Cybercrimes and Policing Responses

Mike Levi
Cardiff University
Levi@Cardiff.ac.uk
IALS 2017

How much e-Crime and what kinds?

- **Why is knowing how much money/harm or what proportion of a population – or particular sub-groups – are victims important?**
  - The problem of ‘facts by repetition’
  - Evading demoralisation through fraud publicity
- Are past trends much guide to the future?
- Public and private sector differences
- Data breaches and collateral damage
  - UK and US govt, Sony, Yahoo, Wonga

Summary of EU experiences

- Almost half Internet users have discovered malicious software on their device, and nearly a third say they have received a scam email or phone call, and other types of cybercrime have been experienced by a substantial minority of Internet users in the EU. The proportions affected have remained similar since 2013.
- UK highest victims of bank card/online fraud; high on other eCrimes.
- The majority agree that the risk of becoming a victim of cybercrime is increasing; insecure about data privacy.
- > half say they are concerned about cybercrime, especially identity theft, malicious software and online banking fraud.
- But to what extent are these concerns the result of ‘shroud-waving’ in what Bruce Schneier has termed ‘The Theater of Security’?
- Social construction of fear for power and profit – cumulative build up

UK Data Breaches Survey 2016

common among those who have had them

ONLY

13% of all businesses set cyber security standards for their suppliers

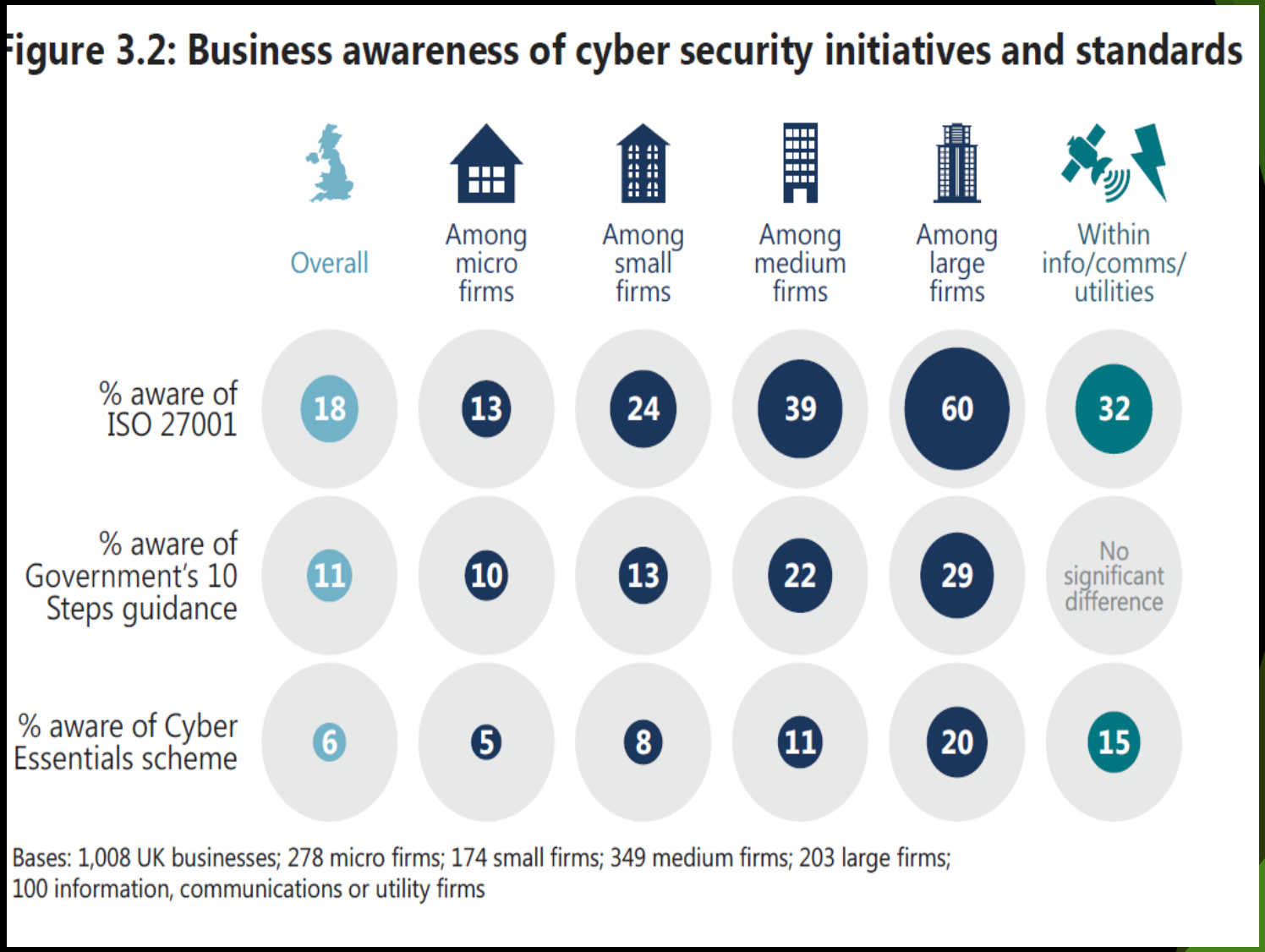
- 25% of medium and
- 34% of large firms do this

Stairway to Cyber-Essentials Heaven

Table 4.2: Proportion of businesses undertaking each of the 10 Steps

	Step description – and how derived from the survey	%
1	Information risk management regime – formal cyber security policies or other documentation and the board are kept updated on actions taken	34%
2	Secure configuration – organisation applies software updates when they are available	88%
3	Network security – firewalls with appropriate configuration	86%
4	Managing user privileges – restricting IT admin and access rights to specific users	77%
5	User education and awareness – staff training at induction or on a regular basis, or formal policy covers what staff are permitted to do on the organisation's IT devices	28%
6	Incident management – formal incident management plan in place	10%
7	Malware protection – up-to-date malware protection in place	83%
8	Monitoring – monitoring of user activity or regular health checks to identify cyber security risks	51%
9	Removable media controls – formal policy covers what can be stored on removable devices	21%
10	Home and mobile working – formal policy covers remote or mobile working	20%

Figure 3.2: Business awareness of cyber security initiatives and standards



Bases: 1,008 UK businesses; 278 micro firms; 174 small firms; 349 medium firms; 203 large firms; 100 information, communications or utility firms

Figure 3.4: Updates given to senior management on cyber security

Q. Approximately how often, if at all, are your organisation's directors or senior management given an update on any actions taken around cyber security?

