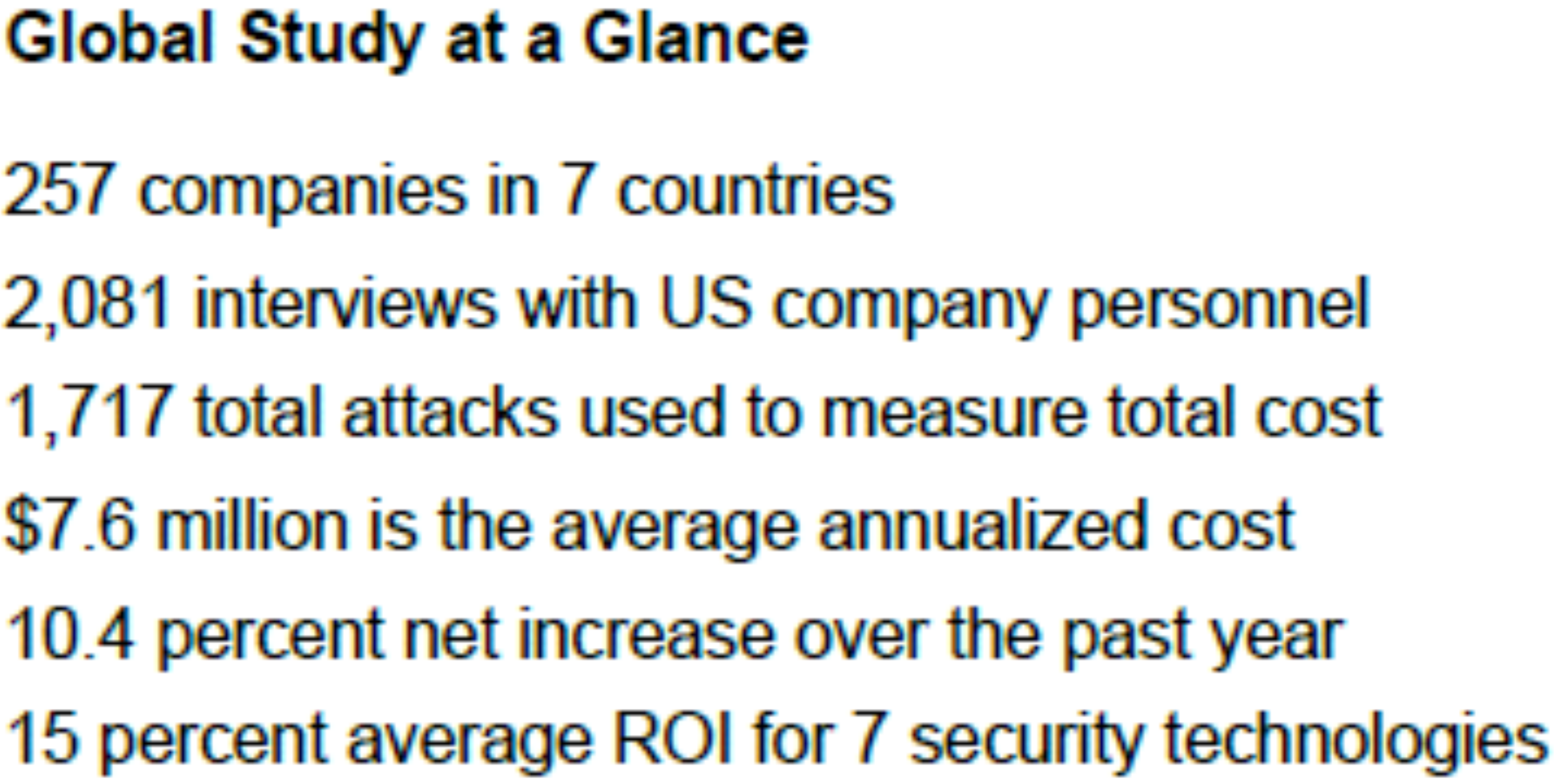
IT Security /Cyber Attacks

Before we begin –
2014 HP Report – Global Cost of Cyber Crime



Global Study at a Glance

257 companies in 7 countries

2,081 interviews with US company personnel

1,717 total attacks used to measure total cost

$7.6 million is the average annualized cost

10.4 percent net increase over the past year

15 percent average ROI for 7 security technologies

Figure 12. Some attacks take longer to resolve

Estimated average time is measured for each attack type in days
Consolidated view, n = 257 separate companies

