SmarTone

Enterprise-Class Information Security for Small and Medium Business

White Paper

Cybercrime is a modern global crime in the era of digital information. Professional hackers attack any business organizations with IT infrastructures or computing devices connected to internet. Even small businesses need enterprise-class information security framework to protect organization's digitalized assets.

SmarTone Mobile Communications Limited
31/F, Millennium City 2,
378, Kwun Tong Road, Kwun Tong. Kowloon, Hong Kong
T: 852 3128 2828 | F: 852 2168 3120

What is Cybercrime?

Cybercrime is criminal activity done using computers (including any connected device) and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as consuming your computing resources for other attack or posting confidential business information on the Internet.

The principle of cybercriminal is similar to those of traditional crime we have been fully aware. The difference is just in the matter of techniques – virtual world over Internet protocols and physical world over physical interaction. The techniques of traditional crimes compared with cybercrime are tabulated as below.

Traditional Crimes	Cybercrimes
Burglary Breaking into a building with the intent to steal.	**Hacking** Computer or network intrusion providing unauthorized access.
Deceptive Callers Criminals who telephone their victims and ask for their financial and/or personal identity information.	**Phishing** A high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.
Extortion Illegal use of force or one's professional positions or powers to obtain property, funds or patronage.	**Internet Extortion** Hacking into and controlling various industry databases (or the threat of), promising to release control back to the company if funds are received or some other demand satisfied.
Fraud Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain an unfair or a dishonest advantage.	**Internet Fraud** A broad category of fraud schemes that use one or more components of the Internet to defraud prospective victims, conduct fraudulent transactions, or transmit fraudulent transactions to financial institutions or other parties.
Identity Theft Impersonating or presenting oneself as another to gain access, information, or a dishonest advantage.	**Identity Theft** The wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception, typically for economic gain.

Black Markets for Cybercrime Tools and Stolen Data

Cybercrime is a growth industry which alerts every organization over the world. The growth is increasingly facilitated by burgeoning black markets in both the tools (e.g. exploit kits and bots) and the take (e.g. credit card information). A report published in 2014, by a non-profit global policy think tank to US armed forces – RAND Corporation, predicts that there will be more hacking for hire, Cybercrime-as-a-Service offering, and brokers.

Cybercrime Tools Market Price

Cybercrime tools pricing model can be one-off or pay-as-you-go and the price varies from a few hundred to ten thousand US dollars subject to the complexity and usefulness of the tool.

Exploit Kit	Price	Year
Mpack	$1,000	2006
WebAttacker (Do-it-youself kit)	$15-20	2006
IcePack	$30-400	2007
Mpack	$700	2007
Eleonore (v1.2)	$700 plus $50 for encrypter	2009
Eleonore (v1.2)	$1,500 fully managed by user	2009
Eleonore (v1.3.2)	$1,200	2010
Eleonore (v1.6 and v1.6.2)	$2,000	2010
Eleonore (v1.6.3a)	$2,000	2011
Eleonore (v1.6.4)	$2,000	2011
Eleonore (v1.6.2)	$2,500 - $3,000	2012
Phoenix (v2.3.12)	$2,200 /domain	2012
Exploit kits that employ botnets	up to $10,000	2012
Blackhole - hosting (+ crypter + payload + sourcecode)	$200/week or $500 /month	2013
Whitehole	$200-$1,800 rent	2013
Cool (+ crypter + payload)	$10,000/month	2013

(Sources: Clarke, 2013a; Fossi et al., 2011; Fortinet, 2012; Goncharov, 2012; Kafeine, 2013a; Krebs, 2013a; M86 Security Labs, 2010; Martinez, 2007; McAfee Labs, 2011; O'Harrow, 2012; Paget, 2010b, 2012; Parkour, 2014.)

Cybercrime Service Price

Distributed Denial of Service (DDoS) is a common attack to disrupt organization's business operation. The service offering is rated for the period of attack.