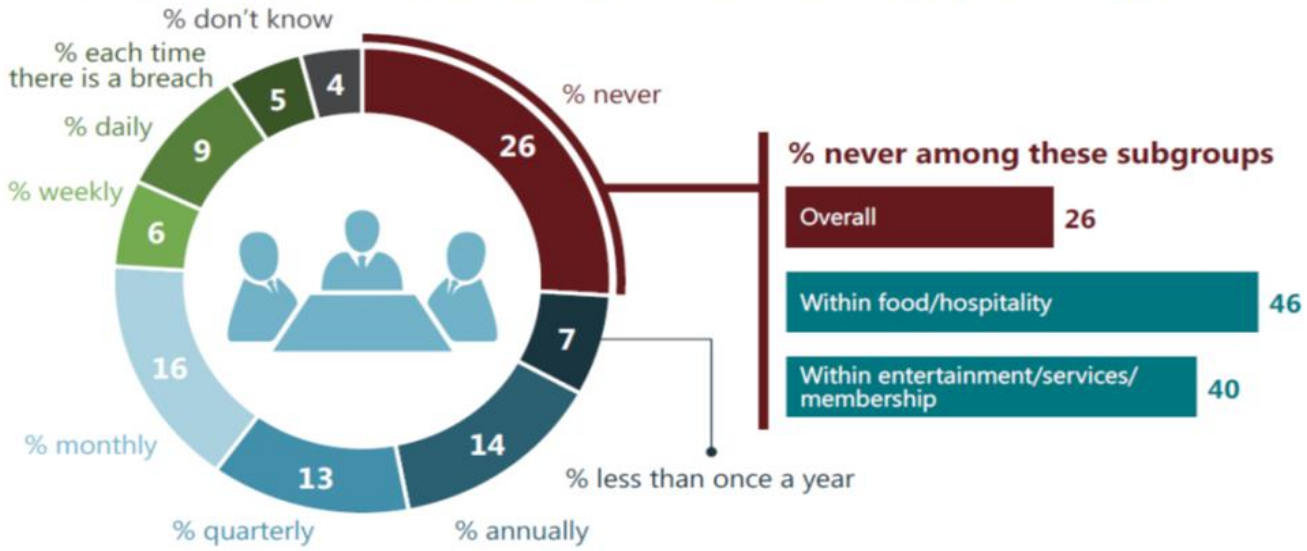
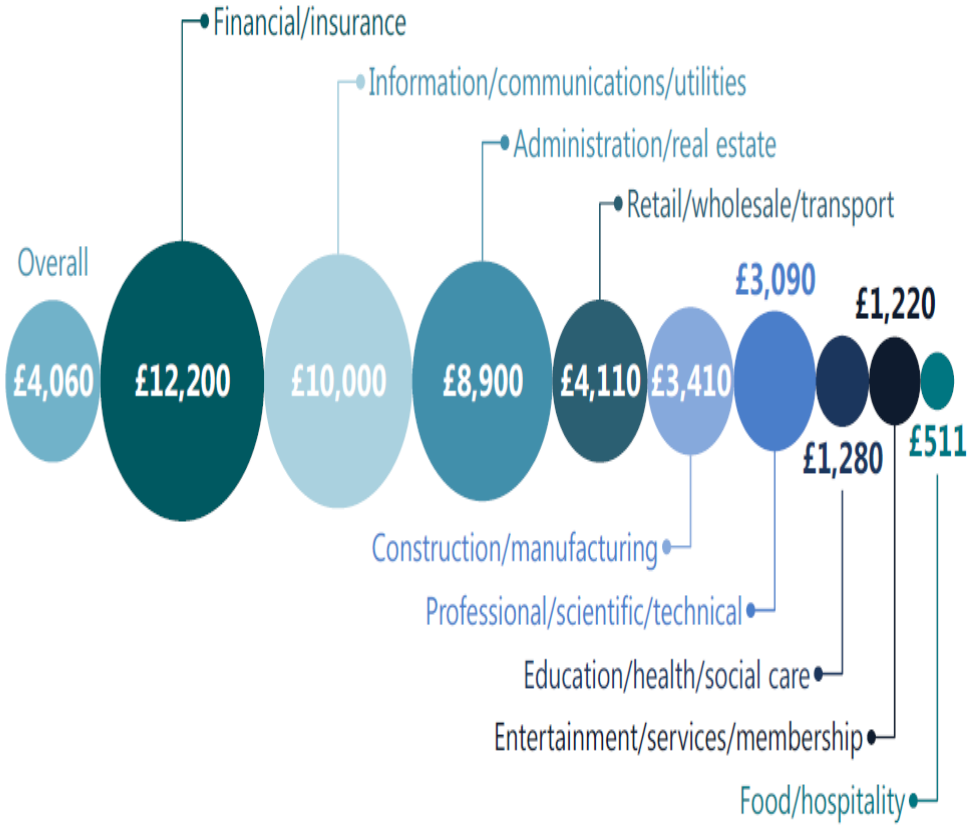