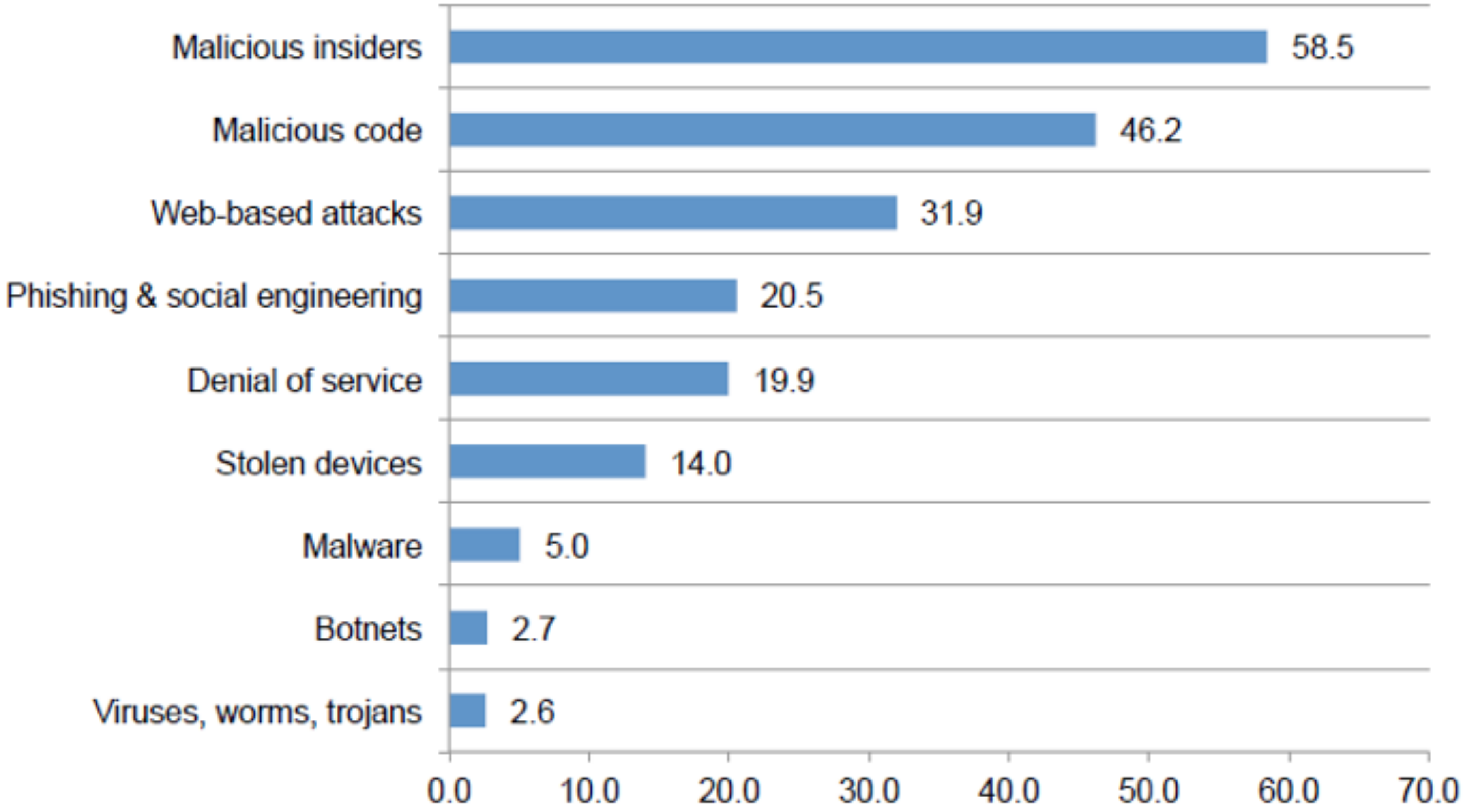


Figure 13. Percentage cost for external consequences
Consolidated view, n = 257 separate companies

