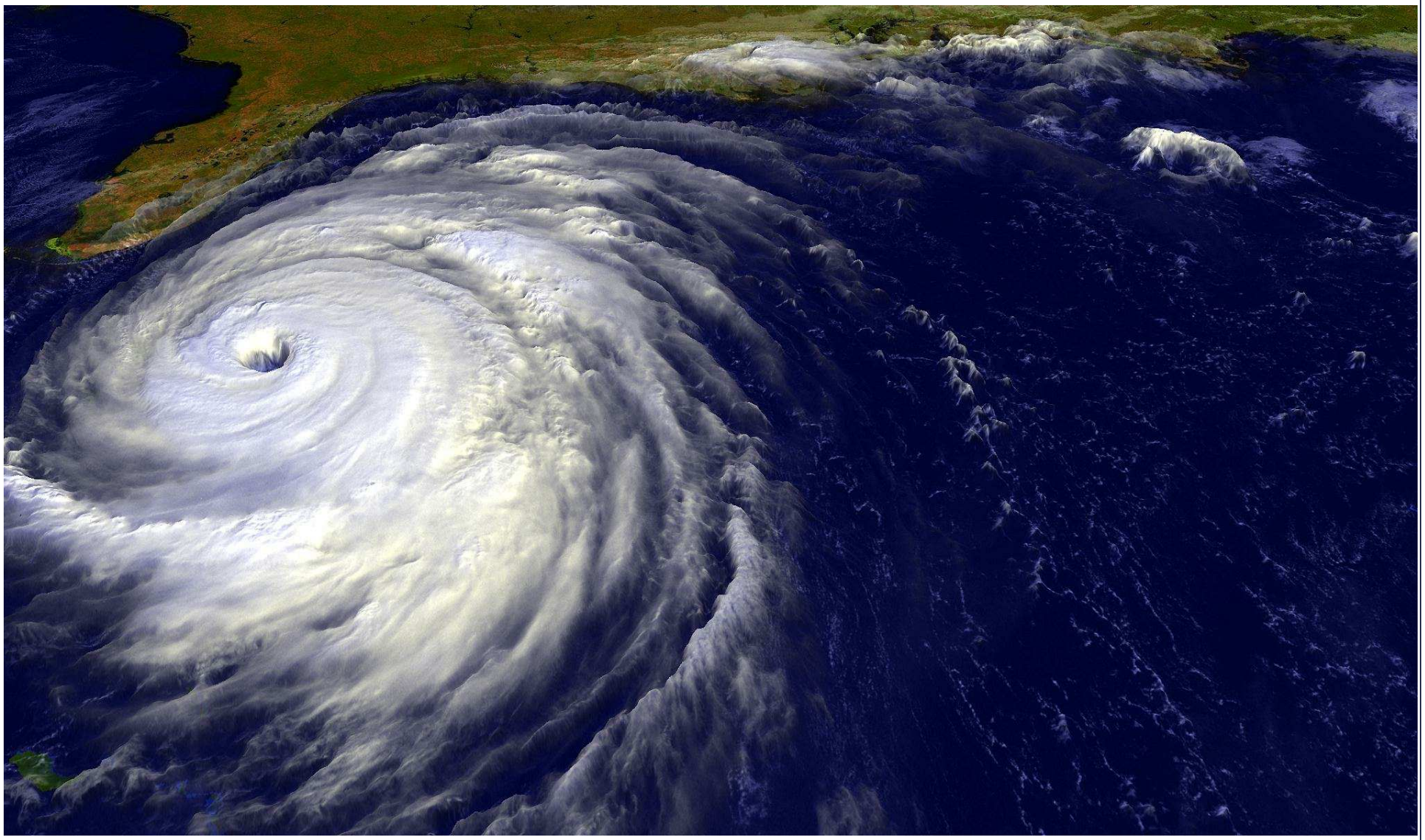
Protect Web Sites from Cyber Attacks

Henry Ng, CISSP-ISSAP CISA
ISC2 Authorized Instructor
Head of Consulting Services
Thales e-Security
Jan 9, 2015