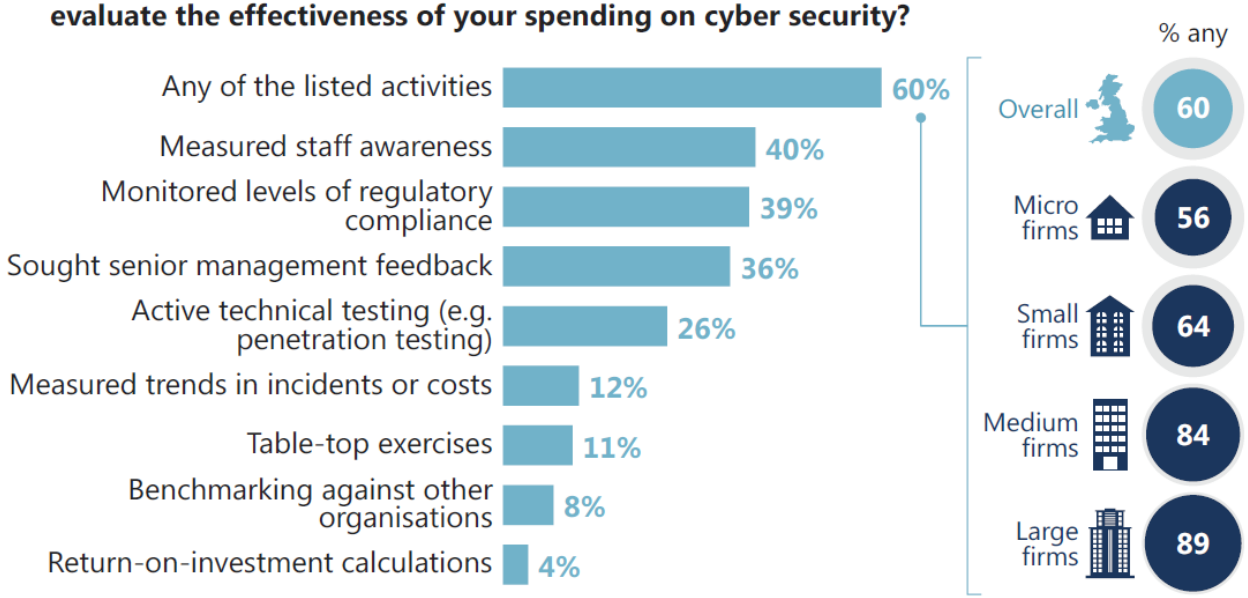
Figure 4.1: Average investment in cyber security in last financial year by sector grouping



Bases: 101 administration or real estate firms; 144 construction or manufacturing firms; 87 education, health or social care firms; 63 entertainment, service or membership organisations firms; 57 finance or insurance firms; 74 food or hospitality firms; 71 information, communications or utility firms; 84 professional, scientific or technical firms; 131 retail, wholesale or transport firms

Figure 4.2: Ways in which businesses have evaluated cyber security spending

Q. In the last 12 months, which of the following things, if any, have you done to formally evaluate the effectiveness of your spending on cyber security?



Bases: 668 investing in cyber security; 155 micro firms; 113 small firms; 255 medium firms; 145 large firms

