



Jamie Randall, CTO, IASME Consortium

Cyber security, data governance and risk

Visit www.iasme.co.uk or call 03300 882 752



IASME Consortium



We are an
accreditation
body for
Cyber Essentials



We own the
IASME
governance
standard



We have 100 certification
bodies and have certified
over 4,500 companies to
Cyber Essentials



- Why is cyber security important?
- What could happen to your organisation?
- What should I do now?



Why is cyber security important?



Why is cyber security important?





Cyber security is about protecting data

Financial
information

Customer
records

Search
History

Personal
information

Confidential
plans

Intellectual
property

Sensitive
personal data



Protect data from motivated people



Hacktivists

“Change the world”

- Examples are:
Anonymous
Syrian Electronic Army



Hackers

Status and technical challenge

- Can be good or bad depending on their actions



Insiders

Privileged access to data

- Can be malicious or, more commonly, accidental



State sponsored

National advantage

- Well funded and targeted
- Gather information



Criminals

Often driven by financial gain

- Theft of data
- Ransomware



How might an attack happen?



Malware



**Social
Engineering**



Vulnerabilities



Cryptolocker Ransomware

Cryptolocker 2.0

Your personal files are encrypted



**Your files will be lost
without payment on:**

11/24/2013 3:16:34 PM

[See files](#)

Info

Your **important files were encrypted** on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key **RSA-4096** generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

[<< Back](#) [Proceed to payment >>](#)



Wannacry Ransomware





How might an attack happen?



Malware



**Social
Engineering**



Vulnerabilities



Social Engineering

From: ☐ Sue Brown
To: ☐ Sue Brown
Cc:
Subject: Please get back to me asap.

Robert

Please do you have a moment? Am tied up in a meeting and there is something I need you to take care of.

We have a pending invoice from our Vendor. I have asked them to email me a copy of the invoice. I will be highly appreciative if you can handle it before the close of banking transactions for today. I can't take calls now so an email will be fine.

Sue



Social Engineering

Your account might be compromised



Spam x



Barclays <corporate.communications@barclays.com>

to

09:25 (1 hour ago)



Be careful with this message. Similar messages have been used to steal people's personal information. Unless you trust the sender, don't click on links or reply with personal information. [Learn more](#)

Dear Customer,

We recently have determined that different computers have logged in your Barclays account, and multiple password failures were present before the logons.

For your security we have temporary suspended your account.
Please download the document attached to this email and fill carefully.

If you do not restore your account by September 22, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes.

Do not ignore this message is for your security.

We apologize for any inconvenience.

Yours sincerely,
The Barclays Team.

Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered.