Offering	Price
1-hour DDoS service	US$ 10
1-day DDoS service	US$ 30 - 70
1-week DDoS service	US$ 150
1-month DDoS service	US$ 1,200

(Source: TrendMicro)

Stolen Credit Card Information Price

The price of the stolen credit card varies with different factors such as geographical region, card type, account balance, etc.

Dumps	Estimate of Price (without PIN, with PIN, PIN and good balance)			
	US	EU	CA, AU	Asia
Visa Classic	$15 $80	$40 $150	$25 $150	$50 $150
Master Card Standard	$90	$140	$150	$140
Visa Gold/ Premier	$25 $100 $200	$45 $160 $250	$30 $160	$55 $150
Visa Platinum	$30 $110	$50 $170	$35 $170	$60 $170
Business / Corporate	$40 $130	$60 $170	$45 $175	$70 $170
Purchasing / Signature	$50 $120	$70	$55	$80
Infinite		$130 $190	$60 $200	$190
Master Card World	$140			
AMEX	$40	$60	$45	$70
AMEX Gold	$70	$90	$75	$100
AMEX Platium	$50			

(Source: McAfee)

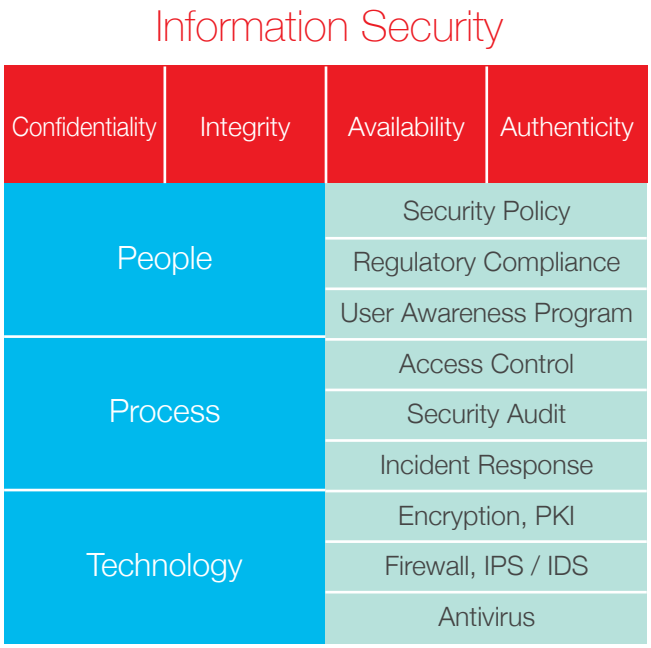
Information Security Framework to Protect your Organization from Cybercrime

Similar to traditional crime protection, the solution involves people, process and technology. When you and your family have a leisure trip in summer vacation, you probably do, at least, the following steps:-

- Save any valuable items including jewelry in a safe box in a bank close to your apartment
- Inform your estate guards for their attention during your trip
- Turn on the light in living room to pretend someone in the apartment
- Lock all the windows as well as your main door

For some have higher awareness or more valuable asset in apartment, they will adopt high-end electronic lock to increase the difficulty to burglary. In addition, some employ burglary detection system to alert police or any security organization for further protection. It is a matter of compromising among the risk of loss and degree of protection scheme.

The cybercrime protection is realized by an information security management framework which involves people, process and technology. The protection is forever-lasting and continuously changing; therefore, you need to assign personnel (at least one person) as a committee or dedicated group to continuously implement and monitor the security protection for your company. In order to assure the business processes and your IT system with the minimal surface exposed to the risk, the security policies, best practices as well as security devices are required to be in place and fully integrated into your business.