Figure 4.6: Most common features of cyber security policies

Q. Which of the following, if any, are covered within your cyber security-related policies?

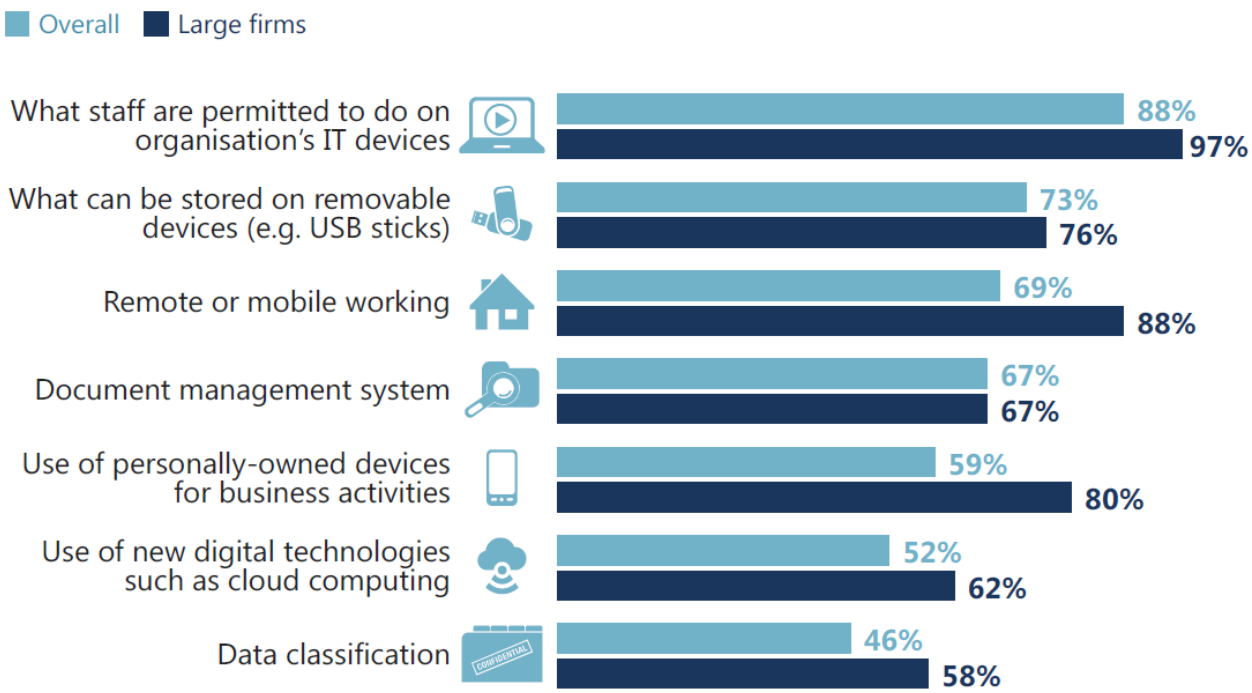
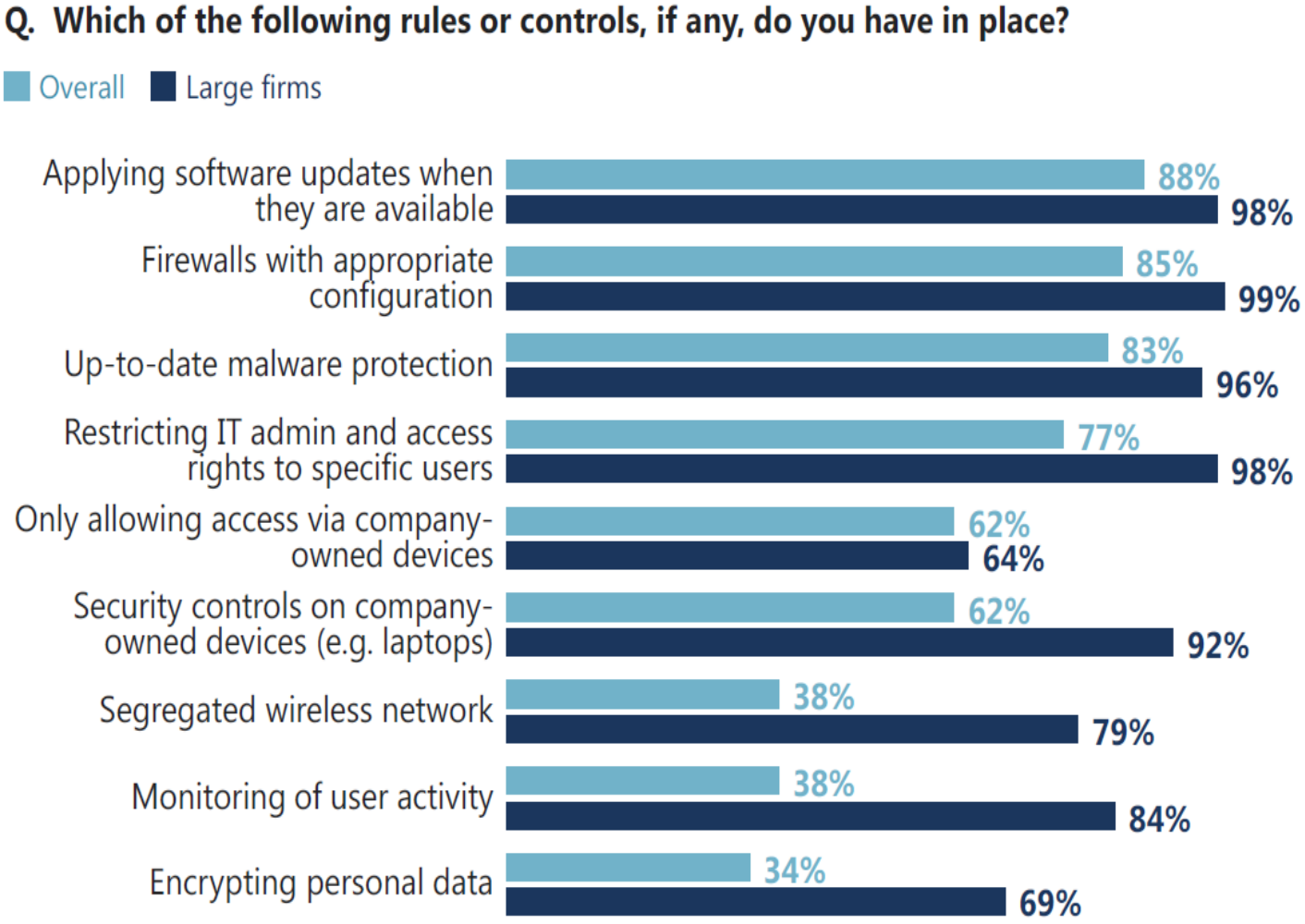


Figure 4.8: Ways in which businesses have identified cyber security risks in the last 12 months

Q. Which of the following, if any, have you done over the last 12 months to identify cyber security risks to your organisation?

Bases: 1,008 UK businesses; 278 micro firms; 174 small firms; 349 medium firms; 203 large firms

