anonymous claims responsibility for taking down the websites of two Danish trade unions, 3F and HK, in protest against an ongoing dispute between the trade unions and a local business. Because the websites were unavailable at a crucial time toward the end of July 2012, 15,000 trade union members did not receive their unemployment benefits on time.

"A 2010 Canadian government report asserted that 86 percent of large Canadian companies had been victims or targeted attacks from Black Hats"

In August 2012, the blogging platform used by Thomson Reuters was hacked, leading to several false posts to its website, including a fabricated interview with a Syrian rebel army leader. Apparently, Thomson Reuters used an old, unpatched version of its WordPress platform, instead of the current version 3.4.1.

LulzSec, a largely U.K.-based group of hackers, has released a manifesto stating that "we do things just because we find it entertaining" and that "watching the results can be priceless." The group also draws attention to computer security flaws and holes by letting people know they have been hacked, such as the National Health Service in England.

Of course, LulzSec, Anonymous and other famous groups have some highly skilled hackers among their members, but quite often they do rely on fairly simple vulnerabilities (such as SQLi) to perform their attacks. Consequently, these attacks are perfectly avoidable. The FBI has highlighted this in its investigation of the Sony hack, and the Department of Homeland Security reached the same conclusion in a report published in 2011.

THE VICTIMS OF WEB APPLICATION PENETRATION

All organisations are potential victims. Intuitively, one would assume that large organisations with valuable data were exposed to a much higher risk than smaller organisations overall. Certainly, a number of high-profile attacks have involved prestigious names (e.g., Sony, RSA, Citicorp, Startfor, AT&T), with an excess of $200 million in losses. These breaches have generated a stronger awareness about the need for network security systems. In addition, several states have laws that require companies to publicly report any event in which their customers' personal information has been compromised, meaning that these are the attacks the public hears about.

A 2010 Canadian government report asserted that 86 percent of large Canadian companies had been victims or targeted attacks from Black Hats, and that efforts to steal intellectual property from the private sector had doubled since 2008.

No empirical data exists quantifying the impact of hacking as a whole, but many modelling attempts have been made to estimate its impact. The German intelligence agency BfV, for example, estimates that Germany loses $21 billion to $71 billion of revenue and 30,000 to 70,000 jobs each year due to intellectual property theft through hacking.

In Frost & Sullivan's opinion, the majority of serious website intrusions are never detected or never made public. True Black Hats always try to keep a low profile and remain as silent as possible. Hacking attacks in the media are usually caused by young hackers and hacktivists. There is clearly more "glory" involved in hacking a Charles Schwab than an unknown SME. Hence, decision-makers erroneously believe that Web hacks only target large organisations.

Small and Medium-Sized Organisations are Most at Risk

We have seen that most organisations (79 percent according to Verizon) become victims of hackers because their websites contain easily exploitable vulnerabilities that hackers identify at random.

The statistics calculated from the case loads of the different security companies all suggest that SMEs are very much at risk, and even if an organisation thinks it has no data of value, it can always be abused as a zombie.

"... When it comes to targeted attacks, Small and Medium-Sized Organisations face a huge risk"

According to Verizon DBIS, 85 percent of the targets of opportunity (or untargeted attacks, as we have called them in the white paper) are organisations with fewer than a thousand employees. Verizon also finds that three-quarters of these SMEs belong to the retail, trade and hospitality verticals, not usually verticals where large amounts of confidential (and therefore valuable) information is held.

Even when it comes to targeted attacks, SMEs face a huge risk. According to the June 2012 Symantec Intelligence Report, 36 percent of all targeted attacks (measured during six consecutive months) were directed at organisations with as few as 1-250 employees, a percentage which has doubled in six months. High-Tech Bridge agrees with this view, adding that "If an SME has something really valuable, the Black Hats will come. It is only a matter of time." Something really valuable that an SME could have is privileged access to the systems of a much bigger partner company. And as we have seen already, it is much easier and faster to compromise a poorly protected SME than to attack the prime target head on.