People, Technology and Process

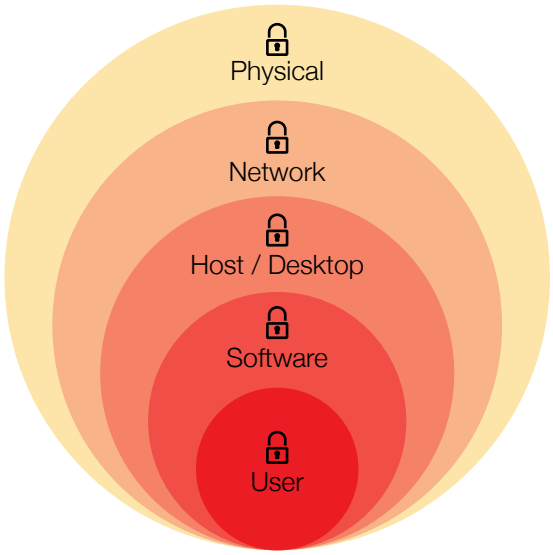
People or the employees of the SMBs are the greatest asset or element of the security system. It comprises of people and various roles and responsibilities within the organization. In another words, the roles and responsibilities of the people are to execute and support the process. Some examples of the key roles of the people are senior management, security administrators, system and IT administrators, end users and auditors.

A good security culture is developed in the following three ways:

- Identity and access management-The roles for different users within the SMEs environment (from administrative to the CEO) are defined and the physical and logical access privileges for all employees are specified. Once these roles are defined, appropriate access are given to the employees.
- Information security organization- All the employees shall be responsible for security.
- Training and awareness-An ongoing effort to raise awareness of the benefits of working in a secured environment. The process includes executive, management, administrator and end-users.

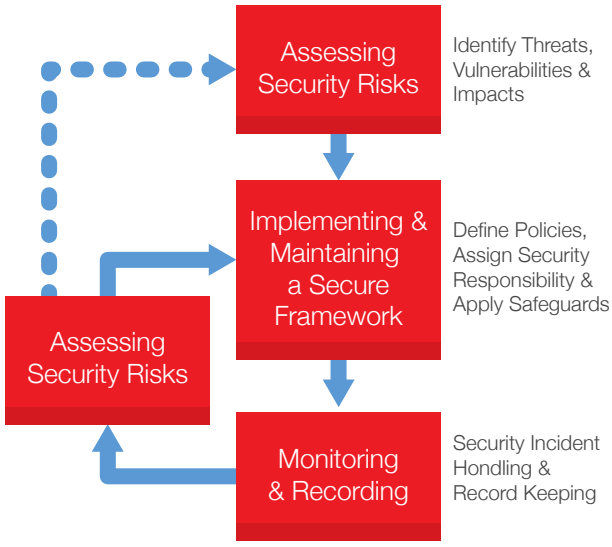
Technology includes tools, methods and mechanism to support the security process so as to mitigate the risk and thereby reduce security threat. The layered security model is commonly adopted in the information security framework which sets up defense layer-by-layer from perimeter towards to the host/device, software and data with different security technologies such as firewall, intrusion detection/prevention system, anti-virus, anti-spam, data loss prevention, end-point encryption as well as identity access management, etc. Besides the security devices, you need a team of skilled people around-the-clock to look after your IT infrastructure for preventing, reducing, and remediating security events.

Layered Security Model / Defense-in-depth



Process is the glue that binds the people and technology. It is described as a cycle of iterative processes that require ongoing monitoring and control. Assessing security risk is the initial step to evaluate and identify risks and consequences associated with vulnerabilities, and to provide a basis for management to establish a cost-effective security program.

Based on the assessment results, appropriate security protection and safeguards should be implemented to maintain a secure protection framework. This includes developing security policies and guidelines, assigning security responsibilities and implementing technical security protections. The essential protections for all level organizations will be further described later in this paper.



(Source: HKSAR OGCIO G51)

