Dr. Phil Legg

Associate Professor in Cyber Security

Information Risk Management

08: Law and Regulation

Date

UWE Bristol | University of the West of England

Today

- Legal and Regulatory issues in Information Risk Management

Computer Misuse Act 1990

A person is guilty of an offence if:

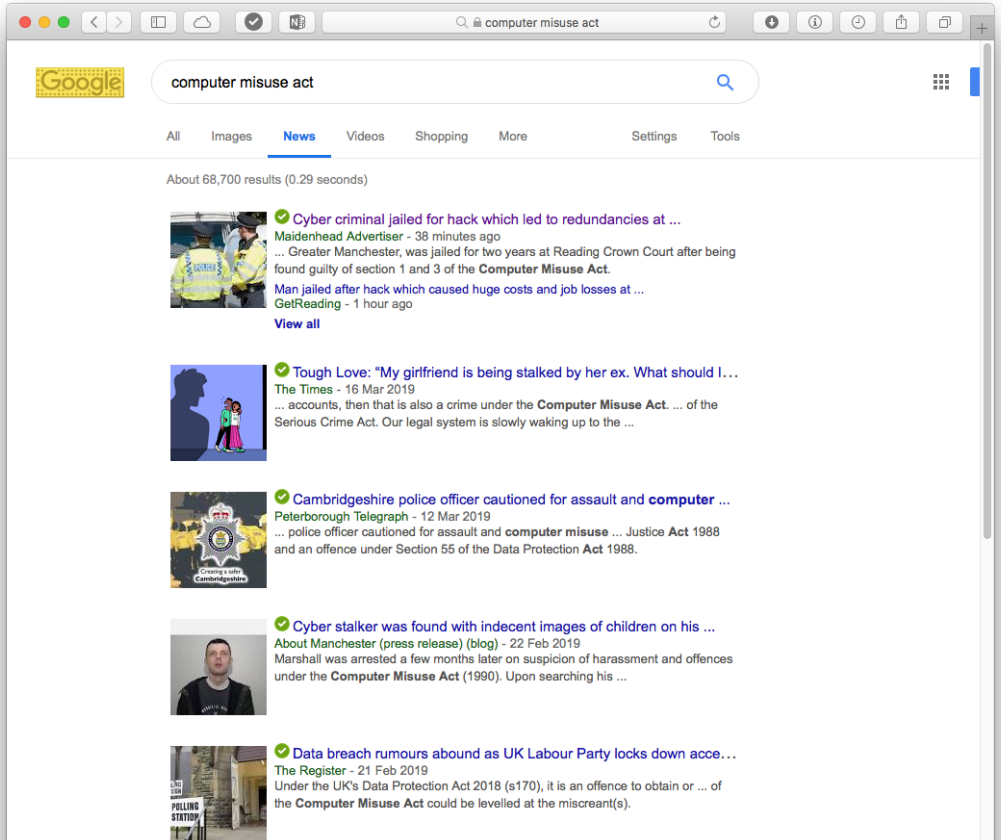
a) He causes a computer to perform any function with intent to secure access to any program or data held in any computer*, or to enable any such access to be secured*.

b) The access he intends to secure*, or to enable to be secured,* is unauthorized; and

c) He knows at the time when he causes the computer to perform the function that that is the case.

http://www.legislation.gov.uk/ukpga/1990/18/contents

Computer Misuse Act 1990



UWE Bristol | University of the West of England

Computer Misuse Act 1990

Suspected teen hacker fac

www.computerweekly.com/news/2240104869/Suspected-teen-hacker-faces-fiv

Home > Topics > IT security > IT risk management > Suspected teen hacker faces five charges under the Computer Misuse Act

NEWS

Suspected teen hacker faces five charges under the Computer Misuse Act

Warwick Ashford
Thursday 23 June 2011 05:00

Share 0 Tweet 0

Essex teen Ryan Cleary, who was arrested in connection with cyber attacks claimed to have been carried out by hacker group LulzSec, is facing five charges under the Computer Misuse Act 1990.

