BLUE COAT

Security Empowers Business

Cyber Security & Employees: Are their Eyes Wide Shut?

Understand and Mitigate the Risk from Insider Threats

EMPLOYEE BEHAVIOUR: A REAL AND PRESENT DANGER?

Yes! According to Blue Coat's latest Global Cyber Security Study.
Employee-enabled cyber threats are a big global issue.

51% use personal devices for work

Nearly **2 in 5** use social media for personal reasons at work

20% open emails from unverified sources

xXx **6%** view adult content

These are potential risks to security that need to be managed – particularly if businesses are to take full advantage of the use of personal devices and social media at work.

Employees inevitably pose a risk.
But do they really understand how perilous their online behaviour is?

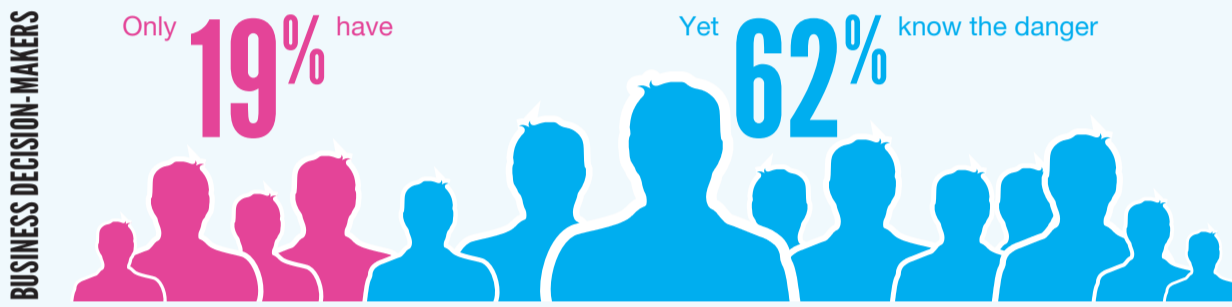## WALK THE WALK: IS THE SAFE SURFING MESSAGE GETTING THROUGH?

Our Global Cyber Security Study showed that employees really do understand their role in exposing their employer to the risk of cyber attacks…

CLICK HERE **73%** know that opening an email attachment from an unverified source is a business risk