**22.09.2015 - Document
attached.zip**

5.1 KB





Social Engineering Victims by sector

Source: Verizon Data Breach report 2017

Industry Phishing

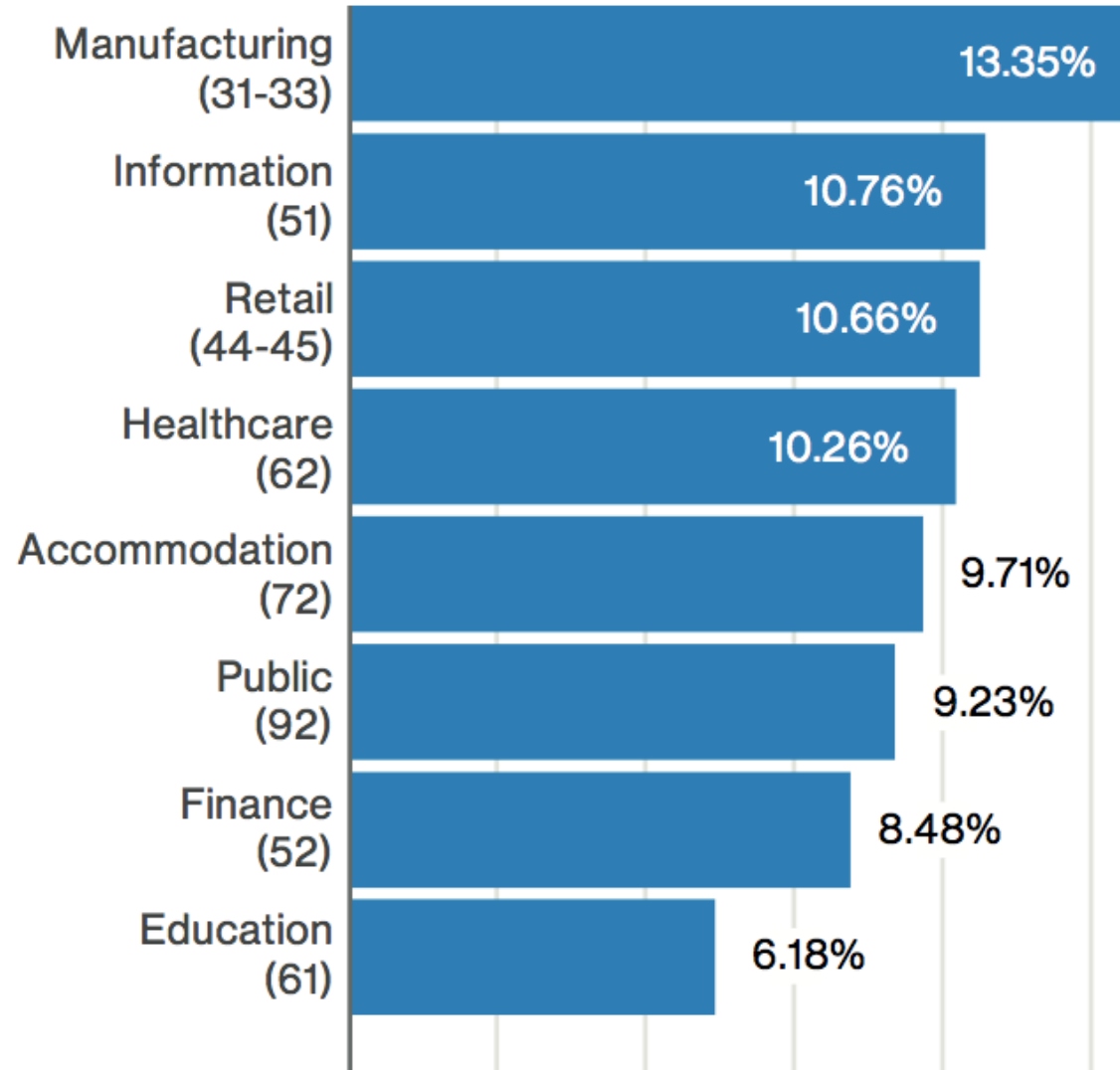


Figure 12: Median click rate per campaign by industry (n=7,153)



How might an attack happen?



Malware



**Social
Engineering**



Vulnerabilities



الصفحة الرئيسية نبذة عن الهيئة مناطق التنمية شروط تخصيص الأراضي الدراسات البيئية دهشور اتصل بنا English



T
D
A

الهيئة العامة للتنمية السياحية

موقع جديس



أحدث أخبار الهيئة

- * ضوابط و اشتراطات فنية
- * طلب مدنى للإستثمار فى مشروع سياحى
- * تحقيق إيرادات غير مسبوقة عن العام المالى 2015 / 2016
- * صرح إستثمارات فى حدود 2,5 مليار جم
- * استرداد 90 مليون و 500 ألف متراً مربعاً



Owned by Ymh

حیرتمنا مش عارفین نوقف مع مين؟؟

مع السیسی ولا مع الاخوان

سیبکم من السیاسه وفرقشوا شویه مع

شای ام حسن (رمز الثورة المضادة) هههههههه



EU General Data Protection Regulation (GDPR)

- All companies are required to keep track of personal data and ensure good policy and procedures in place to protect it
- Must report data breach incidents quickly
- ICO require adequate cyber security measures – these are likely to go beyond the very basics
- Significant potential fines (4% global turnover) if have not taken steps to assess risk to information and put measures in place
- Affects both EU/UK and international companies



EU Network and Information Security (NIS) Directive

- Covers operators of essential services and online services providers such as cloud service providers, online marketplaces, and search engines
- Top level requirements:
 - Managing security risk
 - Protecting against cyber attack
 - Detecting cyber security events
 - Minimising the impact of cyber security incidents



What could happen to your organisation?