THALES



Lessons learnt

- **The worst can happen**
  - A lot of the damaged areas weren't even within the earthquake regions
- **Insufficient awareness**
  - People didn't understand the dangers behind retreating waves
- **No warning? No alerts?**
  - Early warning system not was in place for Indian Ocean

Common IT security threats

- Virus and worm infection
- Web site defacement
- Denial of service attack
- Un-authorized access
- Data leakage and disclosure
- Advanced targeted attack

Example of web site defacement

Many schools had web site issues

Date	Notifier	H	M	R	L	Domain	OS	View
2015/01/07	Hmei7					[redacted].edu.hk/x.txt	Linux	mirror
2014/12/25	d3b~X	H		R		[redacted]k	Linux	mirror
2014/12/24	Obito_Reborn					[redacted].hk/special_noti...	Linux	mirror
2014/12/24	d3b~X		M			[redacted]ng.htm	Linux	mirror
2014/12/24	d3b~X		M	R		[redacted]ng.htm	Linux	mirror
2014/12/05	Rana MendeX	H				[redacted]	Linux	mirror
2014/11/14	Fatal Error	H		R		[redacted]u.hk	Win 2003	mirror
2014/10/27	UTEPA					[redacted]uns2/images/ute...	Linux	mirror
2014/10/06	KkK1337					[redacted].hk/security/la...	Linux	mirror
2014/10/02	Drac-101code					[redacted]k/r00t.htm	Win 2003	mirror
2014/09/25	Virus_Xtc	H				[redacted]du.hk	Win 2000	mirror
2014/09/10	Hacked By Akram Stelle					[redacted]edu.hk/site/imag...	Linux	mirror
2014/09/10	Hacked By Akram Stelle					[redacted]mages/jdownloa...	Linux	mirror
2014/07/21	意梦玉		M			[redacted]kg.edu.hk/images...	Win 2003	mirror
2014/06/19	Saeed.Jok3r					[redacted].hk/Saeed.Jok3r....	Linux	mirror
2014/05/31	DARKWAR2	H	M			[redacted]	Linux	mirror
2014/05/31	DARKWAR2	H				[redacted]l.edu.hk	Linux	mirror
2014/05/28	silent injector	H	M			[redacted]	Linux	mirror
2014/05/03	Red V!per			R		[redacted]er.gif	Win 2003	mirror
2014/04/21	Index Php					[redacted]/images/g.gif	Win 2008	mirror
2014/03/16	d3b~X					[redacted]/ganteng.gif	Linux	mirror
2014/03/04	d3b~X					[redacted].edu.hk/g...	Linux	mirror
2014/02/17	d3b~X			R		[redacted]web/ganteng.gif	Linux	mirror
2014/02/05	Hmei7			R		[redacted]hk/x.gif	Linux	mirror
2014/02/03	Saeed.Jok3r	H				[redacted]hk	Win 2003	mirror

