xyone Cyber Security

Stephen Robinson – Managing Director

20th October 2015
TVLS

xyone Cyber Security

How big is the problem globally?

Victims lose around **€290 billion** each year,

making cybercrime more profitable than the global trade in marijuana, cocaine and heroin combined.

- Europol, 2014

Cyber attacks cost the global economy more than **£238 billion** a year

and **200,000 jobs** have been lost as a result

- McAfee, 2014

As a business, cybercrime would be ranked **27th** in the world based on revenue.

- McAfee, 2014

Cyber crime is a bigger threat than nuclear war

- UK Government, 2013

The cost of cybercrime to the UK economy amounted to £6.8 billion in 2013.

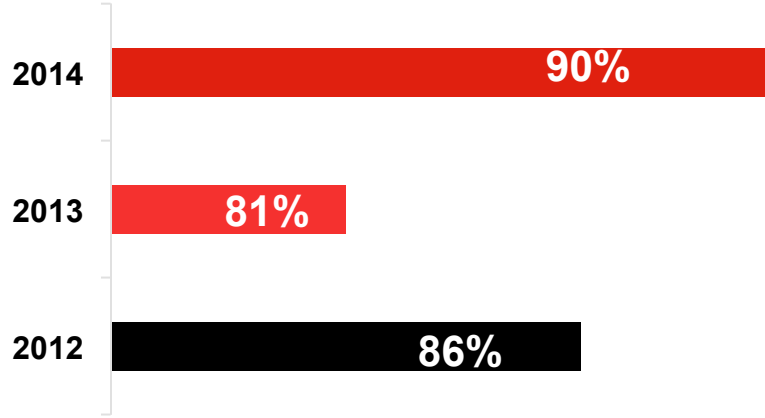
- McAfee, 2014

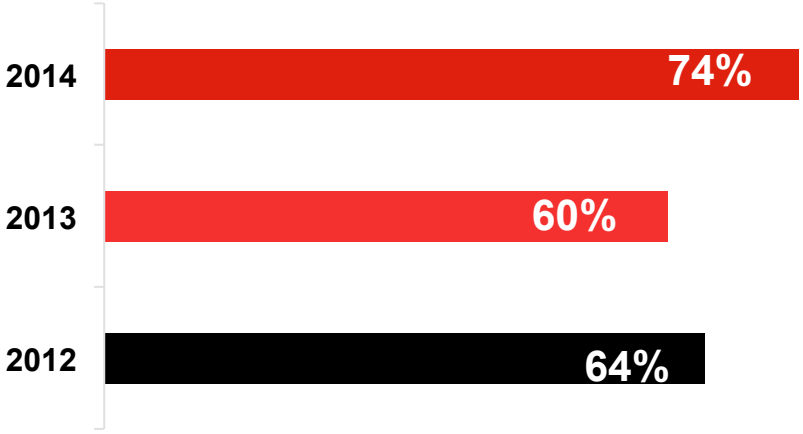
xyone Cyber Security

Cyber Breaches in the UK

According to the **PWC 2015 Internet Security Breaches Survey** released 1st May 2015:

90% of large businesses who participated in the survey suffered a breach in the last year (Up from **81%** a year ago)





74% of small businesses suffered a breach in the last year (Up from **60%** a year ago)

Source: PWC Internet Breaches Survey, May 2015

xyone Cyber Security

The average cost of a breach to a large organisation is

– **More than double the average cost in 2014.** (This could be as simple as through a virus!)

Source: PWC Internet Breaches Survey, May 2015

xyone Cyber Security

The average cost of the breach to a small organisation is

Also has increased significantly again over the past year.

Source: PWC Internet Breaches Survey, 2015

xyone Cyber Security

Video

Cyber Threat to Law Firms

http://www.pwc.co.uk/business-services/law-firms/cyber-security-issues-facing-law-firms.jhtml

xyone Cyber Security

SRA Warns ‘Friday afternoon fraud risk’

The SRA says its is receiving four reports a month of law firms being tricked into giving bank details to fraudsters in so-called ‘Friday afternoon scams’.

xyone
Cyber Security

THE EXTERNAL THREAT STRATEGY:

DON'T GET HACKED!

xyone Cyber Security

Law Firm Facing Cyber Threats

External Cyber Threats

- **Cyber Criminals** - A sophisticated campaign of targeted cybercrime by professionals who obtain personal credit card data or other corporate financial information for resale on the black market.

- **Nation-state espionage** carried out by an organised foreign entity for purposes of compromising company secrets or embarrassing the company.