The charges are in connection with three attacks on targets based in the UK, but police are investigating the 19 year-old's connections to other attacks by LulzSec, which is believed to have targeted websites including those of the US Central Intelligence Agency, the US Senate and electronics giant Sony.

The charges relate specifically to Cleary's alleged involvement in a distributed denial of service (DDoS) attack on the UK Serious Organised Crime Agency (Soca) on 20 June, an attack on the website of the International Federation of the Phonographic Industry in November 2010, and an attack on the British Phonographic Industry's website in October, according to the BBC.

The charges against Cleary include conspiring with others on or before 20 June to construct a botnet of hijacked computers to conduct DDoS attacks, and making, adapting, supplying or offering to supply a botnet,

UK man arrested in connec

m.bbc.co.uk/news/technolog...

NEWS Sections

Technology

UK man arrested in connection with Sony and Xbox hack

16 January 2015 | Technology

The group behind the attack uses a lizard wearing a monocle and smoking a pipe as its identifying logo

Dozens arrested in cyberc

m.bbc.co.uk/news/technolog...

BBC News Sport More

NEWS Sections

Technology

Dozens arrested in cybercrime 'strike week'

3 hours ago | Technology

One raid led to the arrest of a man thought to be involved with an attack on Yahoo in 2012

Data Protection Act

- Data Protection Act: 2018 (previously 1998)
  - http://www.legislation.gov.uk/ukpga/2018/12/contents
    - Incorporates General Data Protection Regulation
  - http://www.legislation.gov.uk/ukpga/1998/29/contents

Data Protection Act

- Personal data shall be:
  - processed fairly and lawfully, and obtained only for the specified purpose.
  - adequate, relevant and not excessive.
  - accurate, and where necessary, kept up to date
  - kept only as long as is required for its purpose.
- Individuals can:
  - View the data that an organisation holds on them.
  - Request that incorrect information be corrected, which if ignored, court order can have data corrected or destroyed.

Data Protection Act

Police checks on partners

m.bbc.co.uk/news/uk-wales-21451611

Police checks on partners broke data laws

By Alun Jones
BBC Newyddion Ar-lein

14 February 2013 | Wales

Police officers and staff in Wales have broken the Data Protection Act 62 times in the past two years.

Four police workers were sacked and 14 resigned as a result of the breaches

Four people were sacked and 14 resigned as a result of the breaches.

They were caught carrying out the breaches for non-policing purposes, BBC Wales has discovered under the Freedom of Information Act.

They included checks on partners, relatives and associates, altering their own records, and passing data to third parties.

A spokesperson for the Information Commissioner's Office, which is responsible for the enforcement of the Data Protection Act 1998, said officers and civilian staff had access to "highly sensitive personal information".

"It is important that they do not abuse this access and only use the information for their policing duties," the spokesperson added.

Top Stories

Outcry as IS 'wrecks' Assyrian site
Archaeologists and officials express outrage about the reported bulldozing of the ancient Assyrian city of Nimrud in Iraq by Islamic State (IS) militants.
31 minutes ago

Pair jailed for Ayesha Ali killing
18 minutes ago

Migrant population 'up 565,000'
4 minutes ago

Features

Special delivery
The man who posted himself to the other side of the world

M&S breached Data Protec

www.computing.co.uk/ctg/news/...

M&S breached Data Protection Act

25 Jan 2008
6 Comments

The personal details of 26,000 Marks and Spencer's employees were stolen last May

Marks and Spencer has breached the Data Protection Act in not encrypting employee data held on a laptop, according to the Information Commissioner's Office (ICO).

The system contained pension details for 26,000 employees and was stolen from the home of a contractor.