THALES

Cyber attacks hit the headlines

THALES

Why would anyone attack us

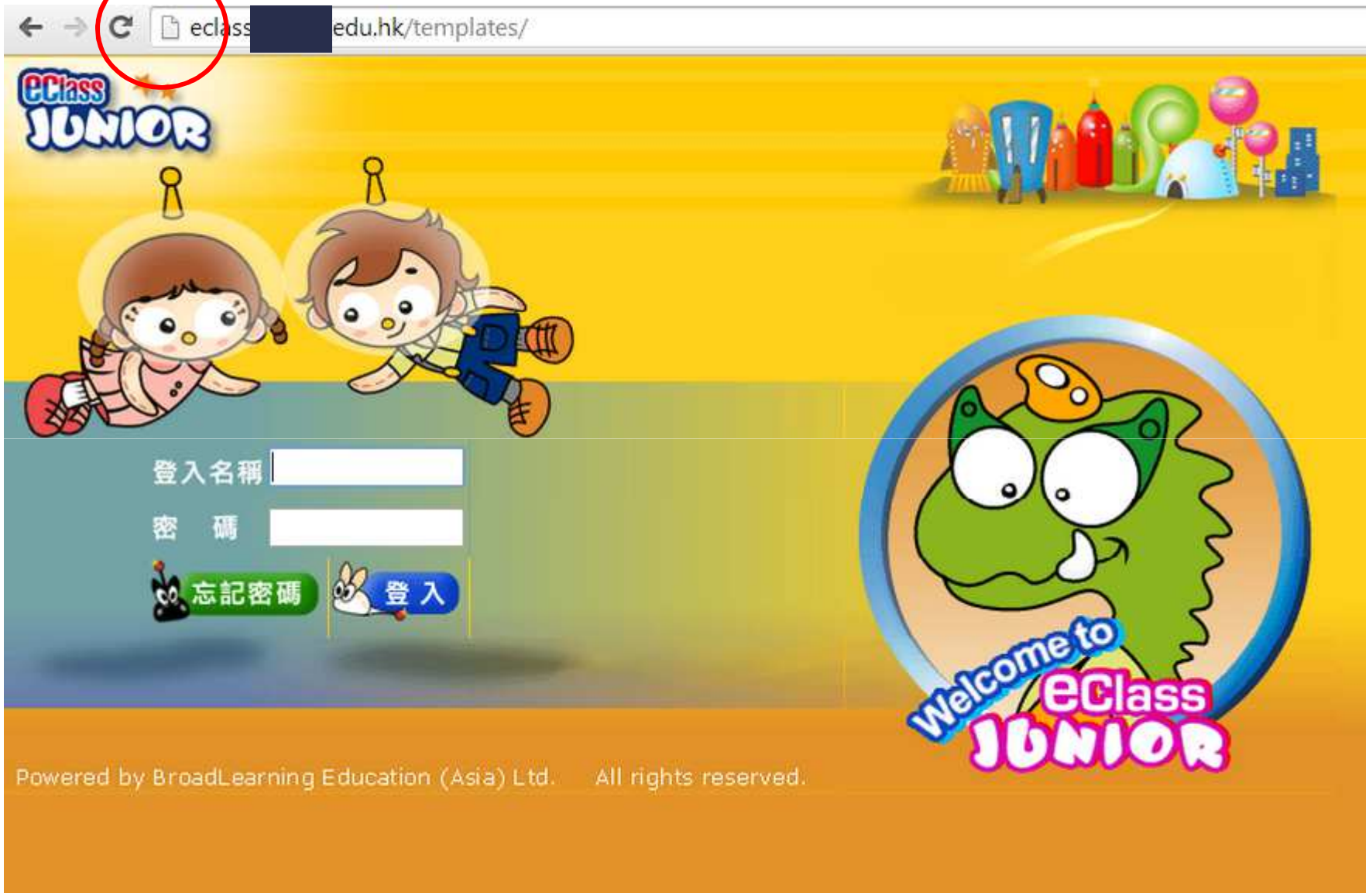
- **Your website is under attack 24 x 7**