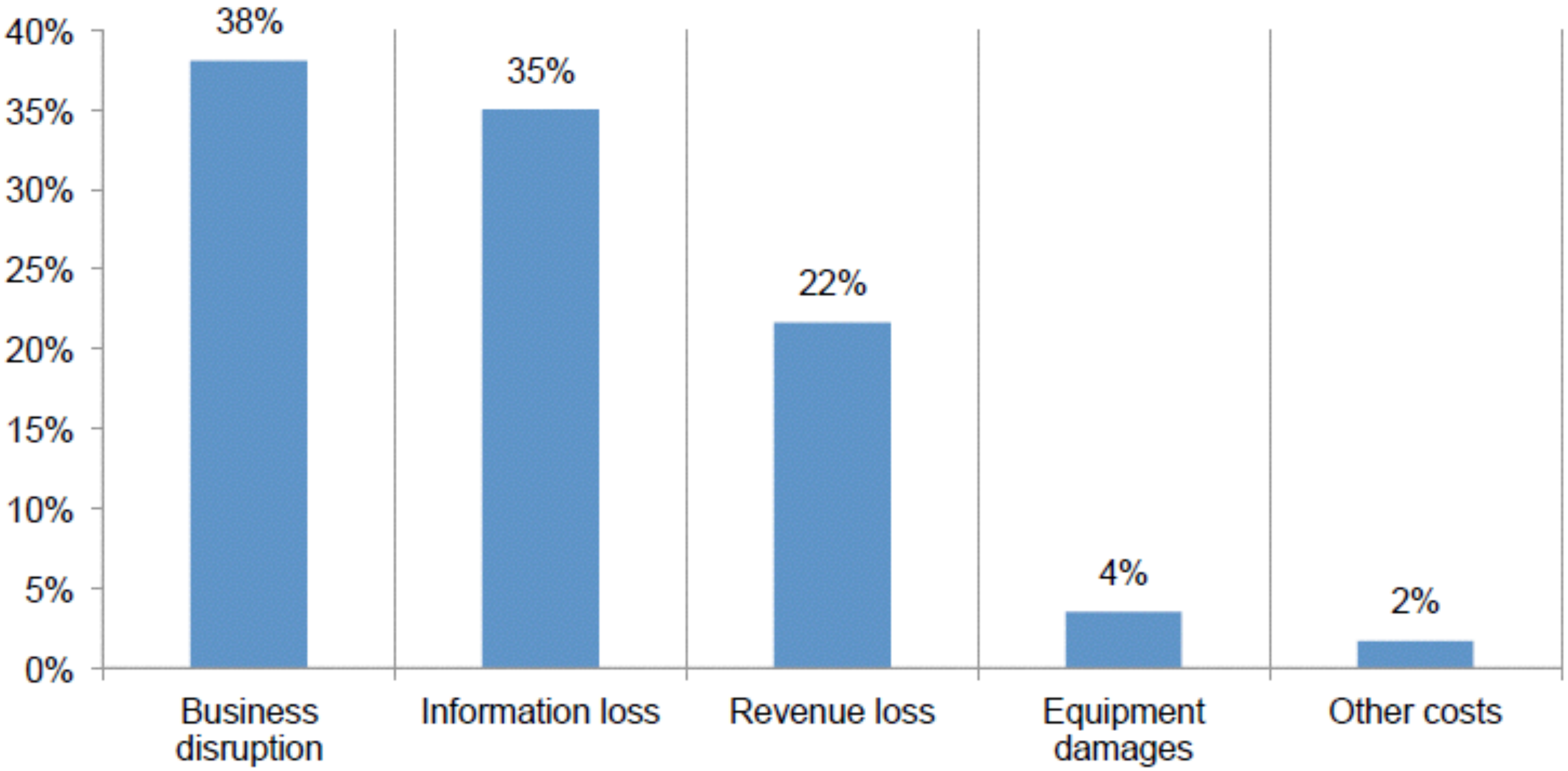


Figure 14. Percentage cost by activities conducted to resolve a cyber attack

Consolidated view, n = 257 separate companies

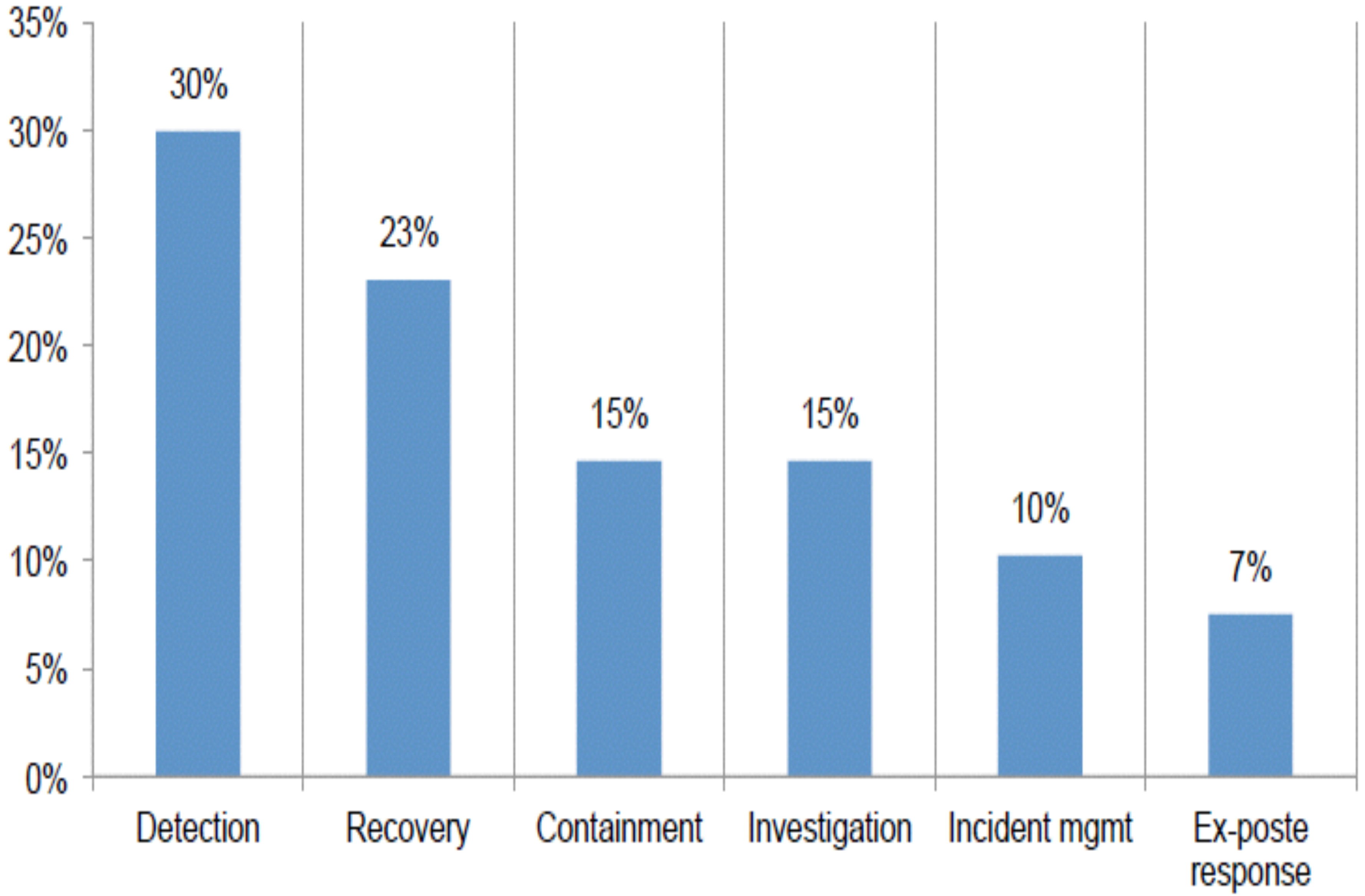
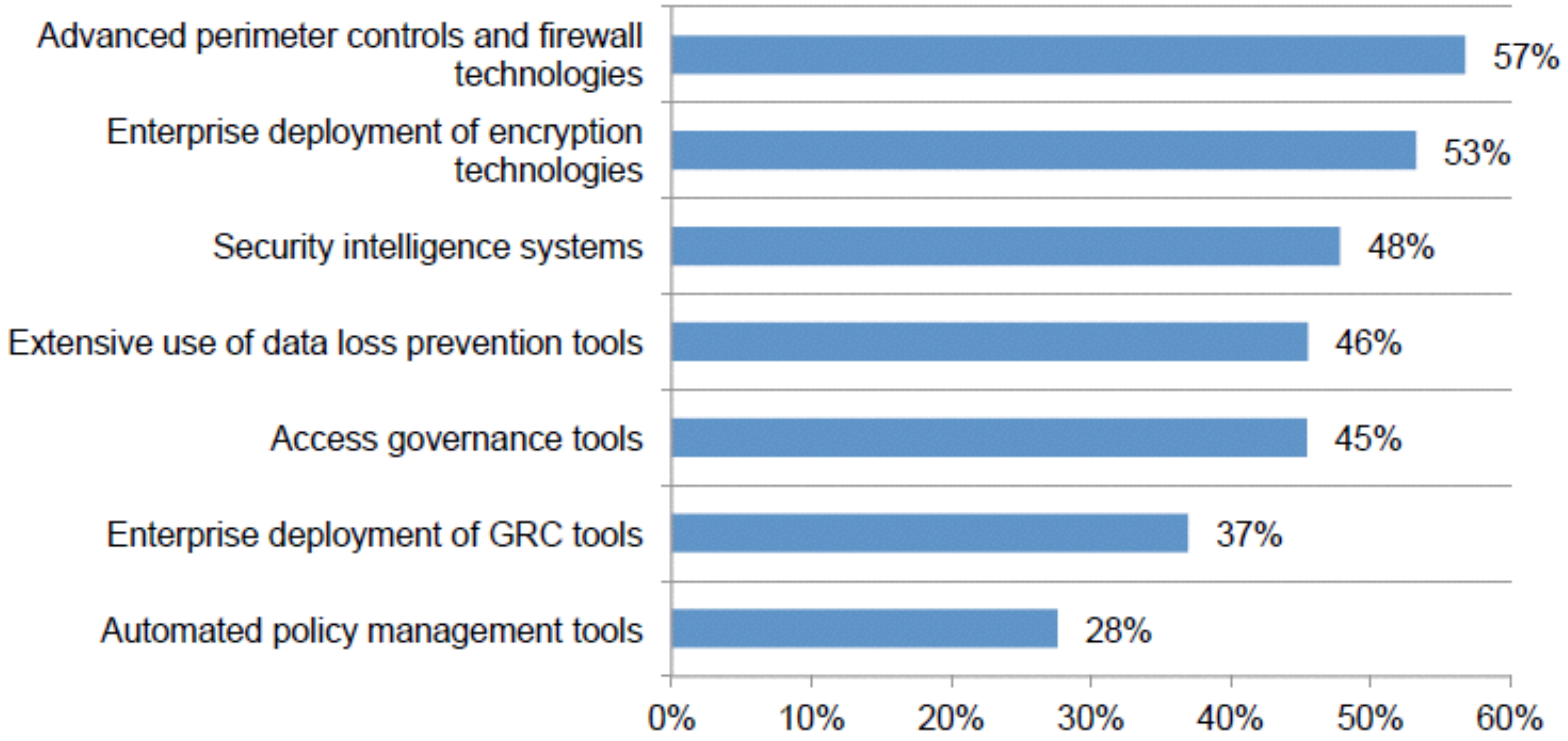