Further reading

- M&S online sales brighten Christmas gloom
- M&S signs £19m Computacenter deal
- M&S employee details at risk

Protecting such information is crucial, according to ICO assistant commissioner Mick Gorrill.

"It is essential that before a company allows personal information to leave its premises on a laptop there are adequate security procedures in place to protect personal information such as password protection and encryption," he said.

The ICO has issued Marks and Spencer with an enforcement notice ordering the company to ensure all laptop hard drives are fully encrypted by April.

Failure to comply is a criminal offence and can result in further action against the company.

General Data Protection Regulation

- A major change to how EU organisations (including UK) should manage data – agreed in 2016, with 2 year period to comply (25th May 2018).
- Some key points:
  - **Increased Territorial Scope** – *it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location*
  - **Penalties** – *4% of annual global turnover or €20M (whichever is greater) for most serious infringements.*
  - **Consent** – *companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form*
  - **Breach notification** - *to notify users within 72 hours of discovery*
  - **Privacy by design** - *the inclusion of data protection from the onset of the designing of systems, rather than an addition*

https://www.eugdpr.org/key-changes.html

General Data Protection Regulation

- Key data subject rights
  - **Right to access** - *whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.*
  - **Right to be forgotten** - *entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data*
  - **Right for data portability** - *the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format'*
  - **Rights in relation to automated decision making**

https://www.eugdpr.org/key-changes.html

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

https://gdpr-info.eu/art-22-gdpr/

Data Protection Impact Assessment

- The GDPR mandates a DPIA be conducted where data processing "is likely to result in a high risk to the rights and freedoms of natural persons". The three primary conditions identified in the GDPR are:

  - A systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.
  - Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences.
  - Systematic monitoring of a publicly accessible area on a large scale.

https://www.itgovernance.co.uk/data-protection-impact-assessment-dpia

Acts and Regulations

- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 1998
- Privacy and Electronic Communications Regulations 2003-2011
- Copyright, Designs and Patents Act 1988
- Malicious Communications Act 1988
- Human Rights Act 1998
- Equality Act 2010
- Terrorism Act 2006
- Official Secrets Act 1989
- Limitation Act 1980
- Digital Economy Act 2010
- Police and Justice Act 2006

Intellectual Property Rights

- IP is a mechanism designed to protect our creative ideas – may be arts, written, musical.
  - Extends to algorithms and software.

- IP includes copyright, patents, industrial design rights, and trademarks.

Intellectual Property Rights

- Patents
  - Granted by government to an inventor, giving rights to exclude others from making, using, selling, offering to sell, and importing an invention for a limited period of time, in exchange for the public disclosure of the invention. An invention is a solution to a specific technological problem, which may be a product or a process.

Intellectual Property Rights

- Copyright
  - A copyright gives the creator of an original work exclusive rights to it, usually for a limited time. Copyright may apply to a wide range of creative, intellectual, or artistic forms, or "works". Copyright does not cover ideas and information themselves, only the form or manner in which they are expressed.

Intellectual Property Rights

- Industrial design rights
  - An industrial design right protects the visual design of objects that are not purely utilitarian. An industrial design consists of the creation of a shape, configuration or composition of pattern or colour, or combination of pattern and colour in three-dimensional form containing aesthetic value. An industrial design can be a two- or three-dimensional pattern used to produce a product, industrial commodity or handicraft.

Intellectual Property Rights

- Trademarks
  - A trademark is a recognizable sign, design or expression which distinguishes products or services of a particular trader from the similar products or services of other traders.

Copyright Law

- Copyright, Designs and Patents Act 1988
- Federation Against Software Theft (FAST) 1984
  - Prevention of software piracy

- https://www.gov.uk/intellectual-property/law-practice

End User License Agreements

- EULA

- Used for proprietary (closed-source) software.
- Contract between licensor and the purchases, establishing the purchaser's rights to use the software.
  - Typically will state that the software can not be copied, modified, or redistributed by the purchaser.
  - May also state how personal data will be used by the software.