Potential cost of a cyber incidents

- Ransomware incident
 - £400 Ransom
 - Over £50,000 IT forensics
- Malware incident
 - £150,000 wire transfer
 - IT forensics costs
- CEO Fraud incident
 - £50,000 wire transfer
- Phone system hacking incident
 - Over £20,000 phone bill



What should I do now?



What should I do now?





What should I do now?

- **Understand your data**

- Review your business processes and systems
- Where is your data?
- How sensitive is the data you hold?
- Who owns it?
- Why do you hold it?
- Important for GDPR





What should I do now?



- **Understand your risks**

- What could happen to your data?
- Look at cyber issues faced by similar companies
- Speak to your peers – which cyber events have they had?
- Form a working group
- Make a list of the potential events and consider how likely they are to happen
- What would be the impact? Financial, regulatory, perception



What should I do now?



- **Reduce your risks**

- What will reduce the chance of the biggest risks occurring?
- Get advice from information security professional
- Comply with an appropriate standard – Cyber Essentials, IASME, ISO 27001
- Learn how to respond to incidents (make plans now)
- Cyber insurance
- Train staff



Standards



**IASME Governance
Standard**
Information Assurance



ISO 27001
Information Assurance



Cyber Essentials Scheme
Fundamental Cyber Security



Cyber Essentials



Access Control



Updating
Software



Secure
Configuration



Malware
Protection



Firewalls



What should I do now?

