



Don't take security off your priority list

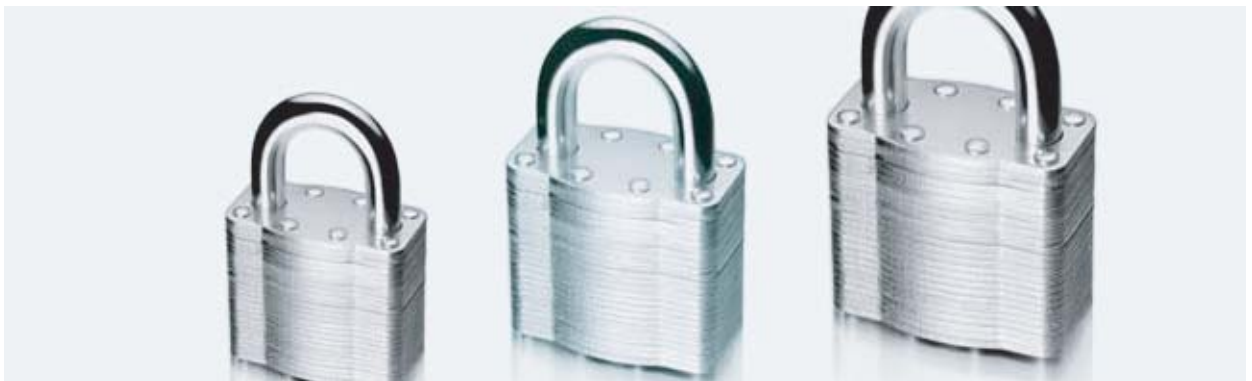
Datacraft's security experts identify security trends in the global marketplace



With the advances of technology and the media hype surrounding security risks, one would assume that security would always remain at the top of organisations' priority lists. From experience, Datacraft's security specialists know that this is not always the case.

Security assessments are conducted for our clients to provide them with a snapshot of their security postures, assessing their overall information security programme and corporate governance. Using our industry experience in security, coupled with the findings of all assessments that we have completed for clients around the globe thus far, we have been able to identify a number of security trends in the marketplace.

Some of the trends identified by Datacraft's security specialists include the following:



Technology is not enough

Organisations' views on security are still primarily focused on hardware and software instead of implementing defence-in-depth strategies. IT departments authorise reactive short-term fixes without looking at the full context of any incidents, or they rely heavily on technology in lieu of programmes that include components of risk management, process, organisation and people.

Organisations rely heavily on security perimeter technologies such as perimeter firewalls and VPNs, with much less focus on internal security. Perimeter technologies need to be expanded and the focus needs to be on internal security measures, such as Internal Segmentation, Intrusion Prevention, Vulnerability Management and Admission Control.

Organisations are realising that in today's business environment, "an internal network is not much safer than an external network". Enterprises are required to provide more users with access to their network and information resources; they have to manage multiple levels of access to their information resources, based on the users' roles and responsibilities, whether it is for customers or business partners requiring access to information, or for mobile users requiring access to applications from outside the enterprise's walls, to name but a few.

People and organisations can have a big impact

Few organisations have incorporated internal security training and awareness programmes into their overall security strategy.

Most end-users and business managers have not been made aware of the security risks of accessing the corporate network while working from home or on the move, and how this can impact the organisation.

Organisations can implement as much security technology as they deem necessary, but without making the end-user aware of how their actions can pose a security risk, technology has a limited effect.

Compliance does not equal security

Organisations in general have yet to accept risk management and corporate governance as core to their overall security programmes and there is still a lot of work to be done involving top management.

Traditionally, security has been left in the hands of the IT department. As such, top management is not really involved in the overall risk management plan of the organisation as it relates to IT security.

There is a considerable lack of awareness among business managers regarding how security impacts the organisation. Most business managers also equate compliance with security, to the detriment of the organisation which is often the case.

The Sarbanes-Oxley Act dictates that organisations need to control access to their systems and also report on the users who have accessed the different systems. To enable this, security tools are required. This doesn't necessarily mean that the organisation is free from hackers, spyware and all other security issues. It just means that the organisation has the ability to check and identify users who access specific systems.

Processes are key

Companies in general demonstrate few efforts around security programme assurance, event logging, incident reporting and pro-active response activities. As such, many organisations do not have an information security strategy that details processes to further ensure complete security.

Some companies also implement the best security technology available on the market, without having the people or the skills to properly manage these tools, and to ensure that proper processes are followed. A practical example is where users make changes on the network. However, without a change management process in place, this may pose a security risk.

While organisations often increase spending on security technologies, the number of incidents continue to rise, which shows that a holistic and proactive approach to security is the best way forward.