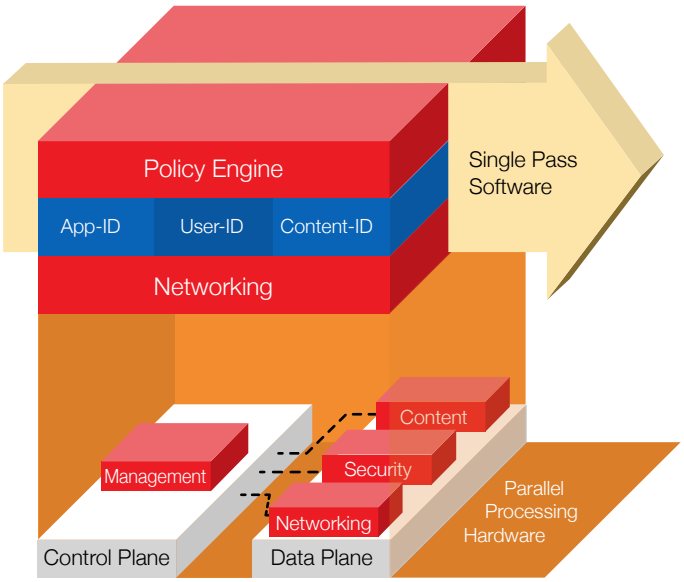
Then, it is followed by a cyclic compliance reviews and re-assessment to provide assurance that security controls are properly put into place to meet your organization's need. This model relies on continuous feedback and monitoring.

Managed Next Generation Firewall Services

Network security control is the first protection layer to prevent intrusion attacks from Internet to your network, to block malicious software from entering into your network via email message or internet browsing from your staff in the network, to stop the exfiltration of your company and personal sensitive data such as credit card information, to filter out spamming and phishing emails, to prevent from advanced attacks such as zero-day exploits and unknown threats, and to provide a virtual patching to your server vulnerable before the official patch from your vendor is implemented in the server. In addition, the network security shall be applied not only to the traffic between Internet and your networks but also the traffic among different network segments so as to reduce the network context from virus infection spreading or bots activities such as access expansion for vulnerable and credentials, which is caused by one compromised machine.

With the rapid development of Internet and mobile computing technology, web 2.0 technologies have been fully integrated into every corner of your digital life including business processes, mobile workforce, social networking, on-line transaction, point-of-sales automation & interaction and so on. The complexity of threat identification from legitimate traffic traversing your network has been exponentially increased.

In the past ten-years, the advanced development in semi-conductor and network security software technologies such as deep-packet inspection, signature-matching, behavioral analysis, etc., Next Generation Firewalls become essential security devices to protect your network from a wide range of sophisticated and dynamic attacks in the web2.0 and enterprise2.0 era. Next Generation Firewalls are equipped with the capability to identify the applications, users and content; as well as to perform the protection functions under a holistic view of network security policy. The security functions include Intrusion Prevention System (IPS), Anti-malware (AV), Data Loss Protection (DLP), Advanced Threat Protection (APT) together with security visibility. The Next Generation Firewalls are designed in software and hardware architecture to perform multiple security protection functions with performance, scalability, extensibility for new threat protection, and visibility awareness. In addition, the Network Firewall often supports VPN access for remote user accessing securely to enterprise network.



(Source: Palo Alto Networks)

Visibility	• Application monitoring • User identity Tracking • Deep packet inspection over encrypted session
Intrustion Prevention	• Application blocking • URL filtering • Vulnerable-based protection • Network behavior analysis
Anti-malware	• Anti-Virus • Anti-worm • Anti-spyware
Advanced Threat Protection	• Threat Emulation Analysis • Anti-bot
Data Loss Protection	• PCI-DSS protection • File type blocking • Keyword filtering