Figure 19. Seven enabling security technologies deployed
Consolidated view, n = 257 separate companies



Why IT security

- **Industry** is a prime target for cyber attack due to the advanced nature of the materials and technologies used, particularly defence related
- **Cyber attack** is rated as a top enterprise risk due to the catastrophic impact and likelihood
- **Minimum Security Standards are required from Internal Customers, External Customers, and Governments.**

- The main risks are internal - 70%

- Of these 70% are 30% deliberate actions and the rest are carelessness / lack of knowledge

How do we protect the information?

Firewall

Web filter

Encryption

Patch updates

MDM protection on mobile devises

External security tests

- Antivirus

2FA 2 Factor authorisation

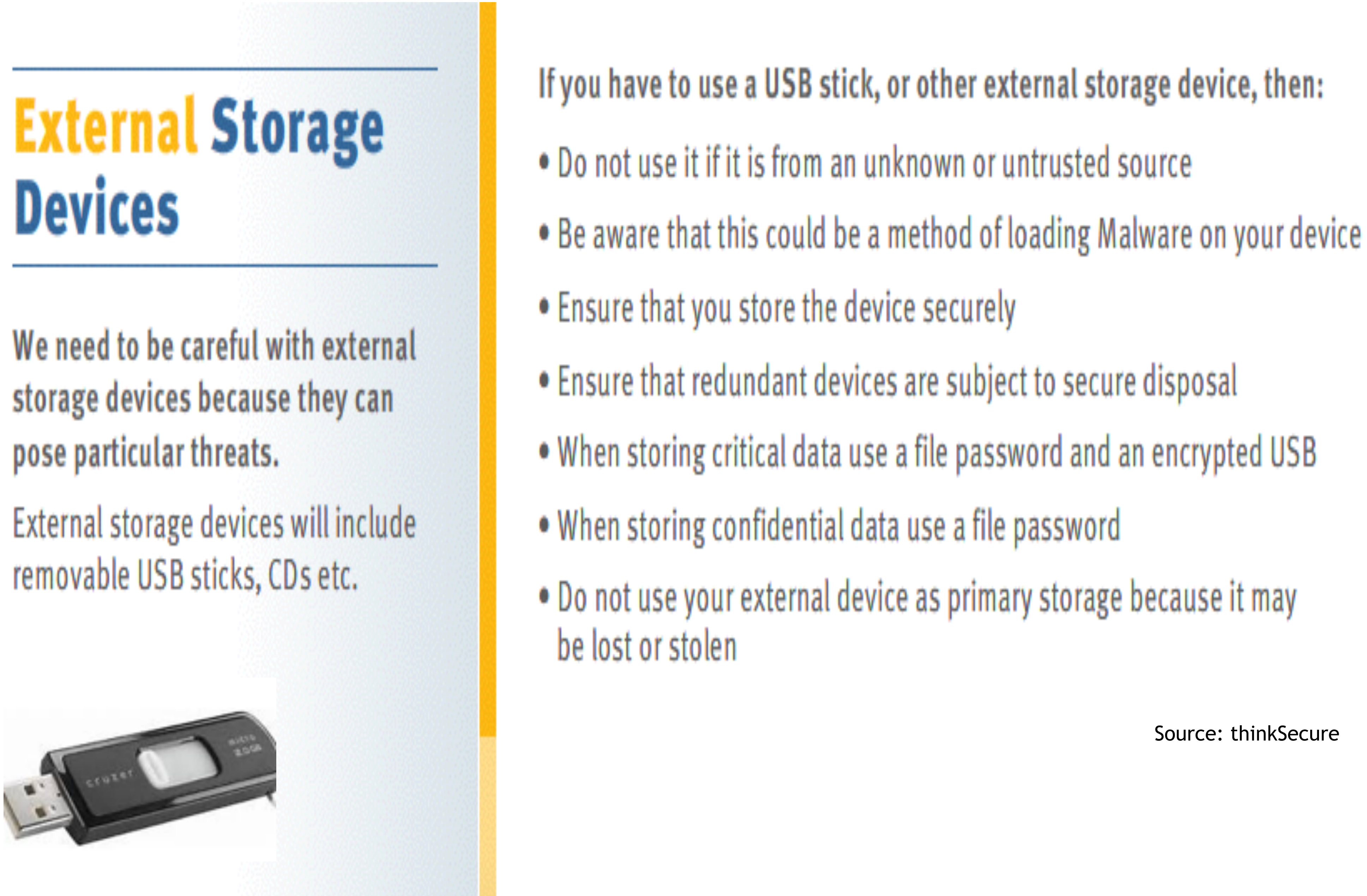
User awareness

Whose responsibility is it to protect information?

