'e Scan

Anti-Virus

8 Painpoints of CIOs and How eScan Handles it

8 Painpoints of CIOs

01. What are the areas of concern with regard to information security?

Ans. Before we answer the above question – let's ask ourselves – What do we mean by Information Security?

Protection of Information and Information Systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction is basically what defines the term Information Security. Moreover, the term greatly surrounds the goal of protecting the confidentiality, integrity and availability of information – be it electronic, print or any other form it translates into.

The right to secure ones information has always been one of MicroWorld's top priorities. Be it with end users, institutions – educational or financial, governments, military, hospitals or private businesses – as a breach could amount to anything from loss of personal data to loss of business. Therefore, securing information is not only a business requirement but also a personal requirement – reason why our SMB, Corporate and ISS implement endpoint security.

Threat Scenario – Past & Present

Threats were noisy & visible to everyone

Threats are silent & unnoticed with variants

Threats were indiscriminate, hit everyone

Threats are highly targeted, regionalized

Threats were disruptive → impact visible

Threats steal data & damage brands → impact unclear

02. What security measure should be implemented to prevent information breach and information theft?

It goes without saying that there has been a sharp increase in cybercrime in the last year. With hackers taking advantage of various vulnerabilities within Windows OS's and third party applications, it goes to show the extent to which malware can be created. While the use of the Stuxnet malware is old news – there have been bigger instances where corporates' have lost more than they could swallow. Take for example the breach of Sony Corporation – over 1 million user passwords were stolen via SQL Injection. To top it off, the passwords were stored in plaintext without any sort of encryption. Other instances include – hack on HBGary, Google, Sony and a handful more noteworthy companies. It goes without saying – in today's day and age, data theft and industrial espionage is of all importance.

Another great insight would be a recent phishing exercise carried out by KnowBe4 among Small and Medium Enterprises. The tests were basically carried out on 3,400 companies where emails were delivered to 29,000 recipients at 3,037 business units; individuals who clicked the link were directed to a landing page which then informed them about the simulated phishing attack.

"Any business that provides access to email or access to its networks via the Internet is only as safe from cybercrime to the degree that its employees are trained to avoid phishing emails and other cyberheist schemes. The more employees within an organization that use email or go online, the greater the risk of exposure to cybercrime" - Stu Sjouwerman (KnowBe4 Founder and CEO).

According to the research carried out, the most Phish-prone industries are:

Travel	– 25%
Education	– 22.92%
Financial Services	– 22.69%
Government Services	– 21.23%
IT Services	– 20.44%

So how does eScan fit into such a scenario?

Both eScan SMB and Corporate versions come with a Web Based Management Console that make it easy for network administrators to monitor and deploy all necessary security measures. It can be in the form of remotely upgrading the client product, enabling or disabling particular modules or it could simply be enforcing security policies across the network. With that said, the main aspect that business units should look into are the access rights maintained across networks. Enforce blocking of USB ports as they are the first target

Endpoints & Endpoint Security

Key Influencers

- Devices and Storage Mediums
- Portability of Data
- Accessibility
- Compliance Laws & Regulations (HIPAA, SOX, etc.)
- Extranet/Intranet Access provided to employees & partners.
- Network Downtime due to infections

points which can be used to spread viruses knowingly/unknowingly.

USB devices are widely used in business and SOHO environments mainly for three reasons:

- Are easy to use
- Have quite a large storage capacity
- Provides fast data transfer

However, this is just the good aspect of it.

The problems faced with USB based devices are –

- Malware and spyware application can be stored and run from USB devices
- The USB drive can be used to store a few hundred documents – which can contain confidential information (intellectual property)
- USB storage devices are small and can get lost easily which in turn translates to data loss
- Most of the USB storage devices provide almost no protection. Thus, it can be said that such devices are not suitable for storing important data.