We are constantly under attack

2013/04/24 20:33:24 FIREWALL TCP connection denied from 124.237.78.181:6000 to 221.127.131.199:6676 (ppp0)
2013/04/24 20:33:24 FIREWALL TCP connection denied from 124.237.78.181:6000 to 221.127.131.199:6677 (ppp0)
2013/04/24 20:25:22 FIREWALL TCP connection denied from 222.186.13.12:6000 to 221.127.131.199:6675 (ppp0)
2013/04/24 20:22:43 FIREWALL TCP connection denied from 183.245.76.134:6000 to 221.127.131.199:8909 (ppp0)
2013/04/24 20:22:43 FIREWALL TCP connection denied from 183.245.76.134:6000 to 221.127.131.199:9415 (ppp0)
2013/04/24 20:22:43 FIREWALL TCP connection denied from 183.245.76.134:6000 to 221.127.131.199:6666 (ppp0)
2013/04/24 20:11:21 FIREWALL TCP connection denied from 221.214.14.253:6000 to 221.127.131.199:1433 (ppp0)
2013/04/24 20:10:42 FIREWALL TCP connection denied from 221.179.6.228:6000 to 221.127.131.199:1433 (ppp0)
2013/04/24 20:08:41 FIREWALL TCP connection denied from 183.245.168.81:6000 to 221.127.131.199:3389 (ppp0)
2013/04/24 20:07:46 FIREWALL TCP connection denied from 24.84.214.249:53369 to 221.127.131.199:6675 (ppp0)
2013/04/24 20:05:53 FIREWALL TCP connection denied from 61.147.103.79:6000 to 221.127.131.199:1433 (ppp0)
2013/04/24 20:03:18 FIREWALL TCP connection denied from 222.186.27.78:6000 to 221.127.131.199:6666 (ppp0)
2013/04/24 20:00:52 FIREWALL TCP connection denied from 221.179.6.228:6000 to 221.127.131.199:1433 (ppp0)
2013/04/24 19:59:50 FIREWALL TCP connection denied from 176.61.139.128:2998 to 221.127.131.199:3128 (ppp0)
2013/04/24 19:59:44 FIREWALL TCP connection denied from 176.61.139.128:2998 to 221.127.131.199:3128 (ppp0)
2013/04/24 19:59:42 FIREWALL TCP connection denied from 176.61.139.128:2998 to 221.127.131.199:3128 (ppp0)
2013/04/24 19:58:41 FIREWALL TCP connection denied from 58.221.60.182:6000 to 221.127.131.199:6675 (ppp0)
2013/04/24 19:58:38 FIREWALL TCP connection denied from 192.198.82.21:6000 to 221.127.131.199:3389 (ppp0)
2013/04/24 19:53:51 FIREWALL TCP connection denied from 222.186.27.78:6000 to 221.127.131.199:6666 (ppp0)
2013/04/24 19:48:44 FIREWALL TCP connection denied from 112.101.64.233:6000 to 221.127.131.199:6666 (ppp0)
2013/04/24 19:42:16 FIREWALL TCP connection denied from 222.186.63.181:6000 to 221.127.131.199:6675 (ppp0)
2013/04/24 19:40:34 FIREWALL TCP connection denied from 222.76.218.81:6000 to 221.127.131.199:1433 (ppp0)
2013/04/24 19:39:28 FIREWALL TCP connection denied from 222.186.45.164:6000 to 221.127.131.199:6666 (ppp0)
2013/04/24 19:38:13 FIREWALL TCP connection denied from 218.22.2.68:6000 to 221.127.131.199:1433 (ppp0)
2013/04/24 19:36:23 FIREWALL TCP connection denied from 58.221.59.172:6000 to 221.127.131.199:6675 (ppp0)
2013/04/24 19:35:01 FIREWALL TCP connection denied from 222.186.45.139:6000 to 221.127.131.199:6675 (ppp0)
2013/04/24 19:34:35 FIREWALL TCP connection denied from 223.4.218.71:6000 to 221.127.131.199:1433 (ppp0)
2013/04/24 19:30:58 FIREWALL TCP connection denied from 142.4.38.49:6000 to 221.127.131.199:1433 (ppp0)
2013/04/24 19:30:45 FIREWALL TCP connection denied from 50.22.220.130:80 to 221.127.131.199:57694 (ppp0)
2013/04/24 19:29:48 FIREWALL TCP connection denied from 118.244.146.200:12200 to 221.127.131.199:6668 (ppp0)
2013/04/24 19:28:48 FIREWALL TCP connection denied from 218.92.244.234:6000 to 221.127.131.199:3389 (ppp0)
2013/04/24 19:27:25 FIREWALL TCP connection denied from 118.244.146.200:12200 to 221.127.131.199:6668 (ppp0)
2013/04/24 19:26:51 FIREWALL TCP connection denied from 221.169.207.102:3143 to 221.127.131.199:23 (ppp0)