Application Specialized Firewall

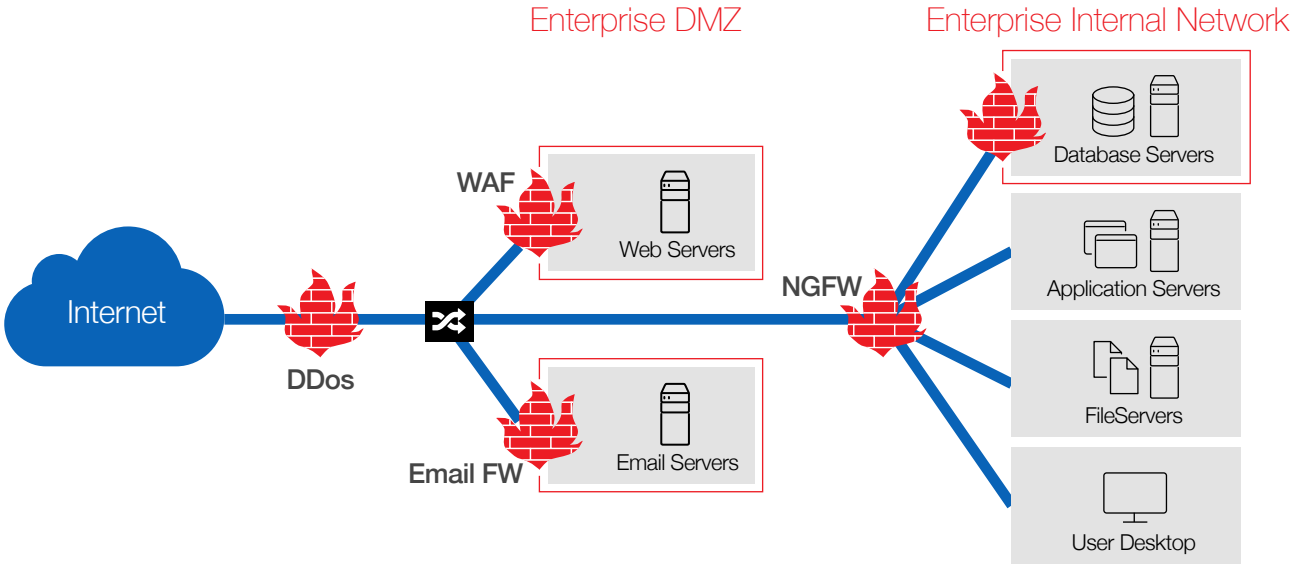
Next Generation Firewalls are a combination of network layer firewalls and application layer firewalls. Application firewalls, in contrast with network firewalls, are not concerned with all traffic. They rather include an application proxy or gateway for the application needed to be inspected and protected. For example, due to the web2.0 technologies as well as the dynamic and rapid development of web portal, web application becomes more vulnerable than others. Hence, Web Application Firewall ("WAF") is specifically designed to protect web application from many types of attacks specific to web application such as SQL injection, broken authentication and session management, cross-site scripting, insecure direct object references, and so on, which are the top-ten threats specified by the Open Web Application Security Project ("OWASP").

OWASP
The Open Web Application Security Project

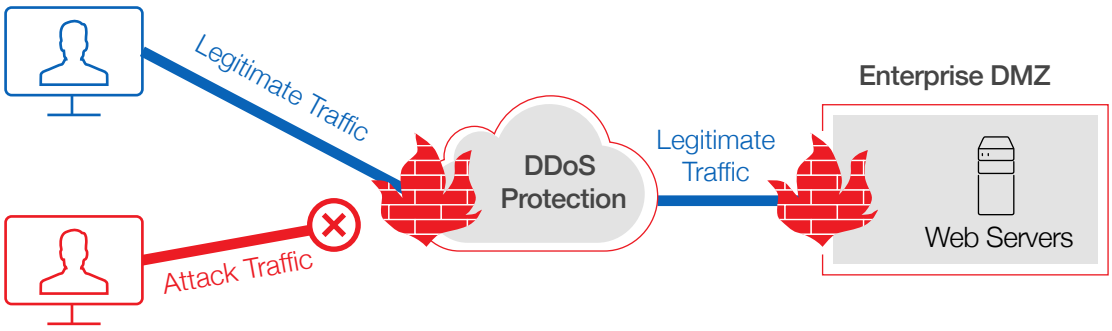
A1	A2	A3	A4
Injection	Broken Authentication and Session Management	Cross-Site Scripting (X55)	Insecure Direct Object References
A5	**A6**	**A7**	**A8**
Security Misconfiguration	Sensitive Data Exposure	Missing Function Level Access Control	Cross Site Request Forgery (CSRF)
	A9	**A10**	
	Using Known Vulnerable Components	Unvalidated Redirects and Forwards	

Network Security Deployment Reference

Network security solution topology is highly depended upon your network topology as well as your business need and budget. However, we recommend you the two-tier network security topology on the right which is a general deployment reference commonly adopted as starting point for fine-tuning enterprise network security control. The enterprise network commonly has DMZ zone for web portal as well as email services which allows inbound traffic from Internet and isolates from the internal network. The internal network may have multiple segments for user desktops, business application servers, database servers as well as file servers. The application specific firewalls are located in the first-tier to protect the applications such as email and web services in DMZ zone; the network firewall is located in the second tier to protect the internal network segments. This firewall can be also used as a VPN gateway for remote users.