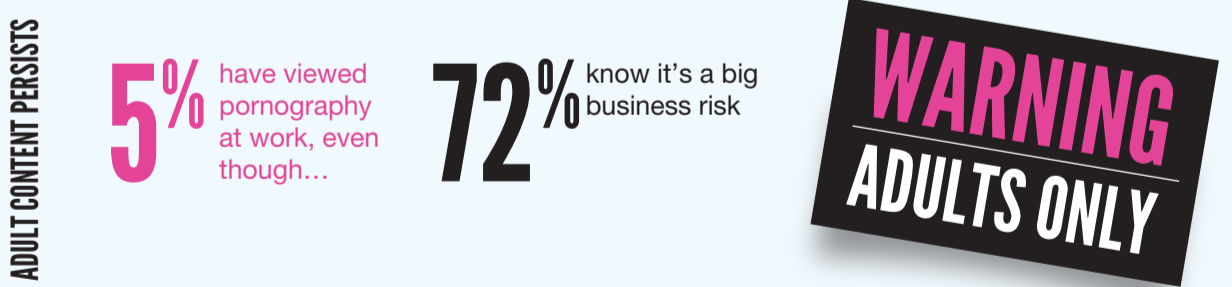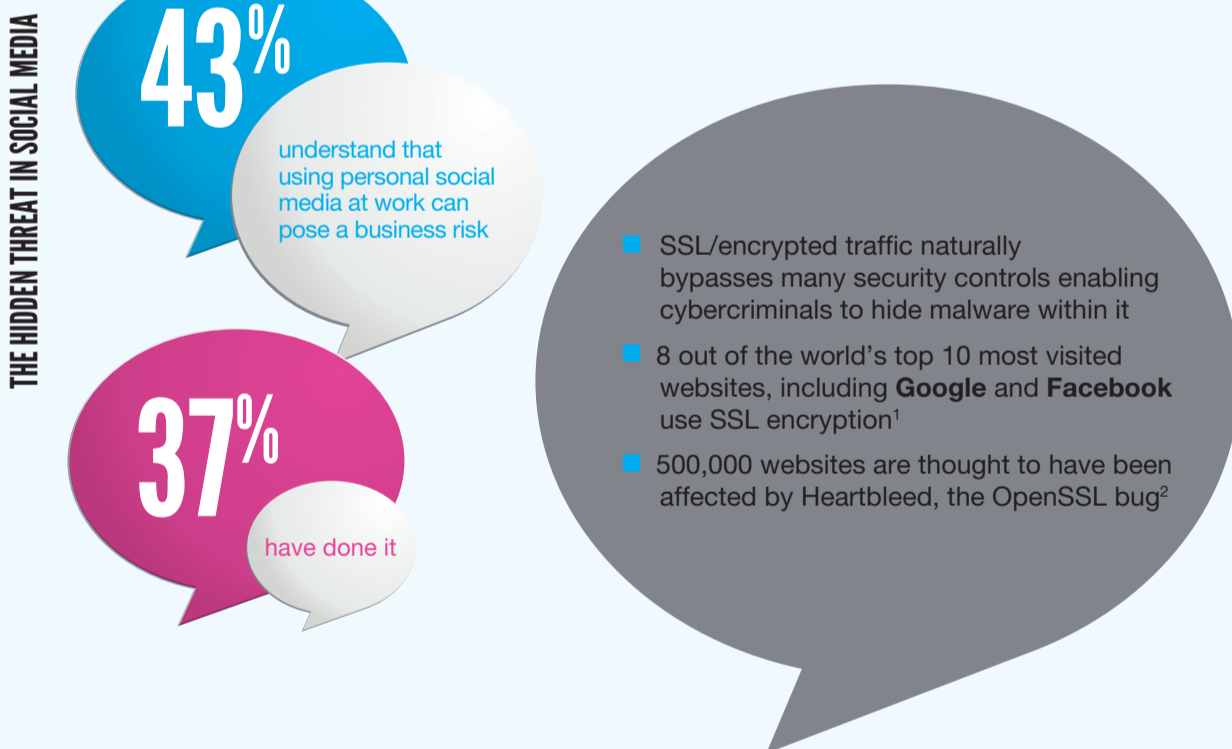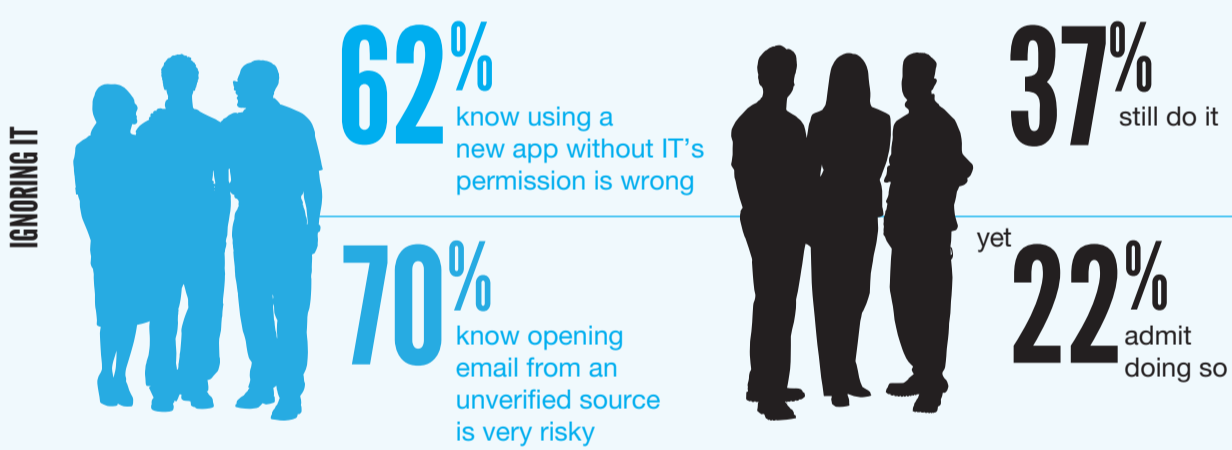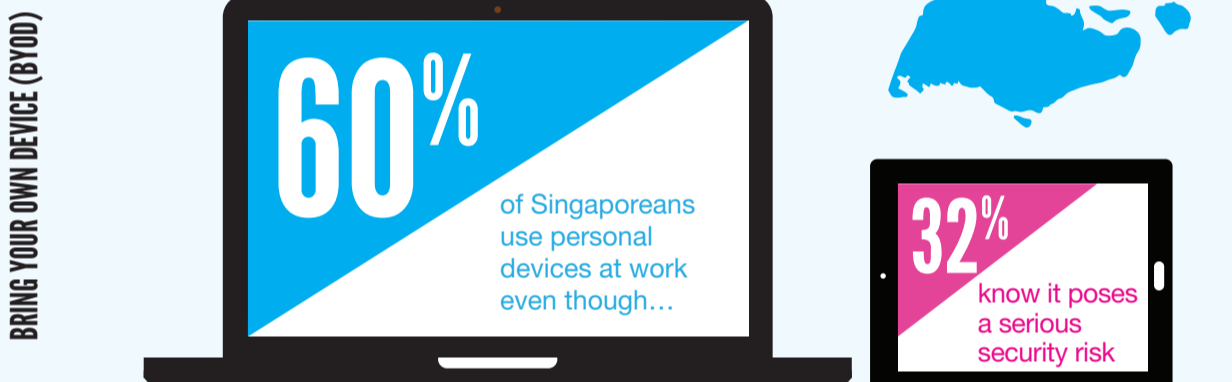DOWNLOAD NOW **65%** know that using a new app without IT's approval is a serious threat