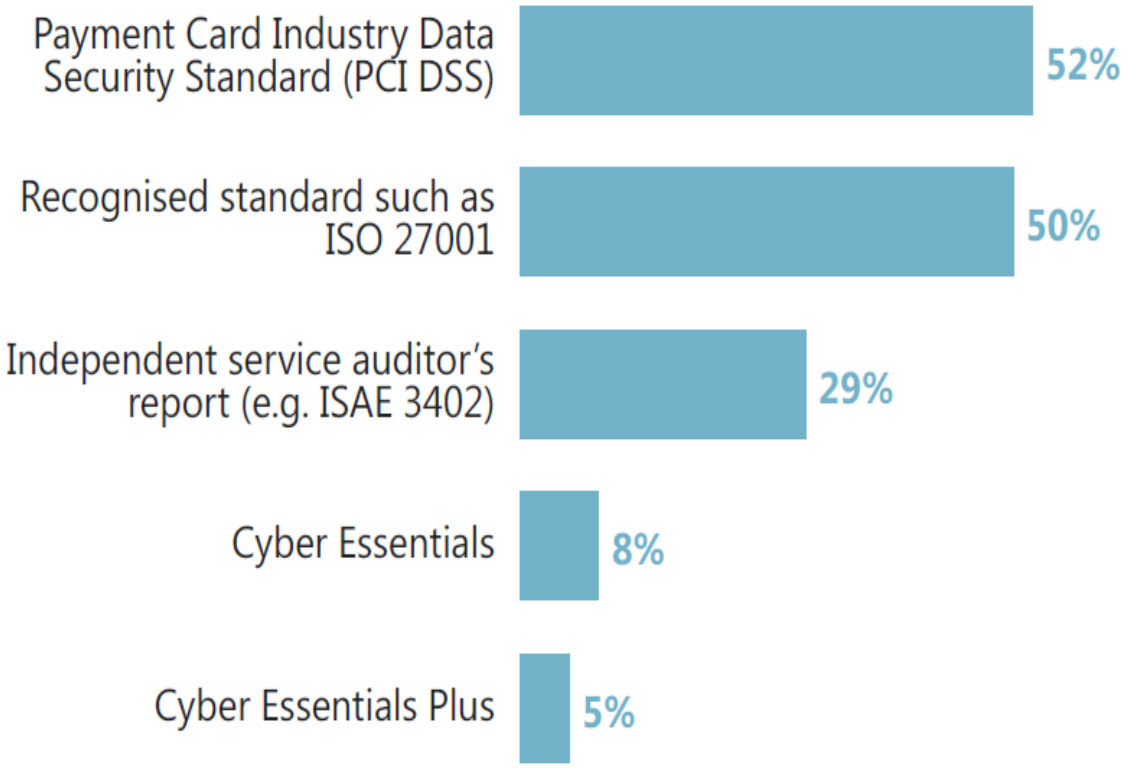
Figure 4.9: Rules or controls that businesses have implemented



Bases: 1,008 UK businesses; 203 large firms

Figure 4.10: Most commonly required cyber security standards for suppliers

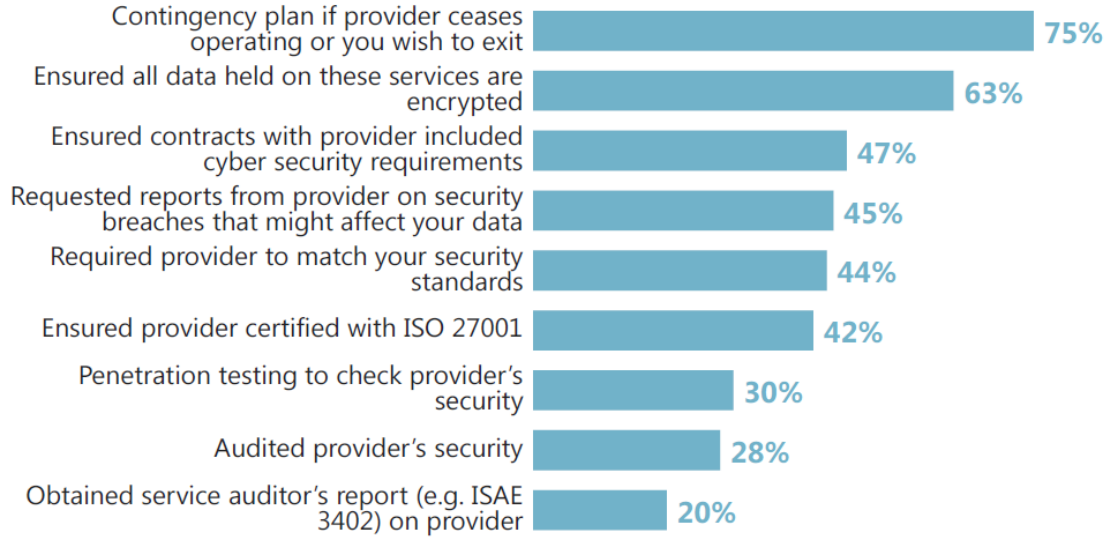
Q. Which of the following, if any, do you require your suppliers to have or adhere to?



Base: 241 with supplier standards

Figure 4.11: Most common ways of validating providers of externally-hosted web services

Q. Which of the following, if any, have you done in the last 12 months to test or validate the security of providers of online services?



Base: 190 that have validated security of external online service providers

Figure 5.2: Types of breach suffered among those who have had breaches

Base: 428 that had a breach or attack in the last 12 months
* denotes a percentage less than one per cent but greater than zero.

Table 5.1: Average number of breaches among those that had any breaches in last 12 months

	All businesses	Micro/small[32]	Medium	Large
Mean number	66	59	189	66
Median number	1	1	2	5
Base	418	110	176	132