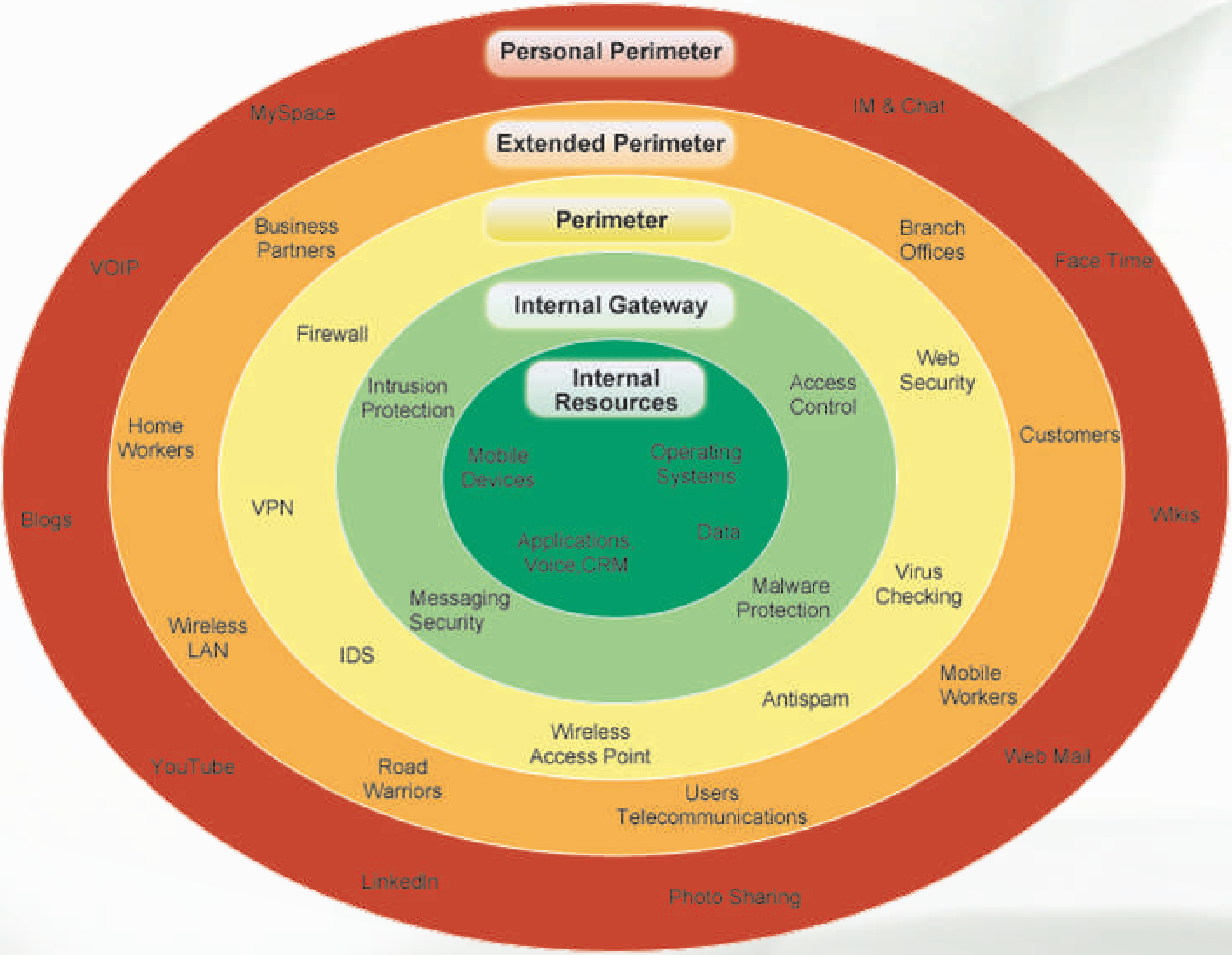
To prevent information from transgressing beyond the premises and policies of a business, the following aspects will need to be considered:

- Monitor all communications going outside of the organization
- Secure all email containing confidential content
- Protect intellectual property
- Prevent malware-related data harvesting
- Enforce strategic user policies
- Block all known Endpoints and communication ports
- Block malicious users along with the possibility of being caught

Endpoints & Endpoint Security

- Loss/leak of confidential information
  - Losing valuable employees
  - Unknown/invisible threats and loss of productivity due to using non-complaint storage mediums
  - Unauthorized intrusions – via Web Servers, email Servers, etc.
  - Access to internal networks via individual end points

8 Painpoints of CIOs



Risks

- 🟥 Very High
- 🟧 High
- 🟨 Medium
- 🟩 Low
- 🟩 Very Low

03. What steps need to be taken into account when a breach is detected?

There are four key steps to consider when responding to a breach or suspected breach:
Step 1: Contain the breach and do a preliminary assessment
Step 2: Evaluate the risks associated with the breach
Step 3: Consider notification
Step 4: Prevent future breaches

Tips:

- Be sure to take each situation seriously and move immediately to contain and assess the suspected breach.
- Breaches that may initially seem immaterial may be significant when their full implications are assessed.
- Agencies and organisations should undertake steps 1, 2 and 3 either simultaneously or in quick succession. In some cases it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs.
- The decision on how to respond should be made on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, organisations may choose to take additional steps that are specific to the nature of the breach.

