Alcumus ISOQAR

Managing Corporate Risk in Cyberspace

The role of certified management systems in cyber security

A non-technical paper for senior decision makers looking to improve the management of cyber security in their organisation

isoqar.com

Contents

Part 1
The Growing Threat

The Costly Menace of Cyber Attacks

Official statistics on the scale of the cyber security challenge in the UK are shocking. A government report in 2018 found that more than four in ten businesses experienced a cyber attack in the previous year, rising to seven in ten for larger organisations.

The reality is that the situation is probably worse: not just because the number and sophistication of attacks grows on a daily basis, but because many organisations aren't even aware they are victims. Figures vary considerably but it is typically 180 to 350 days between breach and detection. And as even casual observers of current affairs will be aware, many organisations are reluctant to admit to breaches, only disclosing them years later.

Some organisations have in the past tried to 'buy off' the hackers. This is no longer an option under GDPR and the Data Protection Act as the ICO (Information Commissioner's Office) must be informed of any significant breaches within 72 hours.

Cybercrime is projected to cost the global economy $2 trillion in 2019 (Forbes, 2016) And yet, just over a quarter of businesses have a formal policy covering cyber security risks. In the charitable sector, it's just one in five.

It's hard to disentangle the broader issue of fraud from cybercrime. Fraud describes trickery used to gain dishonest advantage, usually financial, over another person. The Annual Fraud Indicator 2017 estimated the cost of fraud to the UK as being £190bn a year. Whilst it's individuals who form the majority of the victims, it's often as a consequence of the scammers masquerading as legitimate businesses utilising information that has been hacked. And increasingly, as the scams become more sophisticated, businesses themselves are falling for it.

Far too often, either nothing is done or money is spent in an uncoordinated, reactive way. It's imperative that organisations take a strategic, considered approach to cyber security. This is a problem that cannot be solved by simply throwing money at it. To succeed, you need to implement a strong governance structure overseeing efficient and effective management systems.

What is a 'cyber attack'?
An attempt to gain unauthorised access to systems and data or to cause damage.

Taking Responsibility

As more and more devices become connected to the Internet of Things and we take instant connection to cyberspace - the virtual world accessed through the internet - for granted, the more we expose our organisations to attack.

But the government cannot be relied upon for protection. Cyberspace has no respect for geographic boundaries and the criminals who operate within that domain are always a step ahead. (Indeed, governments have often called for the weakening of encryption in the wake of terrorist attacks, for example.)

It's easy to see why criminals are attracted to this arena: it's hard to police, the chances of getting caught are low - as are the penalties - and the prizes are potentially vast. It's also a rewarding technical challenge for hackers so inclined, helping achieve notoriety in the hacking community. Within a commercial context, the major motivations include:

- corporate espionage - the theft of corporate secrets to gain competitive advantage
- sabotage of systems to harm competitors' operations
- copying of customer data to sell on the dark web
- to manipulate share prices of companies

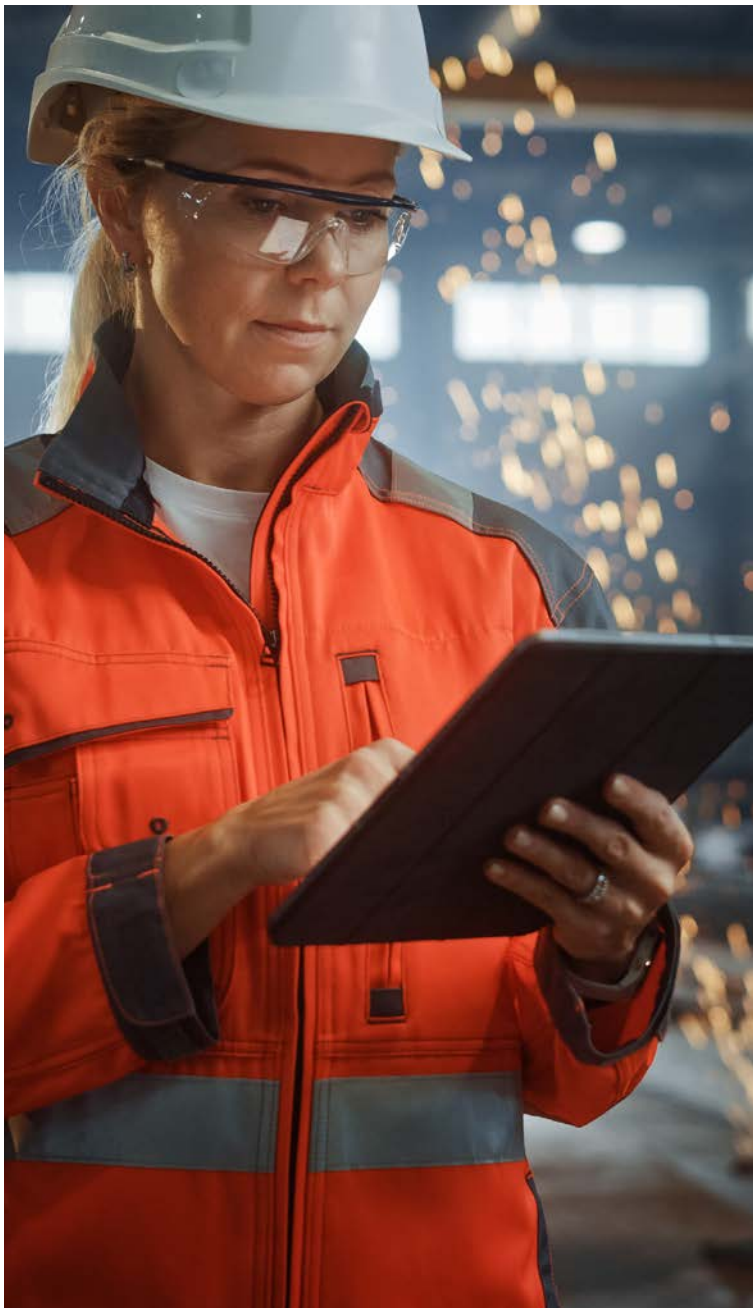
It's curious that so many organisations do not take the threat more seriously. The General Data Protection Regulations (GDPR) - EU legislation couched within the UK's Data Protection Act 2018 - caused many to broadly consider the role of IT in their business and establish policies regarding the collection and storage of personal data, but for the most part the scope of those policies has not extended to cover the wider challenge of cyber security.