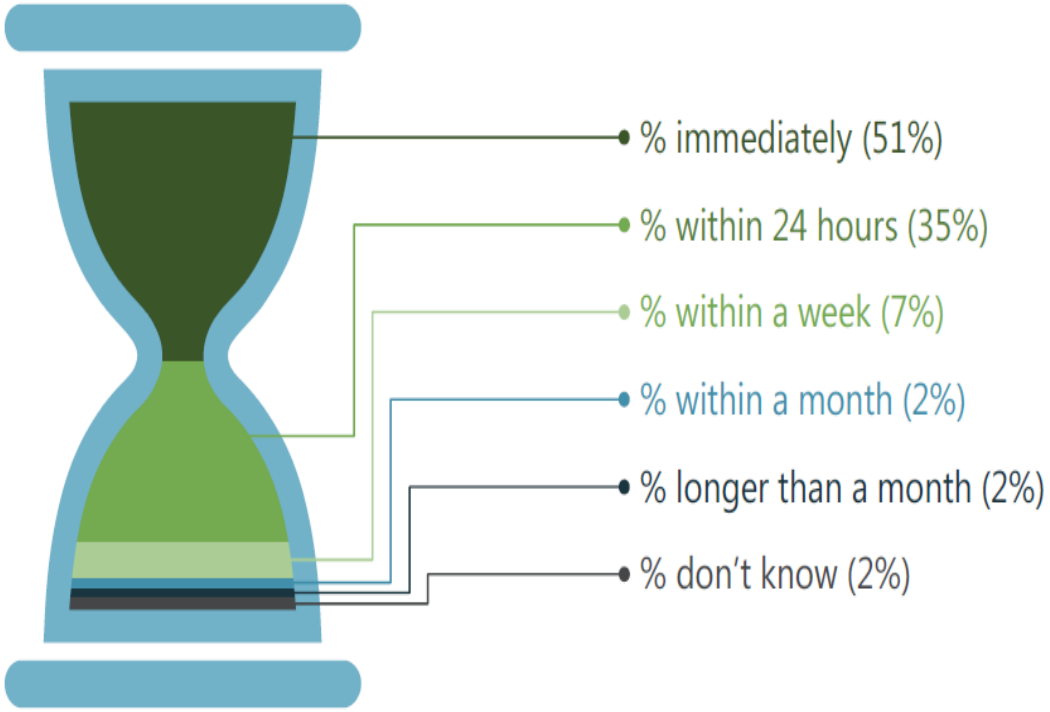
Figure 5.4: Impact of breaches experienced in last 12 months

Q. Have the breaches or attacks experienced in the last 12 months impacted your organisation in any of the following ways, or not?

Base: 428 that had a breach or attack in the last 12 months

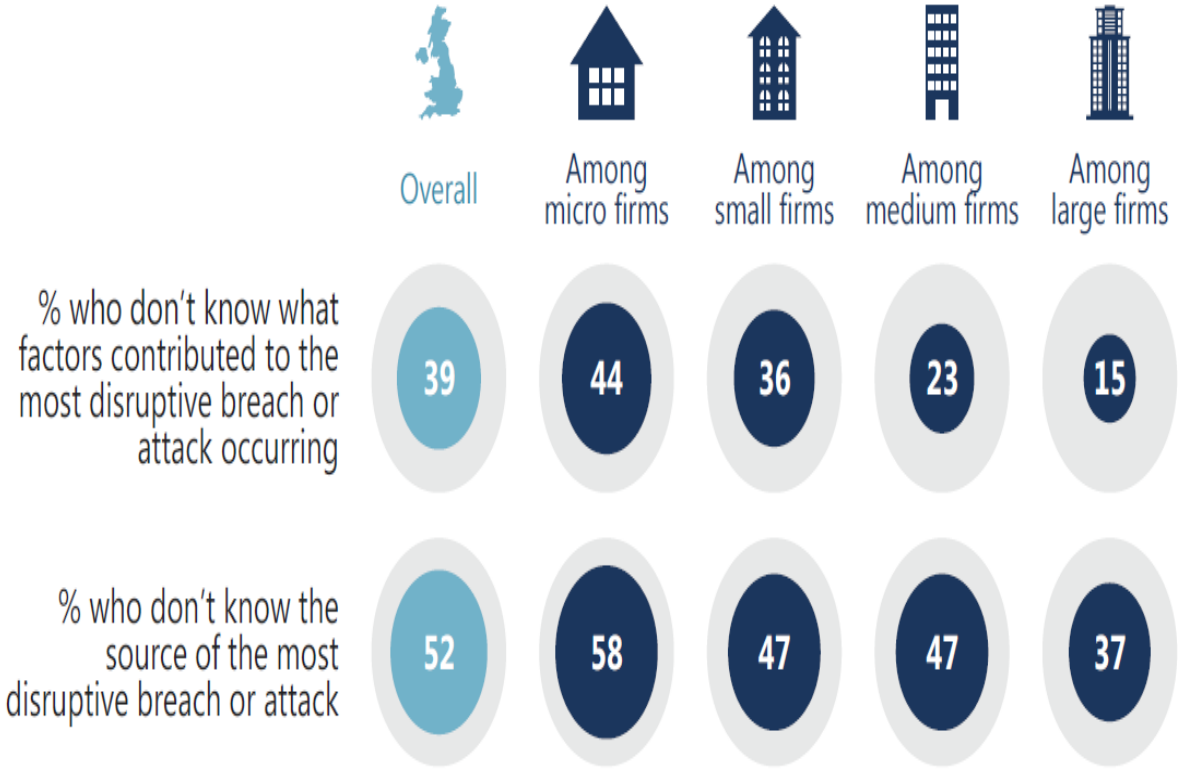
Figure 6.1: Time taken to identify the most disruptive breach of the last 12 month