The 21st century economy relies on technology innovation, services, and intellectual property due to the hollowing out of the manufacturing sector over the past 40 years. Many of today's leading, most dynamic companies were SMEs in a not-so-distant past, and successful start-ups generally survive because they have an idea or a technology that is unique. In short, many SMEs are sitting on incredibly valuable information that is under threat from hackers every day.

At a theoretical level, organisations operating in poor and developing countries should be even more at risk, seeing that they have the majority of their Web applications running on free and open-source software, which is widely deployed and thus frequently targeted by hackers. However, there are no statistics to back up this view. Given the large number of SMEs that still show up in the caseloads of the Western-focussed security reports, we must assume that hackers know no geographic boundaries and that businesses around the world face the same risk.

Security is often Underfunded

The economic recession and the fear of entering into a double-dip recession has translated into budget cuts across many organisations. The public sector has taken a comparatively large hit. This situation has been compounded by constant media attention and sensationalist reporting by analysts and reporters. While it is true that economic growth has slowed down or halted, constant fear mongering has caused everyone to spend far less money. Unfortunately, security solutions are usually some of the first products to suffer from these effects in organizational budget discussions because they do not directly generate revenue.

Security vendors have traditionally struggled to demonstrate a return on investment, and while it is easy to put together a conceptual business case, backing up that business case with hard numbers is almost impossible. It is easy to quantify how much it will cost to repair

Applications that were never on the Internet are now becoming IP-enabled. Even applications that are not reachable by the Web are still on the Internet, such as CCTV cameras. Hackers can capture images from CCTV cameras to see employee keyboards (and their passwords when they type them).

a compromised system, but it is impossible to quantify the value of the damage to an organisation's reputation when that damage could last many years and even lead to bankruptcy.

In Frost & Sullivan's opinion, most of the Web application vulnerabilities that result in systems becoming compromised are perfectly avoidable. So why aren't they avoided; what is going wrong? In SMEs, the root of the problem is usually a lack of budget, time and qualified human resources. In large organisations, the main problems are complexity and bureaucracy when the division of responsibilities is not completely clear. Naturally, large organisations may come up against savage cost-cutting in short-term contingency plans. Security expenditures are always easy to cut because they do not hurt the organisation immediately. Later, of course, cutting security expenditure could ruin the entire organisation.

In many organisations—and this is just as true in public entities as it is in private entities—the strategic importance of IT is not recognised, and consequently, IT security is not sufficiently funded.

Web Security – Core or Chore?

Small and medium-sized organizations are the main victims of website hacks, and they are also the least prepared. Today, many companies employ Web-centric business models (their websites are mission-critical because most customer interaction takes place via the website). Many start-up companies employ a Web-only business model and would go out of business within a few days if their websites were unavailable. Organisations still have a tendency to regard Web security as a cost rather than an investment. In public organisations, services to citizens are increasingly made available through Web applications, which have enabled streamlining, cost reductions and higher user satisfaction, according to research conducted by Frost & Sullivan. This makes public websites equally mission-critical.

Although companies realise the threats and risks inherent in a poor security infrastructure, they view security as a chore when they should view security as a top priority (i.e., as core). Customers invest in security solutions out of fear and for compliance reasons. This will cause them to invest in the minimum level of security that will alleviate the worries and satisfy compliance requirements. Consequently, security has a more difficult sales process as revenue-generating investments receive higher priority.

Organisations need to measure the real value of their websites and prioritise Web application security accordingly. Aside from the incremental value of stolen data, organisations face lost business, lost customer trust, and potential embarrassing investigations and heavy legal fees when they fail to adequately protect their Web applications.

MITRE, THE ORGANISATION BEHIND CVE AND CWE

Frost & Sullivan's network security Senior Industry Analyst Chris Rodriguez interviewed Robert A. Martin, senior principal engineer and outreach lead of MITRE Corporation, the not-for-profit organisation applying its expertise in systems engineering, information technology, operational concepts, and enterprise modernisation to their sponsor's problems.