Endpoints & Endpoint Security

Key Data to be Protected

Data in Motion

- Emails
- Instant Messaging
- P2P
- File Transfers
- Web Posts
- Blogs

Data at Rest

- Laptops/Desktops/File Servers
- USB

04. What is the level of security that needs to be maintained as far as employees are concerned?

If you look at large Enterprises and MNCs of today, you get to see that a great deal of attention is given in protecting the companies electronic assets (mostly from) outside threats. From intrusion prevention systems to firewalls to vulnerability management – while the mentioned few are what most companies implement or follow – the problem of data loss mostly lies from the inside. Be it in the form of email, instant messaging, webmail, website surfing or even file transfers, electronic communications exiting the company apparently go largly uncontrolled and unmonitored – with the potential of confidential data falling into the wrong hands. However, should there be a breach in information, it could create havoc within the organization through fines, bad publicity, loss of strategic customers, loss of competitive intelligence and legal action. Thereby, looking into todays scenerio and competitive environment, data loss is one of the most critical issues that are being faced by CIOs, CSOs, and CISOs.

Three basic aspects need to be borne in mind as far as data loss is concerned:
1. Data in Motion: Any data that is moving through the network to the outside via the Internet
2. Data at Rest: Data that resides in files systems, databases and other storage methods
3. Data at the Endpoint: Data at the endpoints of the network (e.g. data on USB devices, external drives, MP3 players, laptops, and other mobile devices)

With the rise in competition, protection of intellectual property is a major concern for most organizations. From industrial espionage to employees carrying sensitive data, protecting key assets of the business is key to preventing data loss. Company assets or their so called trade secrets could include anything from patterns to codes to even diagrams and flow charts. With such a wide array of aspects to consider employees might not even know they are handling intellectual property.

To tackle such situations and patrol various aspects for data loss, companies need to monitor and control all outgoing communications that leave the company. This would include:

- Monitoring communications going outside of the organization
- Securing email containing confidential content
- Enabling compliance with global privacy and data security mandates
- Securing outsourcing and partner communications

Layers of Endpoint Security

Network Access Control /
Network Access Protection

Control Access
- to critical resources
- to entire network

Based on
- User identity and role
- Endpoint identity and health
- Other factors

With
- Remediation
- Managements

- Protecting intellectual property
- Preventing malware-related data harvesting
- Enforcing acceptable user policies
- Blocking of all known Endpoints and communication ports
- Blocking of malicious users along with the possibility of being caught

Endpoints & Endpoint Security

Reducing Threat Exposure

Information Protection & Control

- Data in Motion
- Data in Rest

Asset Protection & Control

- Asset management
- Desktop computing support
- Application Control
- Security Incident Alerts/logs
- NAC/NAP

05. What kind of access rights should be employed to employees within the organization?

Before even getting into employee rights companies need to develop a thorough understanding and should break down the various types of sensitive data that exist within the organization. This would give a better view of the policies required to control and strategically enforce the kind of data that is needed to be shared.

Having said that, it is critical for companies to understand the kind of security policies that need to be deployed not only organization wide but to break them down individually as per users, departments and remote offices are also of importance. While the need to determine relevant areas that need to be protected, organizations also need to look into the impact data loss has on workflow. This ensures that the solution implemented is by far dynamic and flexible enough to meet the ever changing workflow and processes.

To be able to enforce strict policies, organizations need to identify potential vectors for data loss within the organization. This would include data in motion, data at rest, and data at the endpoint. Aspects such as past breaches, volume of data, likelihood of a breach and total number of users with access to the mentioned vectors will need to be taken into account. With all aspects taken into account focusing on areas that represent higher potential for loss makes it easier to find a solution to the problem at hand.

To be effective and to be able to detect policy violations a Data Loss solution must include:

Multi-protocol monitoring and prevention

Analysis of all major file and attachment types

Selective blocking and/or quarantining of messages

Automatic enforcement of strategic policies

While taking the above into account, administrators also need to ensure that each policy may or may not be the same for people across the network. Different people will have different roles and set responsibilities – therefore it is imperative that the deployed security policy recognises this and then and only then enforce the most appropriate policy across the network.