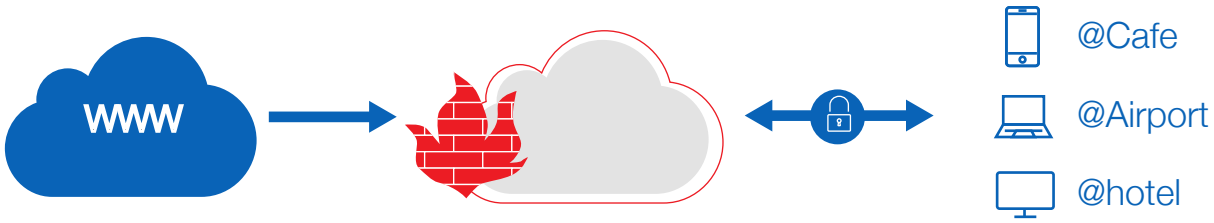
Cloud-Based DDoS Attack Protection and Mitigation



The Distributed Denial-of-Service ("DDoS") attack is common in the latest threat landscape. The attack can be classified as low-&-slow and volumetric-&-fast. The slow attack is to consume your application and server resources up so as to disable your application. This attack can be easily protected by both Web Application Firewall and Next Generation Network Firewall. On the other hand, the fast attack is to consume your Internet bandwidth up so as to disable legitimate traffic to your application. The on-premises Firewalls are no longer helpful to mitigate this type of attack.

Cloud-based solution is available to provide comprehensive DDoS mitigation so as to allow the legitimate traffic to your web applications but divert all the attack traffic to "sweetpots" before entering your Internet access connection. The protection ranges from network layer, DNS layer to application layer.

Security Control for Mobile Workforce

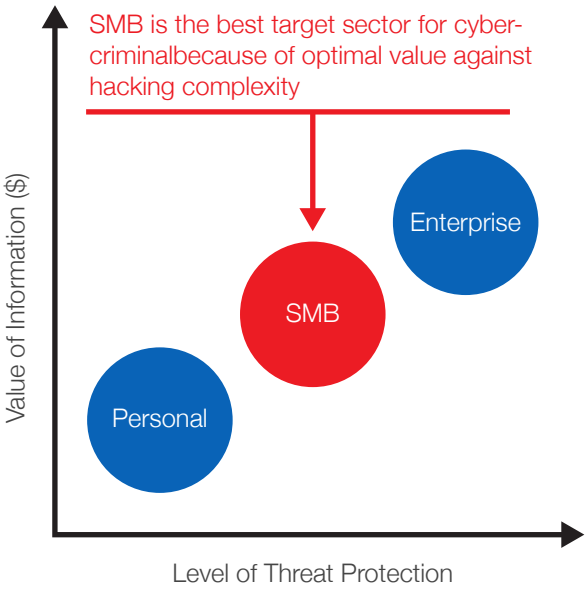


The success of iPhone launched in year 2007 with the advancement of mobile and wireless technology opens up the mobile computing era which greatly transforms people lifestyle from infotainment, productivity, social and commercial behaviors. Mobile computing has been further leaped up by widely deployment of cloud computing. Therefore, enterprises need to have the security control on mobile devices outside of the enterprise security perimeter.