Yet they still pursue risky activities – talking the talk, without walking the walk.
In fact, line of business staff take the risk of cyber crime more seriously than IT decision-makers and participate in fewer risky activities, for example:

**Q:** Have you downloaded apps from **outside** the Apple AppStore or Google Play?

IT DECISION-MAKERS
28% have
61% know it's seriously risky

BUSINESS DECISION-MAKERS
Only **19%** have
Yet **62%** know the danger

AWARENESS vs. ACTION: SINGAPORE USERS BEHAVING BADLY

BRING YOUR OWN DEVICE (BYOD)
60% of Singaporeans use personal devices at work even though…
32% know it poses a serious security risk

IGNORING IT
62% know using a new app without IT's permission is wrong
37% still do it
70% know opening email from an unverified source is very risky
yet **22%** admit doing so

THE HIDDEN THREAT IN SOCIAL MEDIA
43% understand that using personal social media at work can pose a business risk
37% have done it

- SSL/encrypted traffic naturally bypasses many security controls enabling cybercriminals to hide malware within it
- 8 out of the world's top 10 most visited websites, including **Google** and **Facebook** use SSL encryption[1]
- 500,000 websites are thought to have been affected by Heartbleed, the OpenSSL bug[2]

ADULT CONTENT PERSISTS
5% have viewed pornography at work, even though…
72% know it's a big business risk

WARNING
ADULTS ONLY

WHAT'S THE ANSWER? DON'T BAN TECH!

Technology is seen as the key to achieving business goals – even if it increases security risk.

Would you deploy new technologies to achieve your business goals, even if it increased security risk?

69% Global
70% United States
75% Asia Pacific
82% Singapore
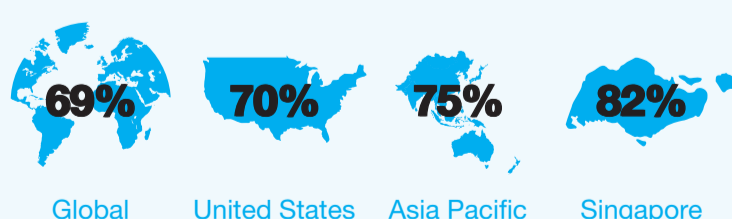
Curb bad behaviour. Protect your organisation.

Trends like social media and BYOD are beneficial. So keep them, don't ban them:

✓ 83% of employees say flexible IT – including BYOD – increases their job satisfaction[3]
✓ Full social media deployment can raise knowledge workers' productivity by 20-25%[4]

INSTEAD, TAKE THREE STEPS TO HELP COMBAT EMPLOYEES' RISKY ONLINE BEHAVIOUR:

01. EDUCATE
Develop a safe usage policy. Try www.staysafeonline.org for help

02. DEPLOY
Dynamic, enforceable security policies by role

03. SECURE
Use technologies, like those from Blue Coat, that deliver granular control to identify potential user-based risks

DISCOVER HOW SECURITY EMPOWERS BUSINESS

www.bluecoat.com