06. What steps need to be considered to ensure employee productivity?

With the steady rise in electronic communications, data in motion (data that travels through and out of the network) is one of the most important aspect that needs addressing. Take for example, an employee sends across documents to his/her personal email address allowing him/her to work from home or for instance a hospital employee accidently sends across patient information to the wrong person. Having said that, outbound email is not the only aspect that needs to be addressed – there are many gateways through which confidential information and company secrets can leave an organization using the Internet:

- Email
- Webmail
- HTTP (message boards, blogs and other websites)
- Instant Messaging / Social Networking
- Peer-to-peer sites and sessions
- FTP

Layers of Endpoint Security

- Network Access Control / Network Access
- Device Control
- Intrusion Prevention
- Firewall
- Anti-Spam / Anti-Phising
- Web Protection
- Anti-Virus / Anti-Spyware

Ordinary firewall and network security solutions are not capable enough to secure data in motion. Moreover, companies have made attempts to address issues regarding data loss via corporate policies and various employee education programs, but without the appropriate controls, employee's can (through ignorance or malicious intent) still leak confidential company information.

To put a lock on data loss and to enhance employee productivity, the following solution with the following capabilities will need to be addressed:

- Block (or alert about) illicit browsing activity
- Prohibit usage of P2P and various other file sharing programs
- Prevent use of gambling and social media websites
- Enforce messaging policy (attachment size, no personal email, etc.)
- Block usage of endpoints
- Add legal disclaimers to outgoing emails

07. What is the process that needs to be followed for evaluating security solutions?

While all the above stated requirements are a must have – deployment, management and reporting are key aspects any company should look for. In other words, the product should be fast and simple to implement within the organizations infrastructure. The product should be easy to maintain and manage thereby cutting down on time spent in understanding the various product related aspects. Moreover, the ability to provide detailed reports of all suspected violations is of utmost importance – without it the product would fail. Administrators and chief officers should have the ability to receive reports about detected violations, with in-depth information that enables them to take the required action. These details include but not limited to: the message sender, contents, attachments, intended recipients and information about the violating content.

08. Application and OS vulnerabilities are probably the most sort after weaknesses by malware writers. Taking this into focus, how does a security solution put a lock on such aspects?

Application and Operating System vulnerabilities are nothing new. They have been there and are one of easiest and most effective ways of spreading malware. Take for instance, Adobe PDF exploits are probably one of the most sophisticated exploits to have grown in the malware industry. Most exploits basically bypass two important defences that Microsoft built to protect its OSs – this would include ASLR (Address Spacing Layout Randomization) and DEP (Data Execution Prevention) – reason why applications need to be updated on a regular basis. The same would apply to OS vulnerabilities as there are a great number of users (Businesses/End users) who have the auto update feature turned off. And as mentioned, an unpatched PC is highly vulnerable to malicious attacks.

For a security solution to be most effective both applications and OSs need to be patched on a regular basis. Therefore to get the best of both worlds all eScan products are capable of downloading critical patches related to the Windows OS. This is done automatically without any user intervention thus keeping the PC patched at all times. As far as application patches are concerned it is advisable to update as and when they are made available.

'e Scan
Anti-Virus

Our Offices

USA:
MicroWorld Technologies Inc.
31700 W 13 Mile Rd, Ste 98
Farmington Hills, MI 48334,
USA.

Tel: +1 248 855 2020/2021
Fax: +1 248 855 2024.
TOLL FREE: 1-877-EZ-VIRUS
(USA Only)

E-mail: sales@escanav.com
Web site: www.escanav.com

India:
MicroWorld Software Services Pvt. Ltd.
Plot No.80, Road No.15, MIDC,
Marol, Andheri (E),
Mumbai- 400 093, India.

Tel: +91 22 2826 5701
Fax: +91 22 2830 4750

E-mail: sales@escanav.com
Web site: www.escanav.com

Germany:
MicroWorld Technologies GmbH
Drosselweg 1,
76327 Pfinztal,
Germany.

Tel: +49 72 40 94 49 0920
Fax: +49 72 40 94 49 0992

E-mail: sales@escanav.de
Web site: www.escanav.de

Malaysia:
MicroWorld Technologies Sdn Bhd.
(722338-A)
E-8-6, Megan Avenue 1,
189, Jalan Tun Razak,
50400 Kuala Lumpur, Malaysia.

Tel: +603 2333 8909 / 8910
Fax: +603 2333 8911

E-mail: sales@escanav.com
Web site: www.escanav.com

South Africa:
MicroWorld Technologies South
Africa (Pty) Ltd.
376 Oak Avenue, Block C
(Entrance at 372 Oak Avenue),
Ferndale, Randburg, Gauteng,
South Africa.

Tel: Local 08610 eScan (37226)
International: +27 11 781 4235
Fax: +086 502 0482

E-mail: sales@escan.co.za
Web site: www.escan.co.za