- A socially motivated data breach performed by "**hacktivists**" who seek to bring attention to their causes.

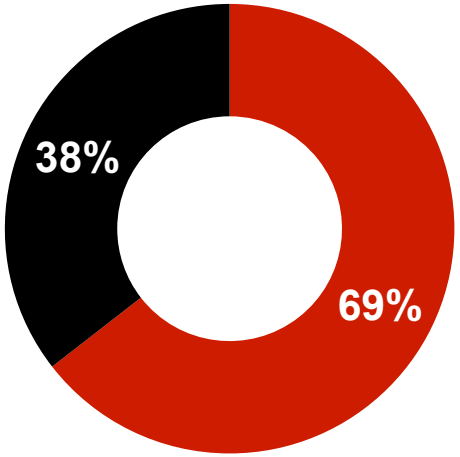
xyone Cyber Security

External Breaches

According to the **PWC 2015 Internet Security Breaches Survey** released 1st May 2015:

69% large organisations and **38%** small businesses were attacked by an unauthorised outsider in the last year.

- Up from 55% a year ago
- Up from 33% a year ago



xyone
Cyber Security

xyone Cyber Security

Penetration Testing

We administer a professional penetration testing service, which we offer on a recurring, managed basis to provide ongoing security for your business. Our in-depth pen test reports are written and analysed by our Certified Ethical Hackers, who will personally advise on the type and nature of vulnerabilities found within your web applications, networks or devices. We use the leading industry methodologies, such as OWASP to ensure accuracy and integrity of our work.

Our services include:

- **Network Penetration Testing**
- **Cloud Penetration Testing**
- **Wireless Network Security Testing**
- **Vulnerability Assessment**
- **Web Application Penetration Testing**
- **VOIP Penetration Testing**
- **Mobile Security Testing**

xyone Cyber Security

Sarah Green, Strategic Operations Manager

THE INTERNAL THREAT STRATEGY: MITIGATING THE HUMAN RISK

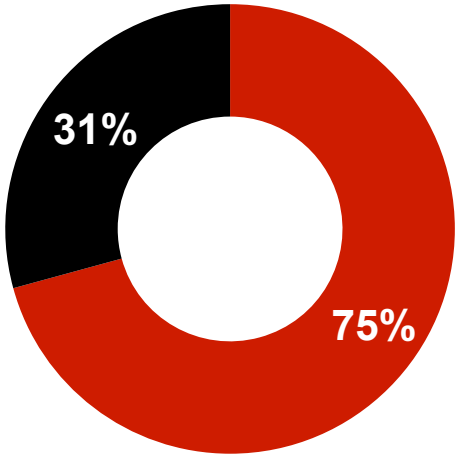
xyone Cyber Security

How likely is an internal breach?

72% Of companies where the security policy was poorly understood had staff related breaches.

50% Of the worst breaches in the year were caused by human error.

↑ Up from 31% a year ago



Organisations suffered staff related security breaches in the last year

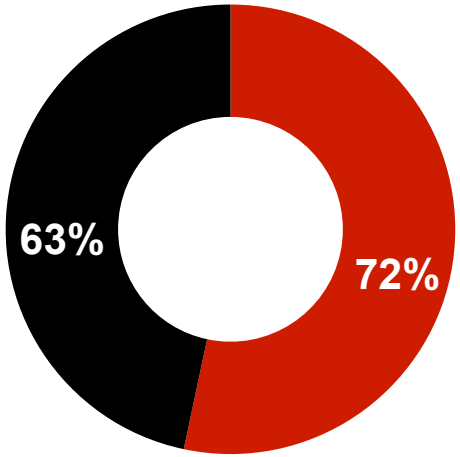
↑ Up from 58% a year ago

↑ Up from 22% a year ago

Source: PWC Information Security Breaches Survey 2015

xyone Cyber Security

How likely is an internal breach?



Organisations provide ongoing security awareness training to their staff.

↑ Up from 68% a year ago

↑ Up from 54% a year ago

Source: PWC Information Security Breaches Survey 2015

xyone Cyber Security

What are the common issues at this point?