Open Source Software Licensing

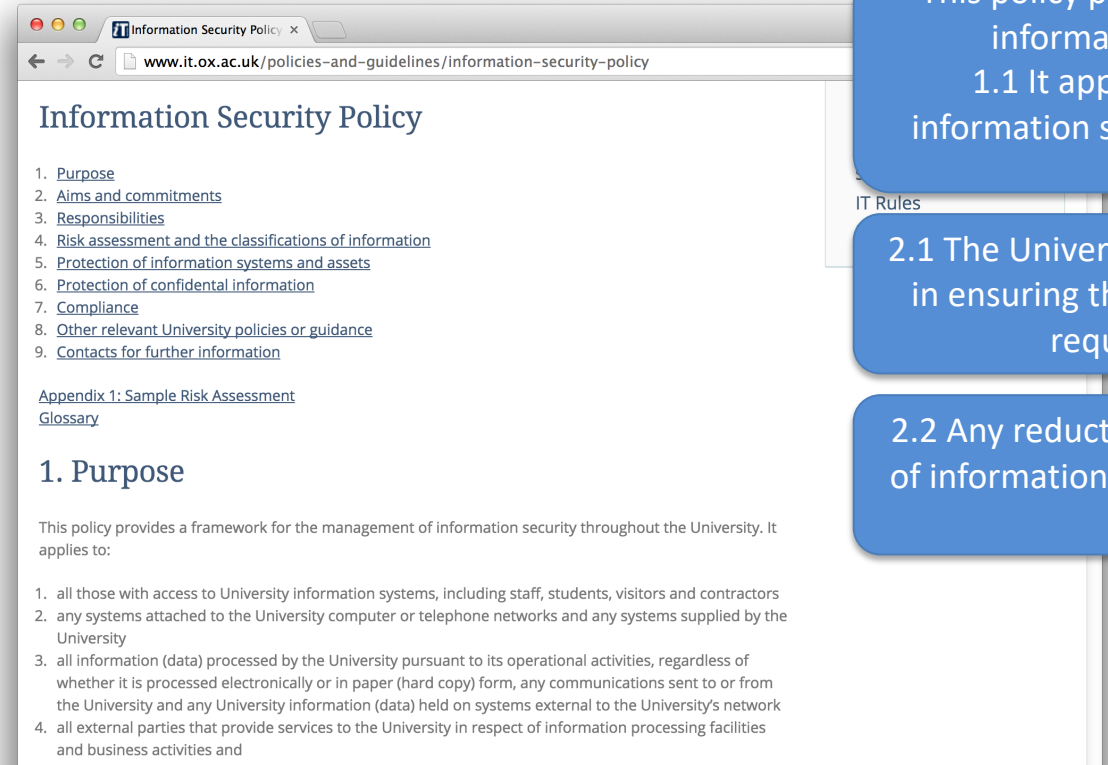
- GPL – GNU General Public License
  - Most widely used free software license.
  - End-user can study, share and modify software.
  - ***Copyleft*** – same rights must be offered for future use.

- LGPL – GNU Lesser General Public License
  - Same as GPL, but is not copyleft.
  - Means code library could be used in another project, and would not require an open-source license (i.e. proprietary).

Information Security Policy

- Documentation of how an organisation will address information security.
  - Should be suitable for employees, stakeholders, contractors, customers.
- Policy should be in line with legislation, and with the business objectives.
- Policy should explain how information (data) will be utilized, stored, managed, and secured.
- Ensures confidentiality, integrity, availability of data.