Q. How long was it, if any time at all, between this breach or attack occurring and it being identified as a breach?



Base: 428 that had a breach or attack in the last 12 months

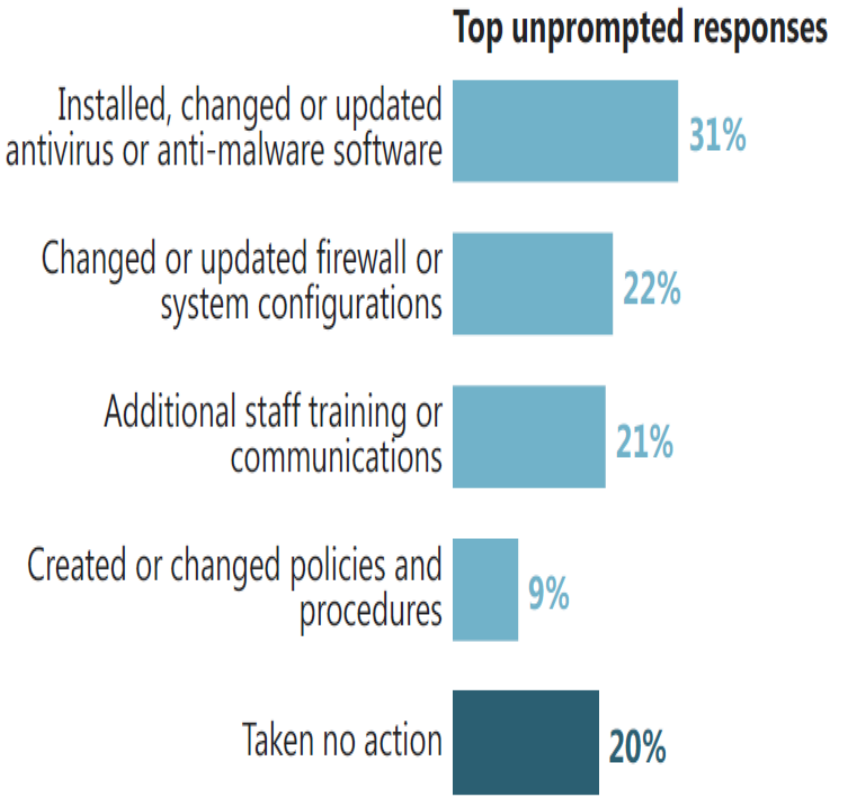
Figure 6.2: Businesses' understanding of the factors and sources behind their most disruptive breaches of the last 12 months



Bases: 428 that had a breach or attack in the last 12 months; 53 micro firms; 58 small firms; 179 medium firms;

Figure 6.5: Most common actions following the most disruptive breach of the last 12 months

Q. What, if anything, have you done since this (most disruptive) breach or attack to prevent or protect your organisation from further breaches like this?



Base: 428 that had a breach or attack in the last 12 months

Some data

- The remorseless rise
  - in e-crime ‘data’ in different countries or globalised via cybersecurity firms
  - In fears about identity theft and state-sponsored espionage/attacks
  - In suspicions that the fall in crime is not real but is an ‘e-transplant’
- > half UK adults aware of mass-marketing frauds, but 2.6 million individuals victims in lifetime; 800,000 in 2012
- 2013 UK data show that in their lifetimes, 500,000 UK adults had fallen victim to a dating/romance scam; 900,000 to a boiler room scam; 700,000 to a charity scam; 900,000 to a ‘need funds for an emergency’ scam; 700,000 by an inheritance scam and 800,000 by a lottery scam
- A quarter of those scammed had been subsequent victims
- All of these have potential demands on policing

Cybercrime – EU Measures

- 2013 – A Directive on attacks against information systems, which aims to tackle large-scale cyber-attacks by requiring Member States to strengthen national cyber-crime laws and introduce tougher criminal sanctions;
- 2011 – A Directive on combating the sexual exploitation of children online and child pornography, which better addresses new developments in the online environment, such as grooming (offenders posing as children to lure minors for the purpose of sexual abuse)
- 2002 – ePrivacy Directive , whereby providers of electronic communications services must ensure the security of their services and maintain the confidentiality of client information;
- 2001 – Framework Decision on combating fraud and counterfeiting of non-cash means of payment, which defines the fraudulent behaviours that EU States need to consider as punishable criminal offences.

Key Provisions of 2013 Directive

- The Directive does not cover breaches of personal data, but rather systemic cyber attacks that compromise data systems. So, pending general data protection regulation, the Directive requires that deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right, will be punishable as a criminal offence.
- It requires: (i) operators of critical infrastructures who are active in the financial services, transport, energy, health industries; (ii) enablers of information society services such as app stores, e-commerce platforms, internet payment, cloud computing, search engines and social networks; and (iii) public administrations, to adopt risk management practices & report major security incidents on core services.
- Let us see how quickly/effectively this will be implemented

Issues of debate

- Will this work? Is efficiency desirable?
- Some MS and business operators concerned about impact on growth. New reporting requirements could impose significant administrative burdens and become *'a factor of reputational risk'* for businesses (particularly for SMEs).
- Moving from a voluntary to a legislative approach risks creating a '*static compliance approach*' that could '*divert scarce security resources from areas requiring greater investment towards areas with lower priority [and] decrease Europe's collective security.*' Counter-argument for a voluntary, industry-led set of standards, similar to those used in the USA.
- No practical guidance is provided as to how a National Competent Authority will ensure consistent application of the Directive at home & across MS.
- Fails to elaborate on what a NCA must do when they receive a cyber-threat warning ENISA - only 17 Member States currently have national cybersecurity strategies. The UK favours a non-regulatory approach; Germany, regulation. So how will co-ordination work?

Continued

- Criteria used to determine when a NCA should report risks to the Cooperation Network are vague, so MSs might apply different reporting thresholds in practice;
- No guidance to deal with situations where MS cannot agree on a co-ordinated response to a cyber-threat. Considerable resistance from some Council members to mandatory sharing of information between Member States;
- Directive does not address concerns that having to seek agreement from each Member State might slow down an effective response; and
- A co-ordinated response across different MS might be complicated by different security levels, operator obligations and code-sharing.
- How will ENISA, the European Public–Private Partnership for Resilience ('EP3R') and CERT-EU cooperate? Too many players – rather like CoE, EU and UN?