Why would anyone attack us

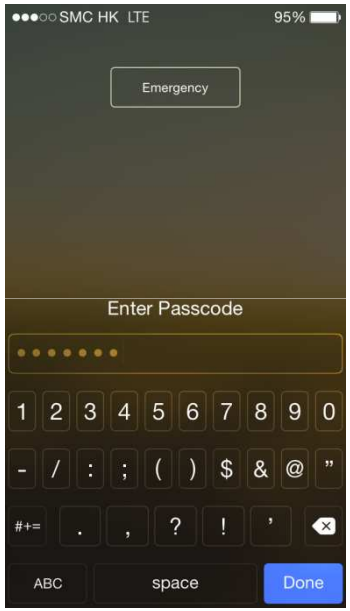
- **Your website is under attack 24 x 7**
- **Unpatched vulnerabilities threaten your website**


eclass [redacted] edu.hk/templates/
eClass JUNIOR
登入名稱
密 碼
忘記密碼
登 入
Welcome to eClass JUNIOR
Powered by BroadLearning Education (Asia) Ltd. All rights reserved.

Why would anyone attack us

- Your website is under attack 24 x 7
- Unpatched vulnerabilities threaten your website
- Hackers are more smart and efficient than ever


Enter Passcode
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
Emergency Call
0
Cancel


SMC HK LTE
95%
Emergency
Enter Passcode
1 2 3 4 5 6 7 8 9 0
- / : ; ( ) $ & @ "
#+= . , ? ! '
ABC
space
Done

Why would anyone attack us

- Your website is under attack 24 x 7
- Unpatched vulnerabilities threaten your website
- Hackers are more smart and efficient than ever
- No matter how small of your website

電子學習在全球各地興起，本港陸續有中、小學校嘗試在課堂引入電子教...而，不少前線教師卻面對軟硬件配套不足、電子教科書貧乏、技術支援人手有限等問題，窒礙電子學習發展。來自資訊科技界別的陳岡毅於今年8月創辦「未來學校聯盟」，以「共享」、「標準化」、「環保」及「平等」為理念，聯同多名志同道合的教師，積極推動電子學習普及化，以建構一個資訊科技教育資源共享生態系統，最終令學生和教師得益。

未來學校聯盟 積極推動電子學習普及化

▲一群教育界熱心人士組成未來學校聯盟，共同推動電子學習普及化，促進學生自主學習。

▲健康長跑徑裝置了「單點RFID晶片戶外檢測系統」，記錄學生的練習成績和分析數據更為便捷。

▲學生透過平板電腦上課，令學習更多元和有趣。

本港的電子學習現時處於萌芽階段，教師及學生均在試用和探索當中。未來學校聯盟創辦人陳岡毅從事資訊科技生意，與學校教師探討如何將資訊科技系統結合教學時，了解到電子學習普及化所面對的問題，他說：「每間學校都有不同的資訊科技教學標準，而供應商會遇上產品數量訂購不足問題，加上現時資訊科技教育無論在設備、軟件和電子書均欠缺一致標準，教師要在技術整合問題上花費大量精力。因此，我希望透過成立『未來學校聯盟』，促進教育界和科技界人員互相分享和協作，共同制訂一套行業標準，讓科技界能夠根據導向，製作合適的電子教學產品，讓教師和學生能夠共享教育資源。」

另一方面，隨着電子學習普及化，或會衍生出大量電子廢物，破壞環境；同時，基層家庭因無力購買流動電腦裝置而出現「數碼鴻溝」問題。陳岡毅表示，聯盟會致力推廣環保工作，促請業界重視源頭減廢，並透過回收二手電子設備，扶助弱勢社群能夠得到平等的學習機會。