Information Security Policy



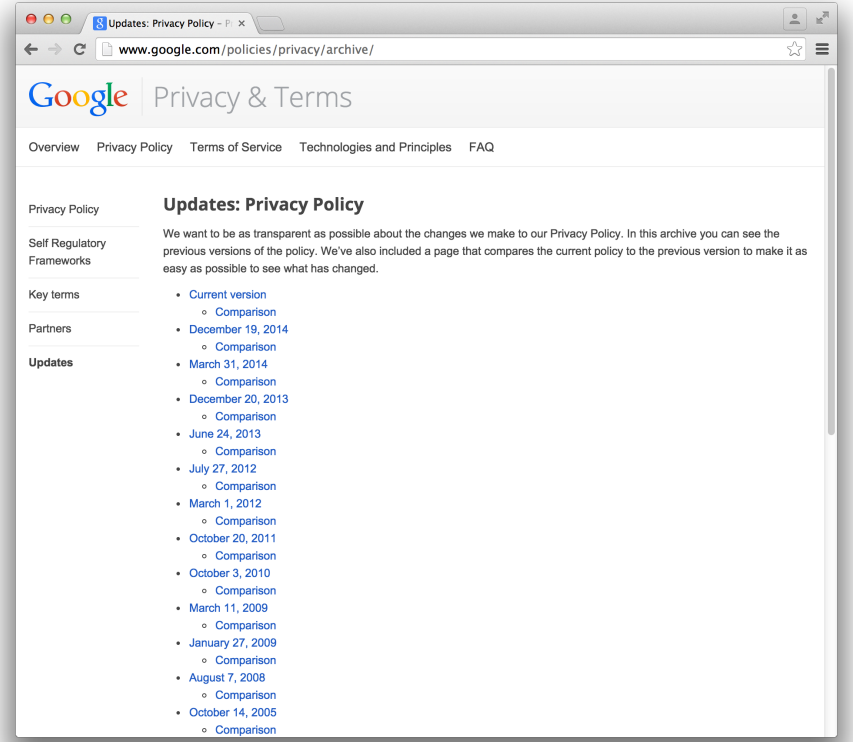
This policy provides a framework for the management of information security throughout the University.
1.1 It applies to all those with access to University information systems, including staff, students, visitors and contractors.

2.1 The University recognizes the role of information security in ensuring that users have access to the information they require in order to carry out their work.

2.2 Any reduction in the confidentiality, integrity or available of information could prevent the University from functioning effectively and efficiently.

Privacy Policy

- Google maintain archive of previous policies, and comparisons.
- Earliest: June 9th 1999
- 17 versions to date (as of February 25th 2015)
- Changes reflect how their business has evolved, and how they use personal data.
- http://www.google.com/policies/privacy/archive/



UWE Bristol | University of the West of England

Privacy Policy

- Examine the different policies and the comparisons.
- Examine the Google Timeline https://www.google.co.uk/about/company/timeline/
  - E.g. Gmail 2004, Google Maps 2005, Youtube 2006, Android 2007)
- Consider how the changes of the business reflect in the privacy policy

T&Cs may apply - A very good documentary to watch!

ePrivacy Regulation

- ***"The *other* EU regulation – was due 2018, but now expected late 2019"***

The regulation states that "electronic communications data should be defined in a sufficiently broad and technology-neutral way so as to encompass any information concerning the content transmitted or exchanged... and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication."

Updated from the 2002 "directive" to a "regulation"

https://www.itpro.co.uk/privacy/32712/eprivacy-regulation-what-is-it-and-how-does-it-affect-me

https://www.i-scoop.eu/gdpr/eu-eprivacy-regulation/

ePrivacy Regulation

Cookies

- "The new regulation recognises that there has been something of an excess of cookie consent requests from websites. The new Regulation aims to make it easier for browser settings to allow blanket acceptance or refusal of tracking cookies and other identifiers, and will clarify that consent is not needed for non-privacy intrusive cookies aimed at improving our internet experience (such as those which remember shopping cart history) or cookies used by a website to count visitors."