- Each individual employee is responsible for classified information he / she possesses not come to unauthorised people

- It is the responsibility of everyone to ensure authorisation of the person who may have access to the information.

Things to consider - External storage device



External Storage Devices

We need to be careful with external storage devices because they can pose particular threats.

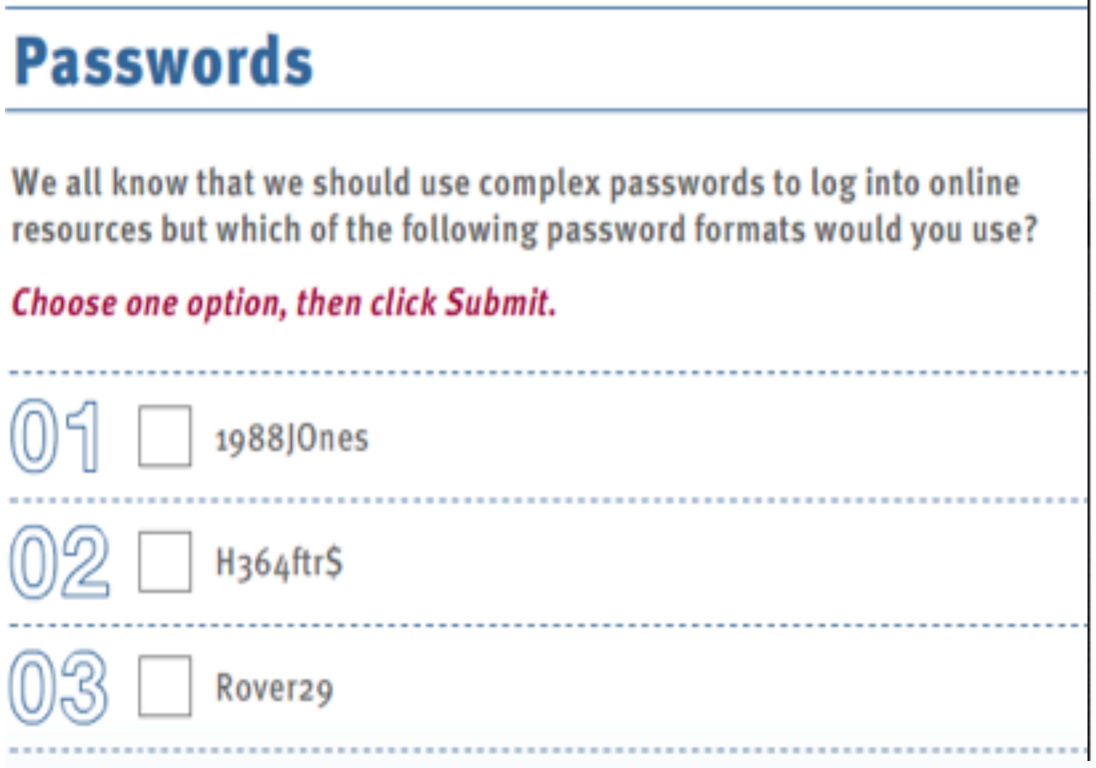
External storage devices will include removable USB sticks, CDs etc.

If you have to use a USB stick, or other external storage device, then:

- Do not use it if it is from an unknown or untrusted source
- Be aware that this could be a method of loading Malware on your device
- Ensure that you store the device securely
- Ensure that redundant devices are subject to secure disposal
- When storing critical data use a file password and an encrypted USB
- When storing confidential data use a file password
- Do not use your external device as primary storage because it may be lost or stolen