向政府提交電子學習意見書

「未來學校聯盟」由籌備至成立短短不足一年時間，已先後舉辦多項推動電子學習的活動，包括：「未來學校雲端之旅」、論壇，以及在港澳信義會小學聯盟成立中央實驗室，研發及測試「學校專用虛擬化VDI系統」。就來年度施政報告和財政預算案，聯盟近日向特區政府提交意見書，期望政府關注電子學習所面對的問題。

教育局電子教科書市場開拓計劃（EMADS）推行兩年以來，電子教科書供應量和學校使用量都偏低。先導會員鄧文雅老師（喇沙小學資訊科技主任）及程志祥老師（港澳信義會小學資訊科技主任）均指出，目前小學電子教科書配套不足，基本上與印刷書本分別不大，未能充分發揮電子功能。黃耀輝副校長（長沙灣天主教英文中學）慨嘆，中學缺乏可用的電子教科書：「基本上完全沒有選擇。」陳岡毅建議政府為業界提供更多支援，令教具、工作紙和題目庫更充足，同時延長開發商兩至三年開發周期，以便累積經驗和成果。

▲未來學校聯盟創辦人陳岡毅認為，教育界和科技界的持份者要共同制訂一套標準，才能令電子學習推行成功。

電子教科書的發展處於起步階段，而政府未有提供額外撥款聘請人手，令不少學校的資訊科技科教師需要兼顧電子學習的技術支援工作，聯盟建議政府新增「電子學習支援技術員」一職，以減輕教師的工作量。另一方面，聯盟建議由科技教師支援各學科教師，逐步實踐先導課堂，以掌握電子學習課堂。程志祥老師表示：「電子學習和傳統教學屬兩極化，透過試教和觀課，方能改變老師的教學觀念。」

▲程志祥老師表示，目前小學電子教科書配套不足。

世界進入大數據年代

隨着智能手機和流動裝置普及，世界進入大數據年代，聯盟建議政府資助全港中、小學興建健康長跑徑，並裝置低成本的「單點RFID晶片戶外檢測系統」，鼓勵學生自主練習健康長跑。長沙灣天主教英文中學體育科主任李德輝表示，系統會記錄學生的練習成績，傳送至學校的電腦數據庫，能夠更科學化地評估學生的表現，而學生和家長透過流動裝置了解自己的數據表現，從而培養學生自主學習精神。此外，透過大數據科學化分析，能夠幫助政府掌握中小學生的運動量和表現，制訂更全面的體育政策。

另外，聯盟建議政府全面展開電子學習的指引：檢討現時招標指引，提高透明度和公平競爭，避免側重同一間機構承接無線網絡基建；打造香港成為「全球資訊科技教育創新和外包服務之都」；以及支援團體進行電子產品設備回收工作，惠及基層家庭。