MITRE's goal is to ensure that everyone is speaking about the same things by "making security measurable." According to Martin, the problem started years ago as different technology disciplines identified security problems and the need to fix them. These researchers developed the techniques and tools that best fulfilled their specific needs. This led to disparate security technologies that, unfortunately in many cases, did not interoperate. Also, applications were not designed with security in mind, and until the early 2000s, software developers were not taught about the variety of things that can make software vulnerable.

MITRE's goal is to ensure that everyone is speaking about the same things by making security measurable.

—Robert Martin, Senior Principal Engineer and Outreach Lead of MITRE Corporation

Furthermore, the security industry itself was hampered by the inability to communicate effectively about vulnerability reports, attacks, and weaknesses. It is this challenge that MITRE has focused on solving.

MITRE is in charge of the Common Vulnerabilities and Exposures (CVE®) programme and other related programmes, such as Common Weaknesses and Exposures (CWE™) and Common Attack Pattern Enumeration and Classification (CAPEC™). CVE is a dictionary for publicly known security vulnerabilities. It is not a database or product in itself but rather an enabler to allow companies, researchers, and organisations to communicate in a universal language about publicly known vulnerabilities. This is why CVE is so useful for databases by organisations such as US-CERT, CERT/CC, National Vulnerability Database (NVD), as well as in vendor advisories for both software vendors and security vendors.

Each reported vulnerability is assigned a unique identifier and a standardised description. The reporting source is a factor that determines how much effort is required to record the publicly known vulnerability's CVE description. A smaller, unknown organization might require more research on MITRE's part and even require that they interact with the researcher. Conversely, the larger software vendors require less work since over the years those groups have been "taught" what is and is not a CVE and their level of abstraction. Then, MITRE would provide a range of CVE identifiers to cover the number of unique vulnerabilities that the vendor might have.

However, CVE identifiers are less useful for vulnerabilities found in a company's custom application, such as an Amazon "shopping cart" application. Because it would only affect that one company, it does not make sense to publish a unique CVE identifier for this and add it to a database—only the affected company cares and once they fix it would be gone forever. Instead, the CWE program would be much more useful. CWEs focus on categorising the different types of weaknesses to help improve understanding of that class of weakness. Because a CWE entry refers to a class of weakness, each entry can reference multiple CVE entries. There are some 50,000 unique CVEs and only 800 CWEs.

CWE identifiers are useful in the process of vulnerability testing of an organization's own applications by tracking the types of vulnerabilities that are being found in their applications such as PHP or ASP. Many applications rely on Javascript or PHP. Therefore, if there is a potential vulnerability it could affect all of their applications written using these technologies.

"Between CVE, CWE, and CAPEC, it becomes possible to communicate in a common vocabulary and improve the effectiveness of the entire Web application security process."

Similarly, Web application vulnerabilities will be based on a type of vulnerabilities (weakness or multiple weaknesses). Even though there is not a database of the unique vulnerabilities in an organization's custom applications, these potential vulnerabilities can still be categorized into specific classes, each with their own causes and remediation processes. So organizations can use the CWE to understand the types of vulnerabilities, and craft a plan for remediation accordingly.

Furthermore, the CAPEC program is very interesting since it is similar to CWE but focuses on the types of attacks that are possible. Thus, CAPEC can be used by companies trying to test their Web applications or by white hat penetration testers that are trying to find a way into a customer's system. CAPEC also provides information about what attacks look like, whether in recon, surveillance, or collection phase. Thus, businesses and security professionals can use this to identify attacks. Frost & Sullivan analysts believe that security vendors will adopt this into their products to detect attacks in the near future.

Between CVE, CWE, and CAPEC, it becomes possible to communicate in a common vocabulary and improve the effectiveness of the entire Web application security process. CVEs can be used for general vulnerability assessment of Web applications based on ubiquitous software such as Apache, Linux, and others. CWE can be used to assess and understand potential vulnerabilities in custom applications. CAPEC can help with the attack detection/simulation phase.

MITRE operates CVE and CWE compatibility programmes, designed to assist organisations in their selection of tools, products and services. In order for security companies to achieve CVE and CWE compatible status, they must meet a complete set of stringent requirements. While the requirements for CAPEC compatibility are written, the program is just starting. In Frost & Sullivan's opinion, this is highly useful to organisations, because they will be able to trust that the CVE and/or CWE compatible security partner has been properly vetted. High-Tech Bridge, which has collaborated with Frost & Sullivan on this paper, is an example of a security company whose proprietary Security Research Lab is both CVE and CWE compatible.