Source: thinkSecure

Things to consider - Password



Passwords

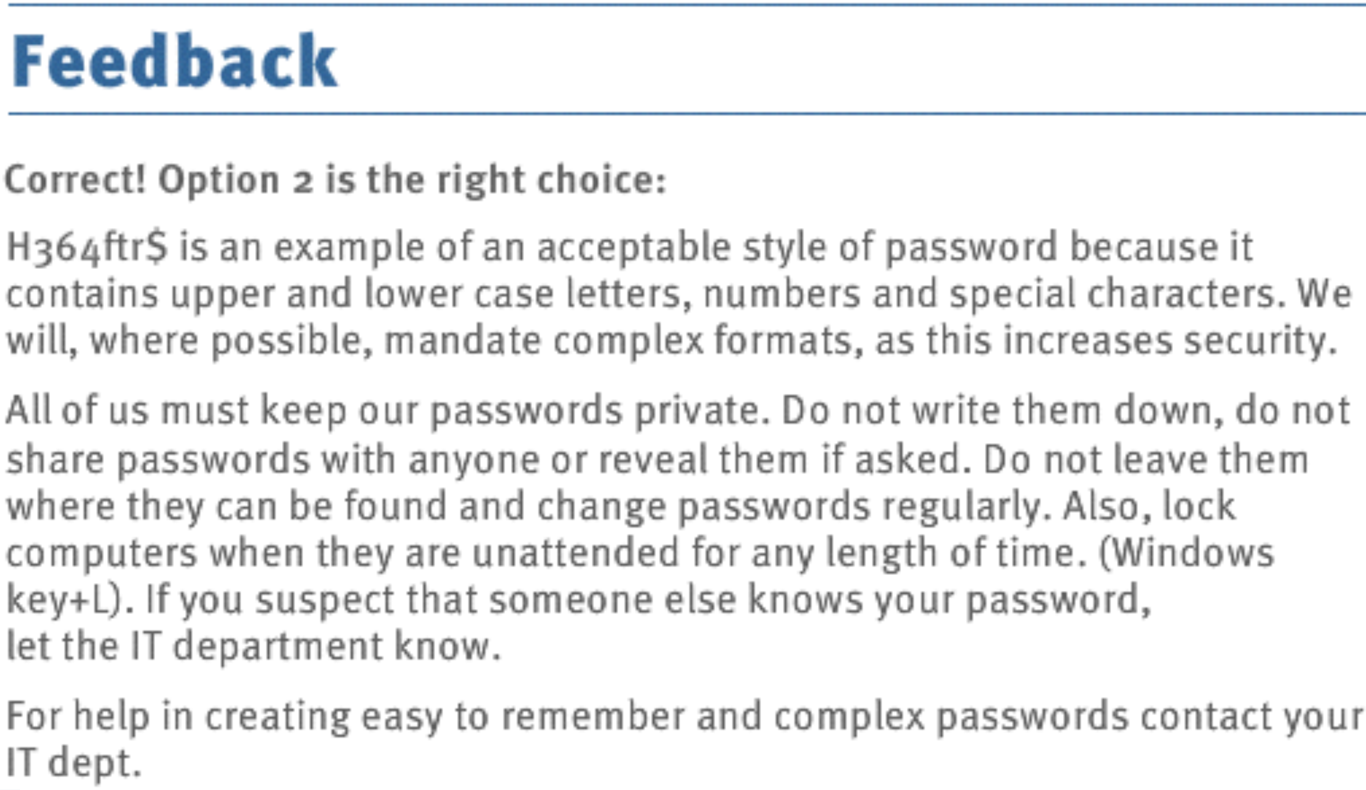
We all know that we should use complex passwords to log into online resources but which of the following password formats would you use?

Choose one option, then click Submit.

01 □ 1988JOnes

02 □ H364ftr$

03 □ Rover29



Feedback

Correct! Option 2 is the right choice:

H364ftr$ is an example of an acceptable style of password because it contains upper and lower case letters, numbers and special characters. We will, where possible, mandate complex formats, as this increases security.

All of us must keep our passwords private. Do not write them down, do not share passwords with anyone or reveal them if asked. Do not leave them where they can be found and change passwords regularly. Also, lock computers when they are unattended for any length of time. (Windows key+L). If you suspect that someone else knows your password, let the IT department know.

For help in creating easy to remember and complex passwords contact your IT dept.

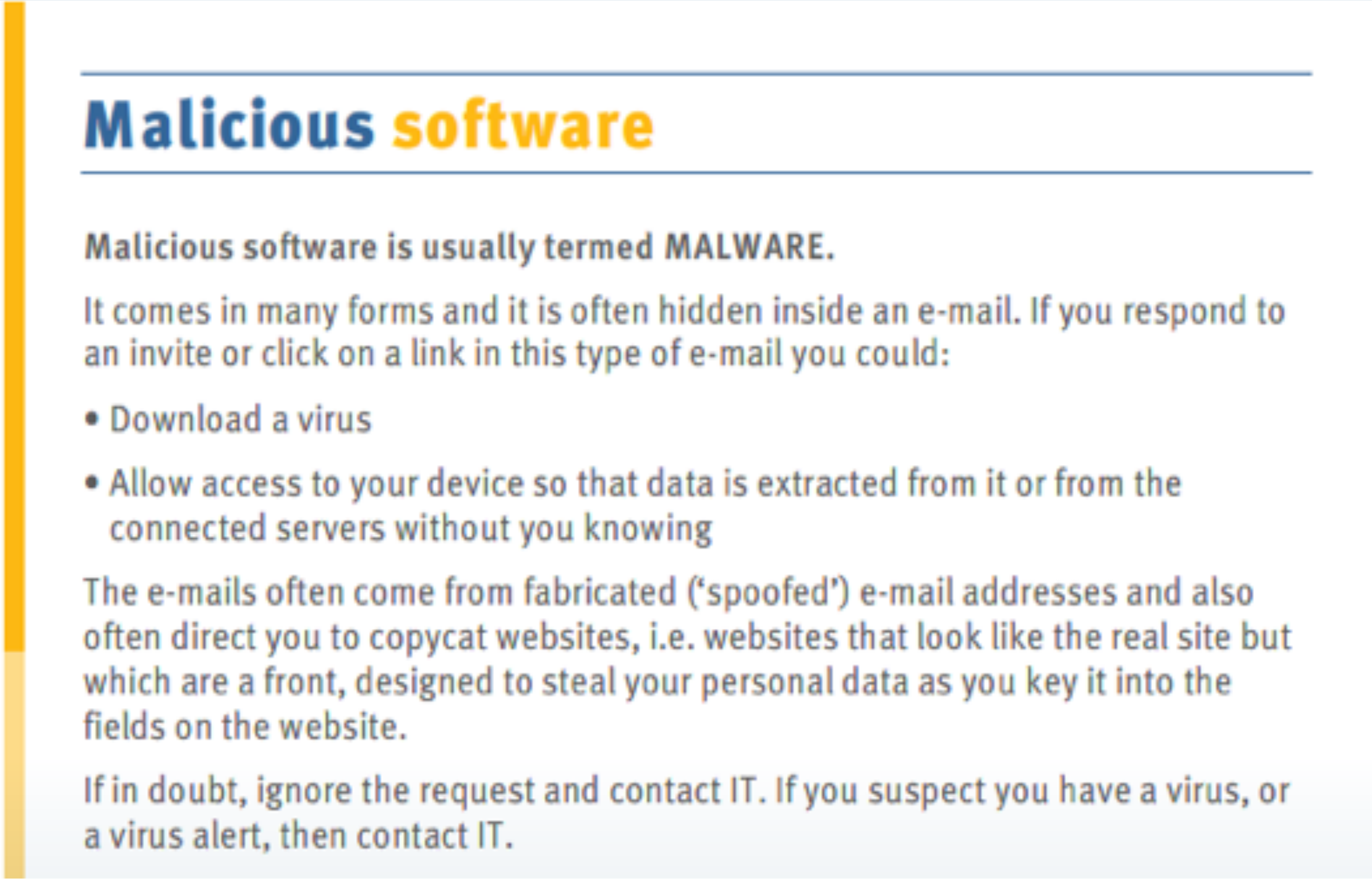
Source: thinkSecure

Mobile phone

- Lock your phone when not in use

- Business information must only be viewed when it is protected by a MDM tool
- The camera may be used only within an area if you have permission.
- It is not allowed to download apps that involve costs or cause security risks for the company

Things to consider - eMail



Malicious software

Malicious software is usually termed MALWARE.