意見書全文

聯盟Facebook

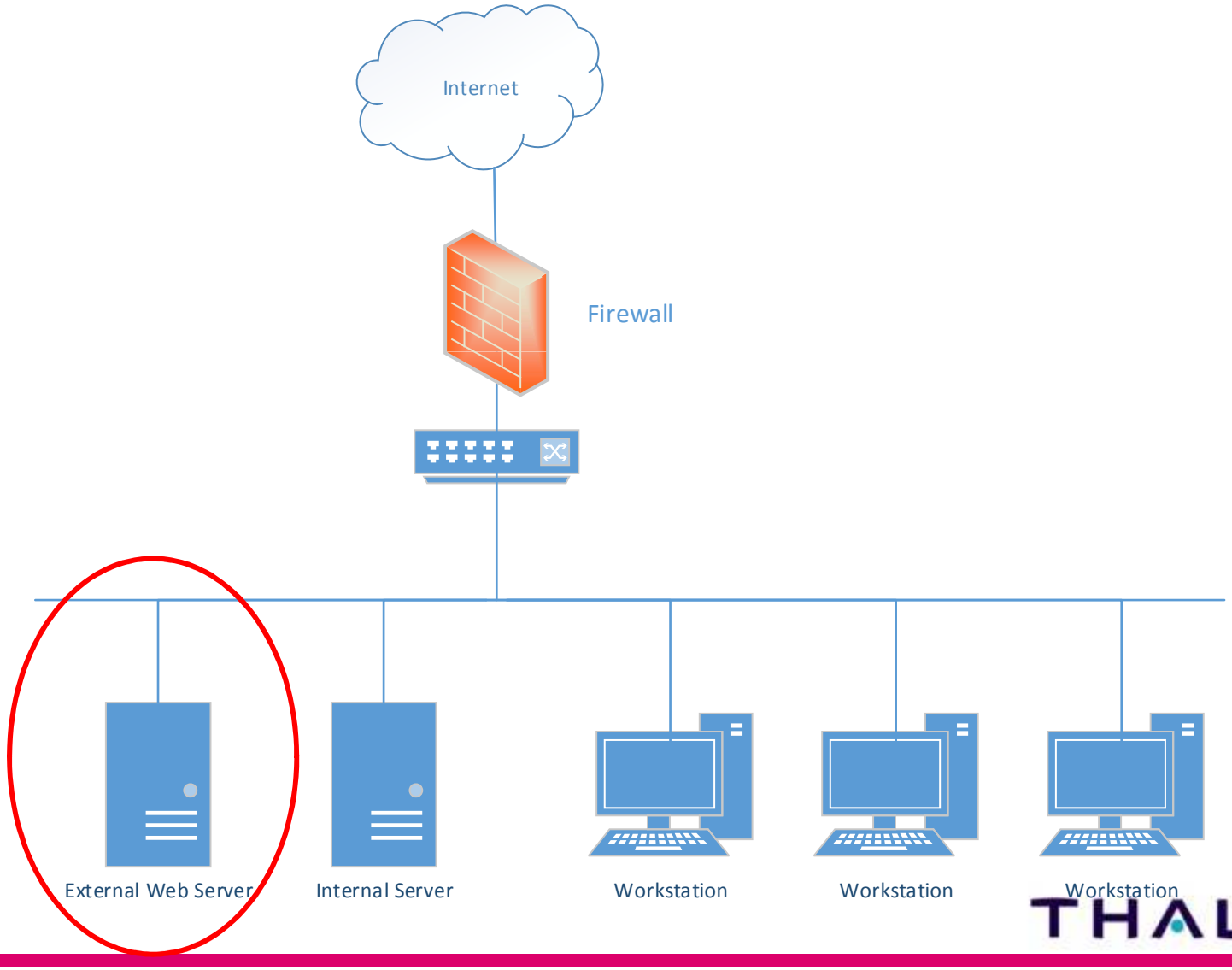
Recommendations - 1

1. Implement basic security controls

- Firewalls
- System security hardening
- Anti-virus
- Wireless encryption
- Workstation lock-down