OPTIMISING WEB APPLICATION SECURITY

In Frost & Sullivan's opinion, there is no absolute solution to the hacking threat. As we have seen in the previous chapters, hacking is highly dynamic, and new vulnerabilities are discovered as quickly as known vulnerabilities are patched. Moreover, website owners must strike the right balance between functionality, user-friendliness and security. Consequently, organisations cannot achieve 100 percent Web application security, but they should certainly strive to optimise security.

The Pillars of Secure Web Applications

As with any other network security challenge, accuracy, comprehensiveness and consistency are important objectives for Web application security. Frost & Sullivan recommends that organisations base their approach to Web application security on three pillars:

Life Cycle	Maintenance	Testing
Integrating security into the application development life cycle; secure Web applications developed by experienced professionals, focussed not only on productivity and speed, but also on security	Proper updating mechanisms for Web applications, taking into account vulnerabilities that were discovered after the application was written; Web servers, where the applications are hosted, also require updating	Regular security audits and penetration tests, conducted by an independent third-party company, with experience and detailed knowledge of Web security

Ideally, organisations take a proactive approach to Web application security based on life cycle, maintenance and testing in order to patch vulnerabilities before hackers exploit them. Unfortunately, organisations must also have the capacity to be highly reactive. Organisations may not realise they have been hacked until complaints start coming in via the media, from customers or partners, or even from law enforcement and intelligence agencies. Law enforcement typically becomes involved if an organisation's compromised systems are used to perform attacks on others.

We said in the beginning of this paper that security was an ongoing commitment. The same philosophy should apply to an organisation's relationship with security companies. Frost & Sullivan recommends that organisations form real partnerships with security companies rather than consider each security activity as a one-off event. Let us discuss the three pillars of security in reverse order.

Testing

There are two testing options available for businesses seeking to secure their Web applications—"white box" and "black box" testing. In the black box testing method, the tester has no prior knowledge of the mechanics of the application. The tester will then try to scan or break the application to find vulnerable code, just as a hacker would. Thus, black box testing best simulates a true hacker scenario.

Conversely, a white box test allows the hacker to have full knowledge and control over the application, including the source code. This method can help the tester find all the vulnerabilities in the Web application. However, this method is less applicable to a real-world attack scenario, except for in the case of a malicious "insider" threat.

Each testing method has their advantages and disadvantages, but ideally the combination of both methods will be the most useful in most cases. While a true black box scenario provides the most relevant real-world results, the tester will be able to conduct the test more efficiently and thoroughly if they have the source code at their disposal. This methodology is known as "grey box" testing, as it provides the tester with enough information to find vulnerabilities in an efficient and relevant way.

Frost & Sullivan recommends that a combination of both approaches be employed because relying solely on one or the other could leave an organisation vulnerable to some attack vectors. In addition, applications developed in-house, the standard practice for the vast majority of websites, require a custom security approach.

Maintenance

The importance of keeping platforms and servers up to date should be a given, requiring no further explanation.

A penetration test will only uncover vulnerabilities that were present during the time the test was performed. No one knows what developments might unfold afterward, e.g., if there is a delay between vulnerability discovery and vulnerability patching.

Fixing Web application vulnerabilities will typically involve code remediation. Custom code updates of this type require a code push that could introduce a new vulnerability.

Life Cycle

The best, most cost-effective way of ensuring Web application security is to integrate a security philosophy into the application development life cycle. In a previous chapter, we saw that Web developers will not worry about security unless specifically asked to do so. Moreover, many Web developers quite often overestimate their skills and knowledge in Web application security, fixing only obvious and easy-to-exploit vulnerabilities and missing advanced ones. In-house development is characterised by the same phenomenon. Unless an organisation's culture emphasises security, quality and thoroughness (some¬times at the expense of speed and cost leadership), the Web applications developed will probably be sub-optimal. Organizations must implement thorough quality assurance testing to ensure that the applications perform only the intended functions.