It comes in many forms and it is often hidden inside an e-mail. If you respond to an invite or click on a link in this type of e-mail you could:

- Download a virus
- Allow access to your device so that data is extracted from it or from the connected servers without you knowing

The e-mails often come from fabricated ('spoofed') e-mail addresses and also often direct you to copycat websites, i.e. websites that look like the real site but which are a front, designed to steal your personal data as you key it into the fields on the website.

If in doubt, ignore the request and contact IT. If you suspect you have a virus, or a virus alert, then contact IT.

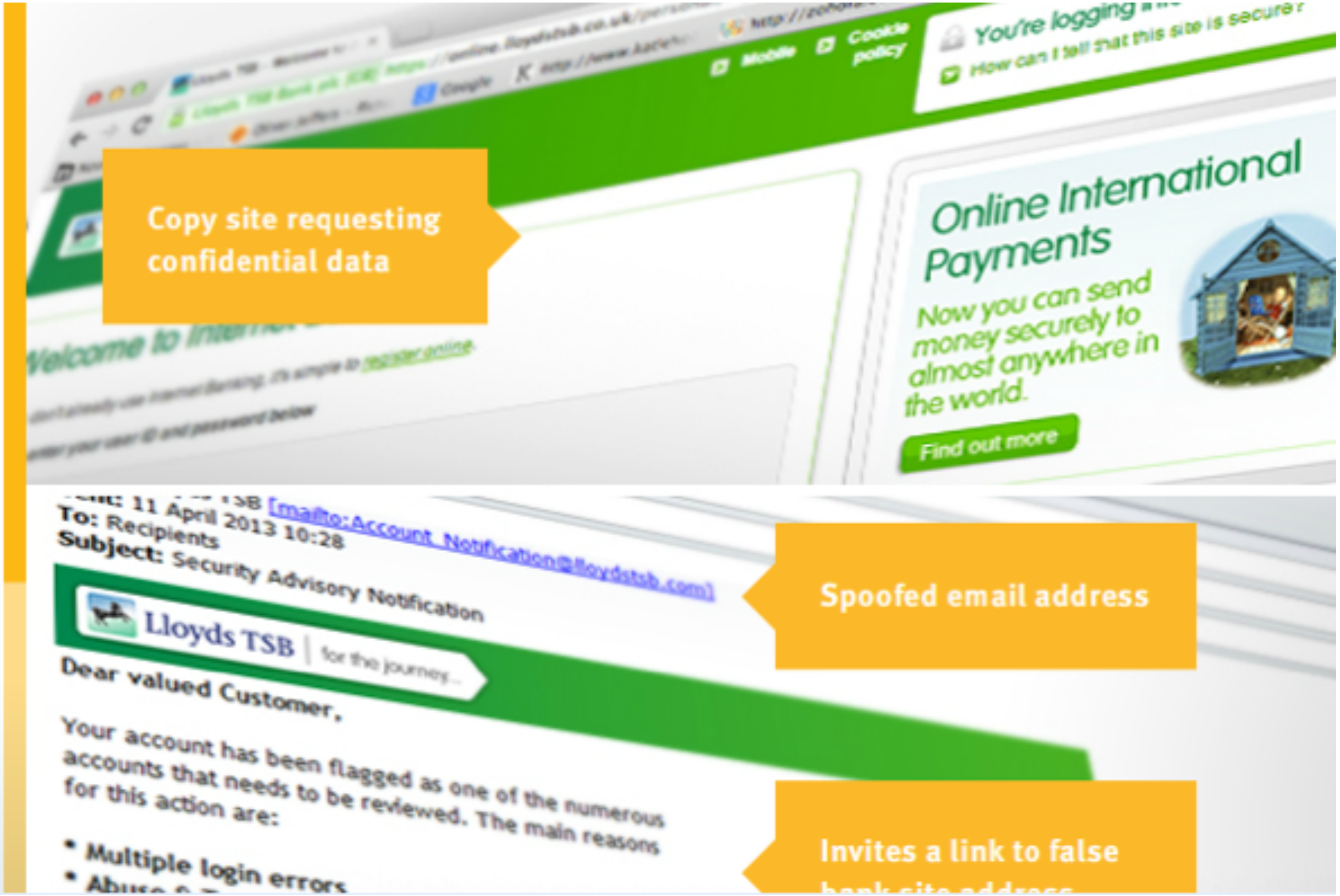
Source: thinkSecure

Phishing for facts

YOU RECEIVE AN E-MAIL THAT ASKS YOU TO VISIT YOUR INTERNET BANK. THE MALWARE HAS SPOOFED THE SENDER ADDRESS AND PROVIDES A GENUINE-LOOKING SITE AT THE LINK.

Always be cautious when invited to click on a link in an e-mail.

Response: Do not assume the e-mail is genuine. Do not respond to these requests. Notify your bank. Delete the email, or if in doubt, contact your local IT department.



Mobile
Cookie policy
You're logging
How can I tell that this site is secure?
Welcome to Internet
register online
Online International Payments
Now you can send money securely to almost anywhere in the world.
Find out more

Copy site requesting confidential data

TSB [mailto:Account_Notification@lloydstsb.com]
Sent: 11 April 2013 10:28
To: Recipients
Subject: Security Advisory Notification

Lloyds TSB | for the journey...