Top 10 mistakes organisations make when it comes to information security:

1. Not having an information security strategy
2. Failing to get executive support for security programme
3. Thinking that security is only a technology or IT department problem
4. Equating compliance with security
5. Authorising reactive short-term fixes
6. Failing to recognise the importance of security awareness programmes
7. Failing to recognise the demise of traditional perimeter security
8. Failing to protect laptop and corporate home-use computers
9. Failing to understand the relationship of IT security in relation to business processes
10. Failing to institute effective change management



About Datacraft's CxO Security Assessment:

The CxO Security Assessment is a unique tool designed to provide senior executives with a snapshot and assessment of the company's information security risk profile. We have combined and adapted a number of international security best practices into a weighted self-scoring questionnaire that takes no more than four hours to complete.

The tool assists CxOs and their teams to quickly assess their company's overall information security programme and corporate governance. The aim is to identify areas for improvement and suggest remediation actions to reduce risk around People and Organisation, Processes, Technology and Risk Management. The Assessment has been compiled based on information sourced from the SANS Institute, Internet Security Alliance, ISO/IEC 17799, COBIT and Gartner, among others.

The CxO Security Assessment has helped many of our clients to:

- ▲ Gain instant access to a security maturity score and recommendations for remediation
- ▲ Develop an action plan based on priorities and strategy recommendations
- ▲ Gain a holistic view of more than 100 functional areas, tailored to the organisation's specific IT dependence
- ▲ Become educated on industry best practices and benchmarked against industry peers
- ▲ Allocate expenses using the scorecard as a justification tool for budgets, progress and expenditure approval
- ▲ Define roles and responsibilities and measure performance against key areas

For more information on Datacraft's CxO Security Assessment, please email compliance@datacraft-asia.com

Alternatively, please contact your Datacraft Client Manager.

HEADQUARTERS

Datacraft Asia Ltd
6 Temasek Boulevard
#26-01/05
Suntec Tower Four
Singapore 038986
Tel : (65) 6322 6688
Fax: (65) 6323 7933

Datacraft Asia Ltd
3/F Citiplaza III
14 Taikoo Wan Road
Taikoo Shing, Hong Kong
Tel : (852) 2513 3168
Fax: (852) 2567 4268

SINGAPORE

Tel : (65) 6517 2000
Fax: (65) 6517 2001

HONG KONG

Tel : (852) 2513 3168
Fax: (852) 2567 4031

CHINA

Beijing
Tel : (86) 10 8525 1108/
1106/1186
Fax: (86) 10 8525 1126

Shanghai

Tel : (86) 21 3222 0068
Fax: (86) 21 5298 6001

Guangzhou

Tel : (86) 20 8558 2553
Fax: (86) 20 8558 3908

Shenzhen

Tel : (86) 755 8207 8511-2
Fax: (86) 755 8207 8513

Chengdu

Tel : (86) 28 8619 8315-6
Fax: (86) 28 8619 8794

Hangzhou

Tel : (86) 571 8527 1271-3
Fax: (86) 571 8527 1290

MALAYSIA

Kuala Lumpur
Tel : (603) 2166 6363
Fax: (603) 2166 7728

Penang

Tel : (604) 647 2875
Fax: (604) 646 4299

THAILAND

Tel : (662) 661 9777
Fax: (662) 661 9778

INDIA

Mumbai
Tel : (91) 22 2498 1212
Fax: (91) 22 2497 1818

Bangalore

Tel : (91) 80 22077000
Fax: (91) 80 22077111

New Delhi

Tel : (91) 11 2693 6800
Fax: (91) 11 2693 6801

Chennai

Tel : (91) 44 2829 4468/70
Fax: (91) 44 2829 3239

Kolkata

Tel : (91) 33 2282 0040/41
Fax: (91) 33 2865 0165

Hyderabad

Tel : (91) 40 5566 7706
Fax: (91) 40 2340 8806

Pune

Tel : (91) 20 2553 9141
Fax: (91) 20 2553 0874

TAIWAN

Tel : (886) 2 2171 3333
Fax: (886) 2 2171 3399

INDONESIA

Tel : (62) 21 835 6422
Fax: (62) 21 835 6423

PHILIPPINES

Tel : (632) 750 9927
Fax: (632) 750 6890

VIETNAM

Hanoi
Tel : (84) 4 9435758
Fax: (84) 4 9435730

Ho Chi Minh City

Tel : (84) 8 823 6750
Fax: (84) 8 825 7848

KOREA

Seoul
Tel : (82) 2 6256 7000
Fax: (82) 2 6256 7199

Daejun

Tel : (82) 42 487 4272
Fax: (82) 42 487 4273

JAPAN

Tel : (81) 3 3259 2222
Fax: (81) 3 3259 2390

NEW ZEALAND

Auckland
Tel : (64) 9 356 5680
Fax: (64) 9 356 5698

Wellington

Tel : (64) 4 470 1650
Fax: (64) 4 470 1666

DATA-CRAFT SUBSIDIARY

Training Partners Pte Ltd
Tel : (65) 6225 9188
Fax: (65) 6225 9288