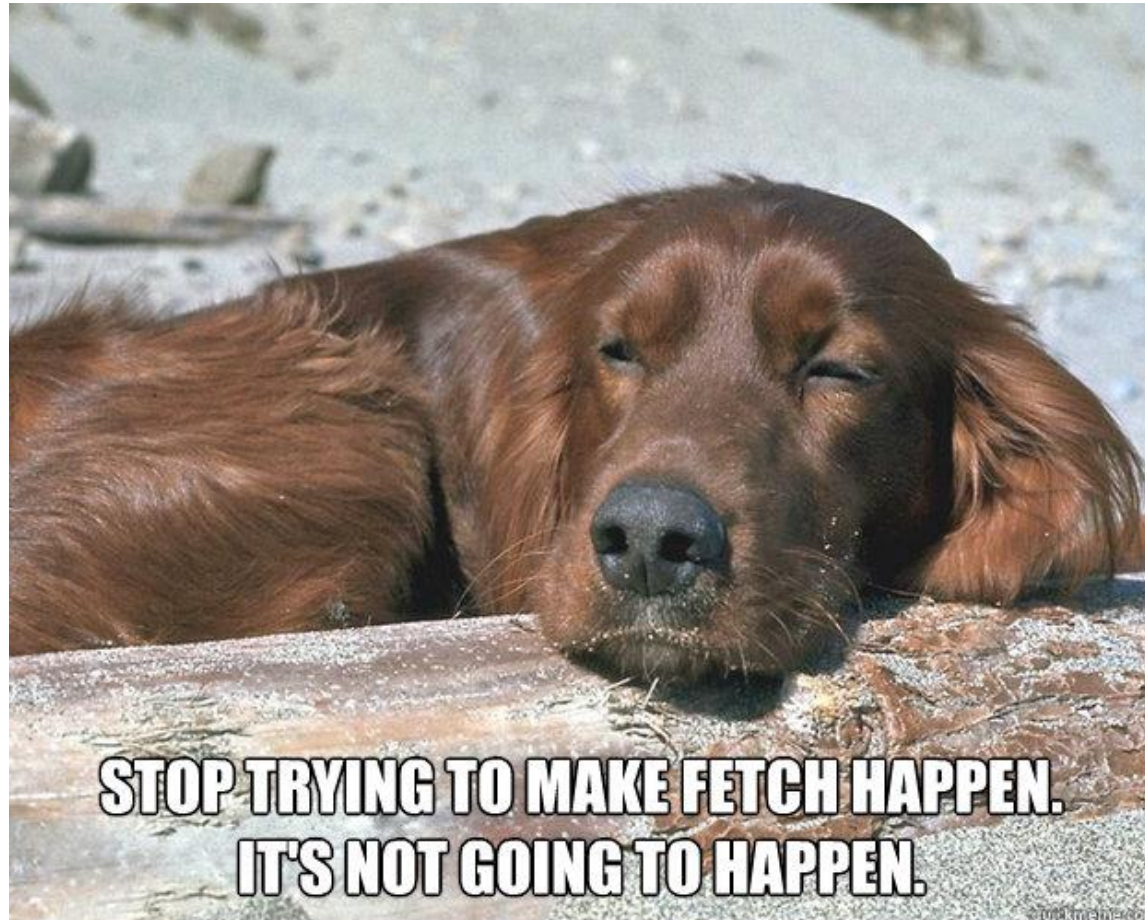


- **Reduce your risks**

- What will reduce the chance of the biggest risks occurring?
- Get advice from information security professional
- Comply with an appropriate standard – Cyber Essentials, IASME, ISO 27001
- Learn how to respond to incidents (make plans now)
- Cyber insurance
- Train staff



Isn't there an easier option?





Isn't there an easier option?