Dear valued Customer,

Your account has been flagged as one of the numerous accounts that needs to be reviewed. The main reasons for this action are:

- Multiple login errors
- Abuse

Spoofed email address

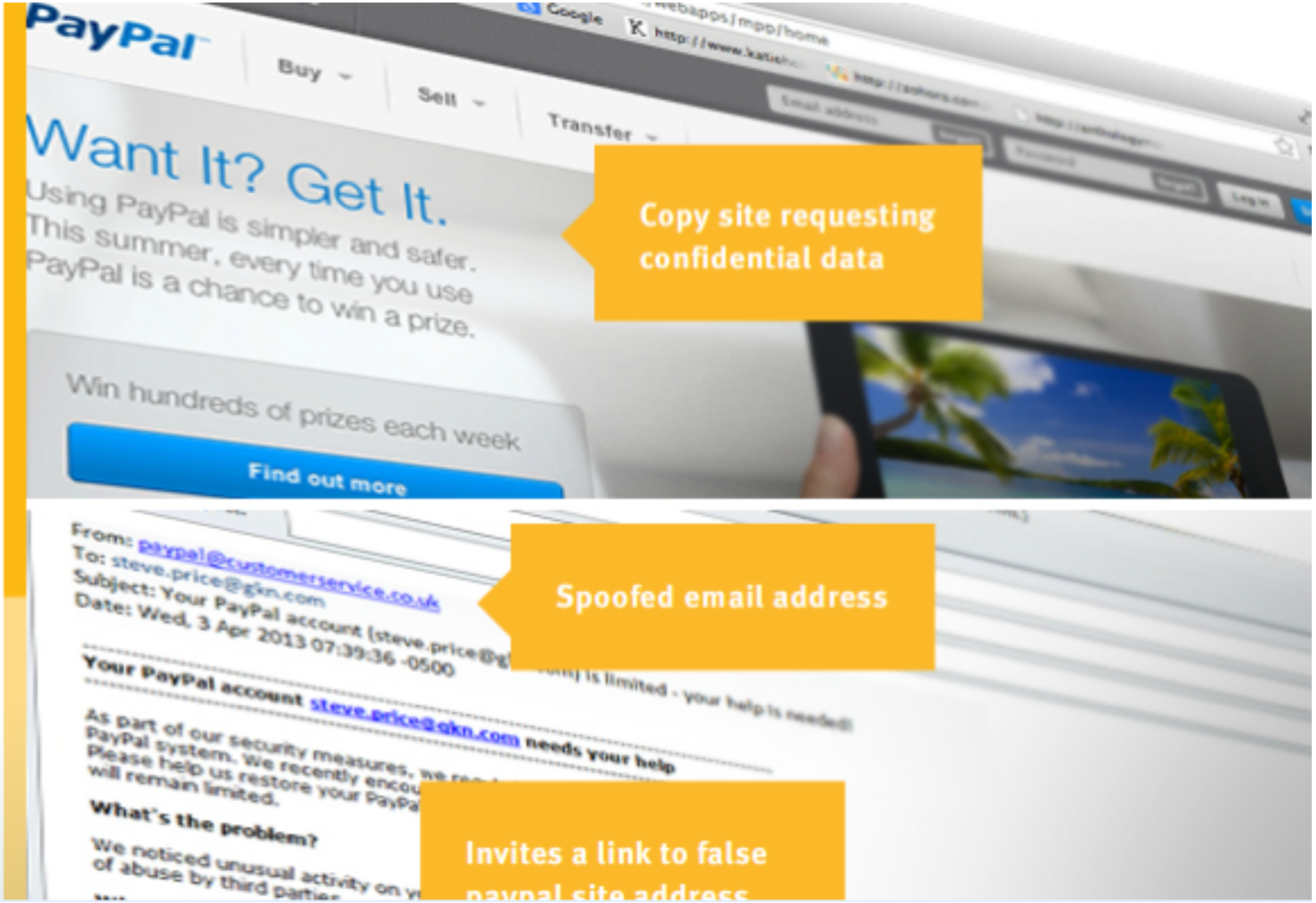
Invites a link to false bank site address

Donate here

YOU RECEIVE AN E-MAIL THAT ASKS YOU TO VISIT YOUR PAYPAL SITE. YOU LOG IN. THE MALWARE HAS EMULATED THE SENDER ADDRESS AND PROVIDES A GENUINE-LOOKING SITE AT THE LINK.

By logging in, you have given away your personal data. If you use the same data for all sites, the loss may be greater.

Response: Do not assume the e-mail is genuine. If it is unexpected, do not click on any links within the email, and delete it. If in doubt, contact your local IT department.



Want It? Get It.

Using PayPal is simpler and safer. This summer, every time you use PayPal is a chance to win a prize.

Win hundreds of prizes each week

Copy site requesting confidential data

From: paypal@customerservice.co.uk
To: steve.price@gkn.com
Subject: Your PayPal account (steve.price@g ... com) is limited - your help is needed!
Date: Wed, 3 Apr 2013 07:39:36 -0500

Your PayPal account steve.price@gkn.com needs your help

As part of our security measures, we re ...
PayPal system. We recently encou ...
Please help us restore your PayPa ...
will remain limited.

What's the problem?

We noticed unusual activity on y ...
of abuse by third parties

Spoofed email address

Invites a link to false paypal site address

Remember

Do not assume an email is genuine.

Be cautious when clicking on Internet links:

You are the target!!!

Ignore the request, delete the e-mail or if in doubt, contact your local IT department.

Things to consider - Social Media

- Be careful about what personal data you reveal on social medias as this information can become a security risk in the wrong hands.

Things to consider - On travel

- If you are working with your laptop on the plane, train or other public places, the computer should be equipped with a protective film on the screen.

- IT equipment must not be checked in it must be carried as hand luggage

High Risk countries

- Different types of threats depending on which country it is.

- High Risk countries have extremely large budgets for intelligence and IT espionage is a cost-effective way to conduct intelligence operations as it requires relatively few staff.