ePrivacy Regulation

Marketing and Spam

- Unsolicited communication through channels such as email, SMS, MMS, instant messaging, Bluetooth, and automated calling machines, will be banned under the regulation. National laws will affect how this is implemented, and people might be protected either by default or through existing 'do not call' lists that are set up to prevent marketing phone calls.
- Marketing calls will need to be identified by a mandatory prefix - primarily so that users have a clear idea of who they are receiving communications from if they wish to withdraw their consent for that particular company.
- The Regulation also states that it is "justified to require that consent of the end-user is obtained before commercial electronic communications for direct marketing purposes are sent to end-users in order to effectively protect individuals against the intrusion into their private life as well as the legitimate interest of legal persons."

ePrivacy Regulation

Internet of things and public Wi-Fi

- "The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications."
- Publicly accessible wireless networks, namely 'Wi-Fi hotspots', will also be subject to the regulation, regardless of their location, the company providing the service, or method in which that service is delivered. Those that are closed from the public, such as business networks, are not subject to the ePrivacy Regulation.

ePrivacy Regulation

"The future of the ePrivacy Regulation and the impact of Brexit on its application in UK"

https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/the-future-of-the-eprivacy-regulation-and-the-impact-of-brexit-on-its-application-in-uk

Which ePrivacy rules will apply in the UK after Brexit?

If the UK leaves the EU without the withdrawal agreement in place, SI 2003/2426 will be retained in domestic law by virtue of section 2 of the European Union (Withdrawal) Act 2018 (EU(W)A 2018). SI 2003/2426 will continue to be interpreted in the same way as it was before the UK's exit from the EU subject to any subsequent amendments (see below).

Domestic and EU case law that applies to the legislation will also continue to be relevant (EU(W)A 2018, s 6(3)). Amendments will be made to SI 2003/2426 under the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations to ensure that they continue to operate effectively after the UK's withdrawal from the EU.

If the Withdrawal Agreement is approved and enters into force on the UK's exit from the EU, then EU law will continue to apply to the UK during the transition period (currently due to last until 31 December 2020, although it is likely that it could be extended to either December 2021 or December 2022). If the Regulation applies (as opposed to merely coming into force) during the transition period, it will become UK national law automatically, by virtue of section 2(1) of the European Communities Act 1972. This provision

GDPR Research

Year 1 of GDPR: Over 200,000 cases reported, firms fined €56 meeelli... Oh, that's mostly Google

https://www.theregister.co.uk/2019/03/14/more_than_200000_gdpr_cases_in_the_first_year_55m_in_fines/

What is GDPR? The summary guide to GDPR compliance in the UK

https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

GDPR Research

How to Make Privacy Policies both GDPR-Compliant and Usable

https://ieeexplore.ieee.org/document/8551442

Are We There Yet?: Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)

https://dl.acm.org/citation.cfm?doid=3267357.3267368

GDPR Research

How ISO 27001 Can Help Achieve GDPR Compliance

https://ieeexplore.ieee.org/document/8760937

One Model For Implementation GDPR Based On ISO Standards

https://ieeexplore.ieee.org/document/8510716

#RSAC: How Corporate Boards Should Look at Cybersecurity Risk

https://www.infosecurity-magazine.com/news/rsac-how-boards-cybersecurity-risk/

https://isalliance.org/isa-publications/cyber-risk-oversight-handbook/

"In the handbook, it states that it is incumbent on the decision makers and the places of authority in organizations to develop a full enterprise risk management cyber-framework, where the governance structure, the accountability, the people, processes and resources are abundantly clear," Kroese explained.

By having that framework, Kroese said that it's possible to dispel the myth that cybersecurity risk cannot be quantified. While it might be hard to get an exact number, he argued that, with a framework, accountability and risk can be managed.

Part of managing risk is being aware of threats, which is where the US government is playing a role. Kroese noted that CISA has information sharing programs to help corporate boards and executive management make strategic decisions about cyber-risk. Since the government has a broader view, it can also help identify areas of systemic risk, where risk spans multiple organizations and even industries.