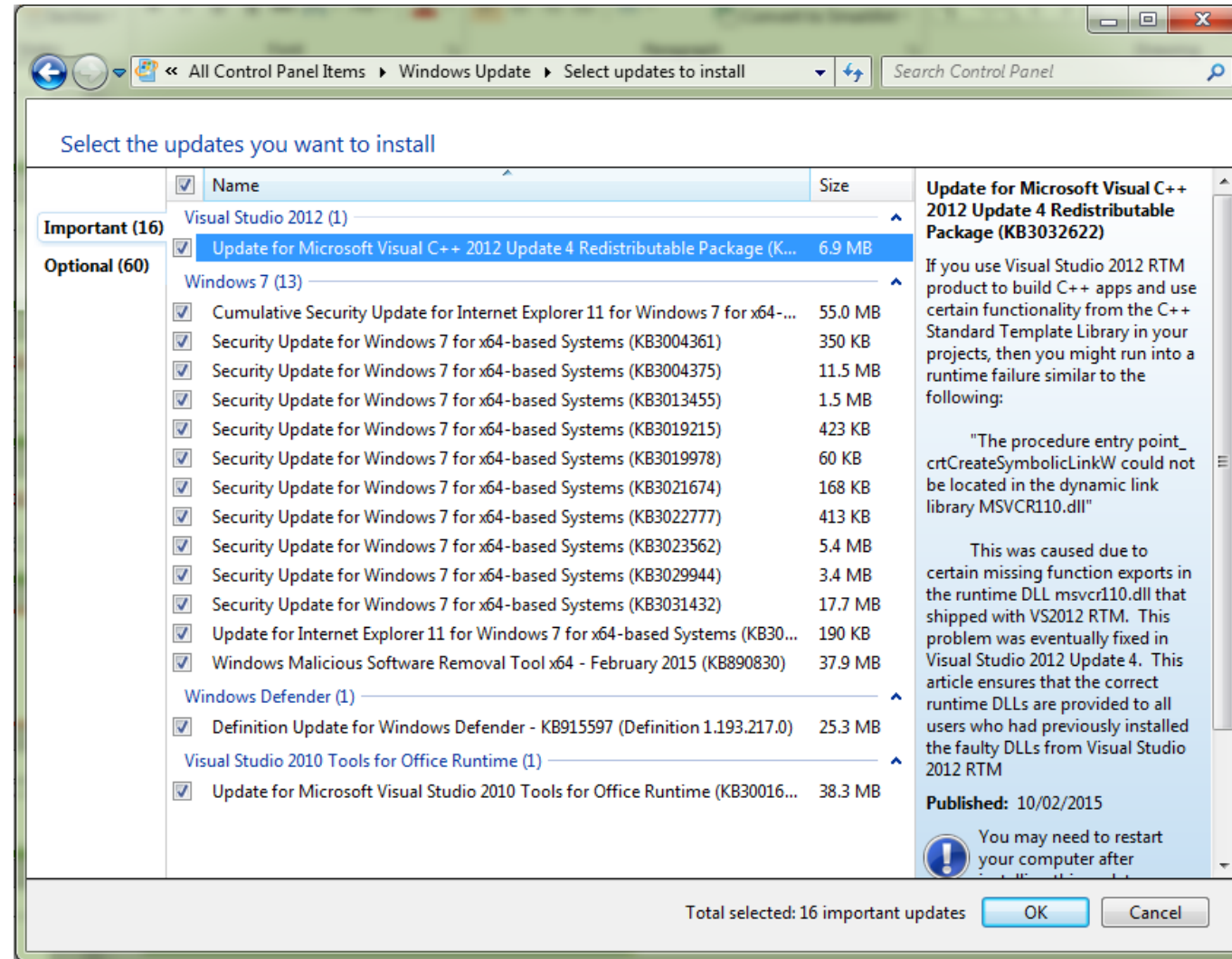


- Manually update all your software on your devices – macOS, Windows, Microsoft Office, PDF Reader, Flash, Google Chrome, accounting software
- AND set all your software to auto-update



Windows Update

Provides patches and updates for Windows and Microsoft products





macOS updates

Accessed via
App Store





Android System Update

Provides patches and updates for Android-based mobile phones and tablets

4:52

Android 7.0

This software update will upgrade your Nexus 5X to Android 7.0 Nougat. Multitask with ease with multi-window, bring your words to life with all-new emoji, and enjoy longer-lasting battery. Learn more at android.com/nougat. This update includes the 2016-08 security patches. Future security updates may be downloaded and installed automatically, possibly using cellular data. Downloading updates over a cellular network or while roaming may cause additional charges.

Requires a restart

Update size: 1171.5 MB

DOWNLOAD

5:29

Android 7.0
Downloading...

This software update will upgrade your Nexus 5X to Android 7.0 Nougat. Multitask with ease with multi-window, bring your words to life with all-new emoji, and enjoy longer-lasting battery. Learn more at android.com/nougat. This update includes the 2016-08 security patches. Future security updates may be downloaded and installed automatically, possibly using cellular data. Downloading updates over a cellular network or while roaming may cause additional charges.

Update size: 1171.5 MB



iPhones / iPad Updates

Provides patches
and updates for
Apple iPhones
and iPads.





Isn't there an easier option?

2

- Don't use administrator accounts for web browsing and email ... ever
- This includes your IT people!
- Use standard user accounts day-to-day



Isn't there an easier option?



- Enable two-factor for all your cloud services (ie Google Apps, Microsoft Office 365, DropBox etc)



Isn't there an easier option?

4

- Empower your staff to delete suspicious or odd emails
- Show them examples of phishing emails
- Make sure there are no negative consequences of staff accidentally delete a “real” email



Isn't there an easier option?



- Backup your most important data somewhere off-site encrypted and keep it safe
- Do it today!



Sources of advice

- National Cyber Security Centre
- Cyber Aware
- Get Safe Online
- Information security consultancies
- Managed service IT providers



Get Safe Online
Free expert advice



IASME Consortium[®]

Thank you

jamie.randall@iasme.co.uk

Visit www.iasme.co.uk or call 03300 882 752