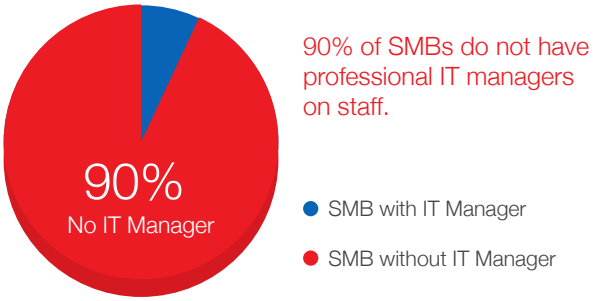
The mobile users can be protected from threats while accessing to Internet outside office under the security polices same as those for enterprise network. VPN connection to enterprise network firewall is one of the choices for mobile users but this way will consume enterprise network bandwidth as well as introduce unnecessary latency if roaming overseas. Cloud-based firewall is the latest solution for mobile users to access Internet securely without passing through enterprise network.

Does Cybercrime Bother Me, a SMB ?

Information security is as important for a small company as it is for a large corporation. Cybercrime is increasing at epidemic proportions, from consumers, to SMB (small and medium business) organizations to large enterprises. And it turns out SMBs are becoming the cybercriminal's "sweet spot". There is sufficiently valuable information to make it worth an attacker's time and the organization's protection level is typically weaker than that of a larger enterprise. The valuable information may be your personal information or company sensitive data.



Some SMBs believe that they are too small to be a target or they do not have valuable information assets to be stolen. However, sophisticated hackers consume your computing and network resources to attack the third-party target. With this indirect attack, you may have a risk in business disruption or become an accomplice in the serious attack to the target.



(Source : National Cybersecurity Alliance, National Small Business Study in 2012)

In United States, the National Cyber-security Alliance found that 90% of SMB did not have professional IT managers on staff, much less cyber security specialists. Verizon Data Breach Investigation Report in 2012 showed that 72% of SMBs reported a data breach in the year.

SMBs do definitely need to implement their own information security framework as soon as possible so as to protect the organization asset and assure your continuous business operation. Our security solution suite is designed to supplement the SMBs' limited budget in IT equipment investment and inadequate IT security expertise for having enterprise-class security protection with continuous support by professional security experts.

SmarTone Managed Next Generation Firewall Services

On top of our fibre-to-premise broadband service, SmarTone provides you an one-stop-shop solution on information security protection for your organization. The solution offer can be in subscription model as the InformationSecurity-as-a-service ("ISaaS") to ease your CAPEX budget burden with the enterprise-class information security protection. Furthermore, our professional team shall continuously provide you advices in security protection to cater your business growth and dynamic global threat landscape.

Our security solution suite for SMB includes:-

- ✓ General practical guidelines to Information Security ideal for guiding you to set up your own security processes;
- ✓ Risk assessment service on your organization to give you a holistic view on your infrastructure vulner ability as well as recommend and help you to set-up security framework best fit to your business;
- ✓ On-premise next generation firewall equipment to protect your data network from intrusion, virus-infection, and advanced attacks;
- ✓ On-premise VPN gateway to enable your staff to securely access to your network remotely;
- ✓ Cloud-based security gateway for your email server to filter out messages with malicious software and phishing messages, to block spamming email, to protect business sensitive & credit card data loss through email, and to quarantine suspicious message temporarily for zero-day virus and auto matically release once the virus signature available;
- ✓ Cloud-based web application firewall with DDoS mitigation service to protect your on-line business from disruption;
- ✓ Cloud-based two-factor authentication facilities to strengthen your system access protection;
- ✓ Managed service in security policy management on firewall and authentication token provisioning to enable your IT resources dedicated to your business-related IT needs;
- ✓ 7 x 24 technical support services to continuously improve your security policies, to reduce organiza tion risk, to analyze security datasets to detect and initiation action for any malicious activity, to regu larly check your security devices, networks and applications for vulnerabilities as well as to identify and respond to security incidents in real-time.

The SmarTone Difference

At SmarTone, we believe in making each day better than the last by challenging the status quo and doing things differently. We strive to be more valuable to our customers and this commitment is reflected in our powerful network, purposeful apps that add real value to people's lives and passionate service.

For further information, please contact your Account Manager
2281 8818
bm_cs@smartone.com

SmarTone Mobile Communications Limited
31/F, Millennium City 2,
378, Kwun Tong Road, Kwun Tong. Kowloon, Hong Kong
T: 852 3128 2828 | F: 852 2168 3120

End of Document