The more complex a system is, the more likely a vulnerability will remain hidden. By examining the code before deployment, risk can be assessed, decisions made and measures taken. By conducting proper input validation, the quality of both an organisation's security and code can be dramatically improved, and that alone should avoid most Web attacks.

Cost or Investment?

In continental Europe, an average manual Web application penetration test in an average organisation with complete reports, providing the organisation with detected vulnerabilities and solutions, can easily cost about $30,000.

For a decent Web penetration test, $30,000 is a fair price, but forking out such an amount for an activity that has no revenue attached to it can seem extravagant, especially to SMEs. Frost & Sullivan is convinced that the seemingly high price is a huge issue, prompting many companies to rely on cheap, incomplete solutions or to ignore Web application security altogether.

Businesses may also rely on penetration testing services offered by vendor partners. However, these services have little value if performed by under-qualified or biased third-parties. For example, many security companies sell sub-par automated vulnerability scanning as "expert ethical hacking" and "manual penetration testing," using "fair price" as their main sales argument. Whereas they may not leave customers out of pocket, they certainly leave them vulnerable, as not all vulnerabilities are detected during automated vulnerability scans. Organisations appreciate the difference between a manual penetration test performed by a certified auditor and an automated vulnerability scanning managed by an IT support engineer, but they get what they pay for.

Because few security companies perform this work correctly, the reputation of the entire security industry is called into question with organisations considering penetration testing "useless" because their websites were hacked anyway.

As a result, organizations may consider ethical hacking to be a high-risk investment. However, businesses can reduce this risk by ensuring that penetration tests are performed by third-parties who do not have conflicting interests and who have specialized and up-to-date knowledge in the area of Web application hacking techniques, references, proof-of-background checks, certifications and years of experience. Considering the high cost of a security breach or data loss (in monetary terms as well as brand reputation), Web application security is an important investment.

Security is an ongoing commitment and an indispensable process; therefore, businesses must seek out reputable, specialized, and experienced Web application testing companies to partner with. This is an important decision and businesses should require references, documentation, and demonstration of skills.

Please reference the white paper titled "The Importance of Ethical Hacking – Emerging Threats Emphasise the Need for Holistic Assessments," which details numerous best practices for selecting Web application testing partners.

"[...] businesses must seek out reputable, specialized, and experienced Web application testing companies to partner with."

THE FROST & SULLIVAN LAST WORD

Organisations worldwide completely underestimate the threat to their websites, and they also fail to realise that the consequences of a compromised Web application can go way beyond the Web server.

This threat is just as real to small companies as it is to large organisations. We have discussed that SMEs are much less prepared, which leaves them in a tight spot. With hacking on the rise, from organised criminal groups, amateurs and political activists, the threat is not going away.

If anything, the threat will get worse. As we have seen, Web-centric business models have dominated economic growth and job creation in recent years, and this boom in the importance of Web applications acts as a stimulant to hackers, meaning that Web application security will continue to increase in importance. Because Web applications constantly change and new hacking techniques are discovered, businesses cannot expect to achieve 100 percent secure Web applications.

However, businesses should aim to secure the most high-risk, obvious and exploitable attack vectors. Hackers must weigh the value of the target against the cost of the work to achieve their goal. Therefore, businesses should achieve a moderate and reasonable level of Web application security through careful and security-aware software development, ongoing penetration testing, maintenance and monitoring. These practices will help deter targeted attacks, untargeted attacks, malware and hackers. In turn, these practices will prevent costly security breaches.

Security is an ongoing commitment requiring time, dedication, investment and the right attitude from all employees. Developing a security-conscious culture is a step in the right direction, as is the adoption of security standards such as CVE and CWE. To complete the journey, Frost & Sullivan recommends that organisations form real, long-term partnerships with stable, reputable security companies capable of providing the individual solutions that will optimise Web application security.

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Colombo
Dubai
Frankfurt
Hong Kong
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Manhattan
Mexico City
Mumbai
Moscow
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw
Washington, DC