Changes in cyber-enabled fraud risks

- *Which* sorts of *frauds*?
- *Which* sorts of *fraudsters?*
  - Are e-crimes becoming truly democratised via downloading kit?
- Operating from what sort of places?
- Public and private sector differences
  - Cyber-enabled/dependent/assisted
- Changes in the technology of controls

Policing Responses England and Wales

NCA
National Crime Agency

TEAM CYMRU

Financial Fraud Action UK
Working together to prevent fraud

DCPCU
Dedicated Card and Payment Crime Unit

cifas
Leaders in fraud prevention

GET SAFE ONLINE
Get Safe Online
Free expert advice

Met and City of London Priorities

- Industry-funded DCPCU Strategic Tasking & Co-ordination Group Priorities:
- **1. Remote Payment Fraud - 6012**
  - To work with bank investigators to target those criminal gangs responsible for remote payments.
- **2. Staff Integrity**
- **3. Social Engineering - Telephony**
  - To identify criminal groups…who are targeting largely vulnerable individuals and businesses.
- **4. ATM**
  - To proactively target organised gangs committing fraud at ATMs.

- **FALCON Mission: To reduce the harm caused by fraud and cyber criminals in London.**
- Ensure all Action Fraud (AF) referrals to the MPS are effectively responded to by dedicated fraud / cyber investigators
- Provide excellent victim care and seek compensation for our victims wherever possible
- Significantly increase the numbers of arrests and charges relating to fraud and cyber crime
- Proactively target cyber criminals and fraudsters, focusing on stemming the harm caused by the most prolific Organised Crime Groups
- Work in partnership with businesses to improve our response to fraud and cyber crime affecting London's businesses
- Undertake targeted prevention work with industry partners that designs out crime, tackles the enablers of cyber crime & fraud and raises awareness within the public and businesses

Who are we targeting for Protect and Prepare?

- Who are we targeting for Protect and Reassurance?
  - Individuals
  - SMEs
  - Larger Businesses – financial and non-financial
  - CNI
  - Central and Local Government not in CNI
- For what behaviours can ‘governance’ *politically* say to people and organisations:
  - This is your *own* responsibility to look after and we won’t help you if you haven’t done so

Reassurance Policing & the 4 Ps

- *Feeling* safer and/or *being* safer
- What are our objectives for which sectors & behaviours against which *effectiveness* can be judged?
- Who needs Pursue *by the police* and for what sorts of offenders and what behaviours is this realistic?
  - What can be done about these constraints?
- How can we sell these limitations to the public?
- Who are we using for 'third-party policing'?
  - CPNI, WARP (Warning, Advice and Reporting Points), CISPs, et cetera
  - Get Safe Online (and [over?]proliferation of advice from government and private sector)
  - ISPs/social media (in their evolving forms)
  - Designing out e-risks at source – an illusory goal?

The challenge for Government, police and ‘nudgers’

1. Convince general public & business that cyber crimes affect them personally

2. 

3. A culture shift that embraces complex sets of behaviours and continuous reappraisal; not a ‘one off’ issue (e.g. seat belts)

Public and private policing

- The mission of the police is “protect the weak, support the fearful and vulnerable, thank the helpful and lock up the bad guys” then Met Police Commissioner Sir Ian Blair (3 July 2005)
- Require private sector to be unpaid army of informants (AML SARs regime)
- Get private sector to pay for policing of crimes for which they find *public* police powers useful
  - In which countries is this a state-only function?
- Corporate investigation agencies for more complex e-crime cases/’self-cleaning’ – but when does this happen?
- What technologies of policing are available and are actually used for ‘financial crimes’?

Some models for action

- The targets for cyber-fraud/extortion are very widespread
- Need more understanding of teachable moments to divert offending
- Prevention should be built-in with minimal effort or administered in a more bottom-up way through peer groups, community level bodies and charities, to help individuals and SMEs adopt easy security processes - regular efforts from them are not practicable.

Some models for action

- Scope for experiments involving warning ‘pop ups’ on screen for those who fall victim to offers that could have been fraudulent, though need careful management of media concerns
- Larger organisations can/should promote good security practice in the organisational frameworks already established, paying attention to insider as well as outsider threats. Executives should consider if they really need the access privileges they have all the time
- Firms and govt. should think about what core assets need to be protected and separate them from ICT access
- Need to identify those individuals, businesses and government bodies who are at risk of repeat victimisation, to focus prevention efforts on the most ‘vulnerable’, community level efforts.

Some Thoughts for the Future

- Offline and online strategies differentiated
- Disruption strategies – including take-downs of websites, botnets and dark markets – reduce harm, especially if websites are taken down early
- but we know little yet about the longer-term signalling and market reduction effects of these 'whack-a-mole' measures
- Scope for experiments, e.g. warning 'pop ups' on screen for those who fall victim to offers that could have been fraudulent or fake, though need careful management of media concerns.
- More focused Internet Governance could deal with these Global Bads, but the politics of international opportunity reduction are very hard to achieve.

Futures

- Impact of global people migration
- Impact of Financial Action Task Force-led anti-money laundering (AML) measures
- Extended MLAT changes via AML and CoE Convention and pre-Brexit EU/UN proposals
- Impact of controls on other types of crime
- Impact of criminal network analysis technologies
- But how do we legitimate current policing or reform it?
  - Who needs and deserves a policing response?
- Rethinking and re-balancing high and low policing

Modern Crime Prevention (Home Office 2016)

- Up to 80% of cyber crime can be prevented if members of the public & businesses take simple precautions, equivalent to locking front doors.
- Campaigns will focus on three simple steps everyone can take that will prevent crime:
  1. Using strong passwords made up of three random words (e.g. fur-dis-bat);
  2. Installing security software on all devices; and
  3. Downloading software updates which contain vital security upgrades to correct bugs or vulnerabilities that hackers and cyber criminals can exploit.
- Working with online financial and retail services to help the public to better understand key online security principles, that will reduce their risk of being a victim of crime (particularly fraud), and help them to make an informed choice about where to take their business.

Stop refunding victims of online fraud - MPS Commissioner *Bernard Hogan-Howe said that the public were being "rewarded for bad behaviour"*

Commander Chris Greany said that the public should take as much care online as in the real world.