- Where is the copy of the signed policy?
- When was it last updated?
- Is it enforceable to be used for disciplinary action?
- Does it include clauses about cyber/information security?
- Does the training relate to the procedures in your policies?
- Was your employee trained recently or just at induction?
- Can we recover from this breach?
- What is it going to cost?!

xyone Cyber Security

Internal Threat Mitigation Action Plan:

Board Awareness Training
set the culture of security from the top

Policy Enhancement
include cyber security procedures and make enforceable

Company-wide Training
for management and staff to adopt the enhanced policies

Policy Enforcement
ensure all staff are trained and agreed to the relevant policies

Management
allow HR to keep staff profiles and a record of signed policies

xyone
Cyber Security

“People are your biggest asset and your greatest vulnerability”

A rogue employee or group of employees who purposely leak confidential data, provide an unauthorized person with access to the corporate information systems or steals electronic documents.

xyone
Cyber Security

INFORMATION SECURITY STANDARDS

THE GLUE THAT STICKS IT ALL TOGETHER!

xyone Cyber Security

Cyber Essentials

What is it?

Government accreditation scheme, self-assessment questionnaire

What it does:

- Provides guidance to ensure basic cyber security controls are in place
- Checks that the firm has processes for remediating common threats
- Ensures ‘80% of common internet-based threats are prevented’

What it doesn’t do:

- Staff awareness training
- Checks for any existing vulnerabilities within websites/network
- Checks that information security policies are in place

xyone Cyber Security

CYBER ESSENTIALS PLUS

Cyber Essentials Plus

What is it?

Government accreditation scheme, self-assessment questionnaire with technical verification

What it does:

- Ensures the company's network and website are protected from common threats
- Checks that the company's mobile devices do not present risk to the infrastructure
- Verifies that the answers in the self-assessment questionnaire are true

What it doesn't do:

- Protects from a hacking breach or any manual exploitation
- Offer complete protection from all cyber security risks
- Check that information security policies are in use

xyone Cyber Security

ISO 27001

What is it?

International standard certification of your Information Security Management System

What it does:

- Sets policies and procedures to manage all information security processes in scope
- Ensures that policies are implemented and are in use
- Checks that internal information management risks have been addressed

What it doesn't do:

- Protect from the external threat to the company's IT systems such as a cyber-attack
- Train staff to recognise the cyber/information security threat
- Provide remediation of common cyber threats/viruses

xyone Cyber Security

Lexcel Practice Management Standard Law Society Accredited

Lexcel

What is it?

Standard of excellence for law firms, v6 recently incorporated with information management requirements (section 3)

What it does:

- Ensures internal policies and procedures are in place for information management
- Ensures policies are implemented and enforced
- Ensures staff undergo information management training

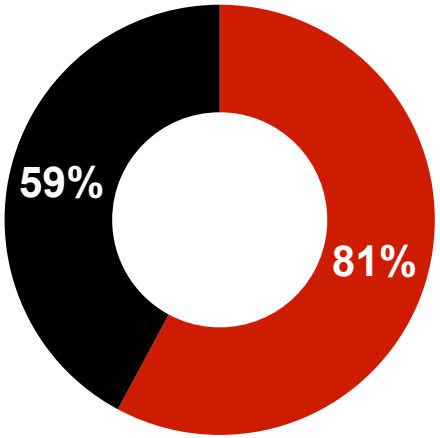
What it doesn't do:

- Protect against any external threats to the firm's IT systems
- Provide a plan for the ongoing mitigation of common cyber threats

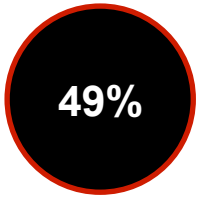
xyone Cyber Security

Benefits of getting certified

- Use guidance as a backbone for implementing and managing security
- Competitive advantage
- Increase potential for winning contracts
- Meet mandatory stipulations within contracts
- Enhance customer trust
- Enhance own peace of mind
- Protect assets and IP
- Address growing cyber risk



Organisations have implemented or plan to implement ISO 27001.



Of respondents badged to Cyber Essentials or Cyber Essentials Plus, on their way to accreditation or plan to be badged.

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

Information Security Management System ISO 27001 Certified

Lexcel Practice Management Standard Law Society Accredited

xyone Cyber Security

Law Firms top 5 reasons For Not Embracing Cyber Security

- Education
- Management buy-in
- Transfer of responsibility – we have an IT team!
- Lack of pressure from clients/contracts
- The ‘it’ll never happen to us’ culture

xyone
Cyber Security

C|EH™
Certified Ethical Hacker

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®

ISOQAR REGISTERED
UKAS MANAGEMENT SYSTEMS 0026

Certificate Number 12422
ISO 27001

CYBER ESSENTIALS

CYBER ESSENTIALS
QG
Accredited Certification Body

xyone
Cyber Security

Thanks for listening!