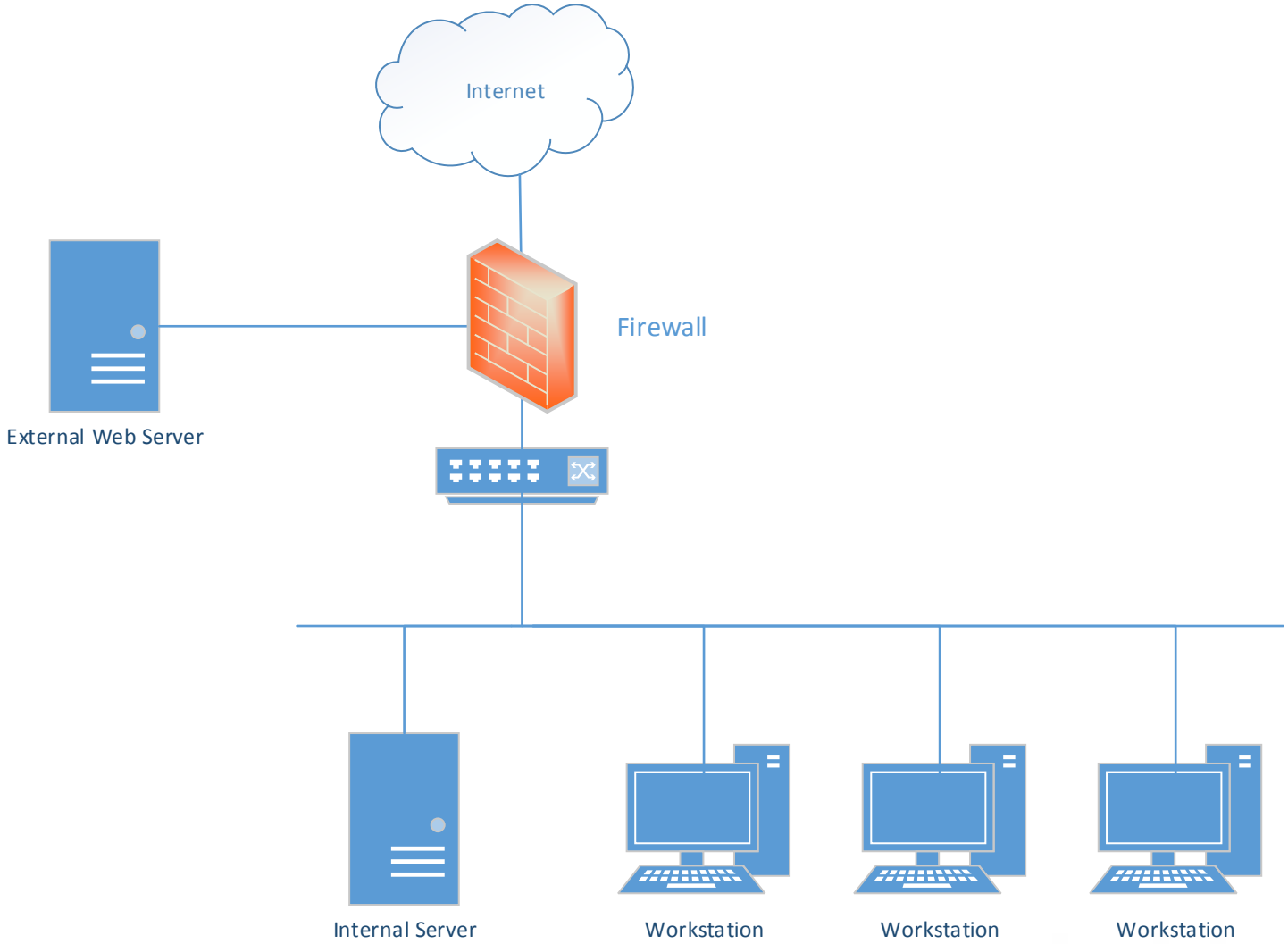
Recommendations - 2

2. Implementation segmentation



Recommendations - 2

2. Implementation segmentation



THALES

Recommendations - 3

3. Implement additional security best practices

- Installing Web Application Firewall (WAF) in front of web application to continually check all traffic to detect and prevent web-based attacks
- Update to the most current version and install all relevant security patches and vendor security recommendations
- Perform vulnerability assessment to assess web security issues
- Enforce security configuration standards according to industry-accepted system hardening standards
- Include security requirements as part of the procurement process

Recommendations - 4

4. Build Risk Awareness

Source for more information

- **OWASP – Open Web Application Security Project (www.owasp.org)**
- **CIS – Center for Internet Security (www.cissecurity.org)**
- **NIST – National Institute of Standards and Technology (csrc.nist.gov)**
- **HKCERT – Hong Kong Computer Emergency Response Team (www.hkcert.org)**
- **Hong Kong Government - Infosec Web Site (www.infosec.gov.hk)**

Thank You

Henry Ng, CISSP-ISSAP CISA
ISC2 Authorized Instructor
Head of Consulting Services
Thales e-Security

+852 2534 6625 (O)
+852 9317 6844 (M)

THALES