The government's Cyber Essentials (and Cyber Essentials Plus) certification scheme, which encourages self-help for organisations to implement basic technical controls, is a good starting point but has its limitations and has seen low take up.

So, how vulnerable are you to cybercrime? How do you manage the risk? What measures should you take to implement robust management systems and working practices to enhance your organisational resilience?

Later on in this paper you will learn about why internationally recognised, third party certified management systems are the ideal mechanism to enable your organisation to address the cyber security challenge.

What is 'cyber security'? Cyber security is the convergence of people, processes and technology to protect the integrity, confidentiality and availability of hardware, networks, software and data from attack, damage or unauthorised access.



How Cyber Attacks Happen

It's important to remember that cyber attacks often don't come from outside the organisation. Nor are they always financially and criminally motivated. Many are 'inside jobs', sometimes caused by incompetence or poor internal systems, but often deliberate. The motivation might be spite, political or in the case of the so-called 'script kiddies', just pure bravado.

Indeed, not all apparent breaches are attacks at all. Something as simple as a member of staff getting write control over a key document and making unauthorised changes can cause as many problems as any hacker.

Regarding external attacks, there are many and varied reasons for the technical failings within systems, networks and devices which allow attackers to gain unauthorised access by exploiting vulnerabilities. For example: design flaws; failure to keep software up to date; user error; enabling staff to use their own devices (i.e. BYOD - Bring Your Own Device) and poor practice with user privileges.

But none of these and the myriad other reasons for failure can be addressed in a satisfactory, sustainable way without first getting your house in order in terms of good governance.

In essence, failings usually happen because senior management do not take their responsibilities seriously enough.

In May 2018, the Crown Prosecution Service (CPS) was fined £325,000 by the ICO after they lost unencrypted DVDs containing recordings of police interviews.

The National Cyber Security Centre's 10 Steps to Cyber Security guidance places 'Risk Management Regime' at number 1 and identifies this as a board level responsibility.

It is essential that the same level of rigour is applied to assessing cyber risks as to any other aspect of the business. They NCSC says that this can be achieved by "embedding an appropriate risk management regime across the organisation, which is actively supported by the board, senior managers and an empowered governance structure".

They identify that lack of effective risk management and inadequate management leads to:

- **Exposure to risk:** Without effective governance processes the board will be unlikely to understand and manage the overall risk exposure of the organisation.
- **Ineffective policy implementation:** The board has overall ownership of the corporate security policy. Without effective risk management and governance processes the board cannot have confidence that its policies are being consistently applied across the business as a whole.

Conversely, it is important that the board balances risk against opportunity, and this can only be achieved at a strategic level. Risk decisions taken within a dedicated security function, rather than organisationally, may focus solely on achieving high levels of security. This may result in an overly cautious approach to risk, leading to missed business opportunities or additional cost.

If you suffer an attack you should report it to the National Fraud & Cyber Crime Reporting Centre.

Cyber Harm - Counting the Cost

In a report published in 2018, researchers from the University of Oxford and University of Kent identified at least 57 ways in which cyber attacks can have a negative impact on the economy, individuals and even nations.

The comprehensive report identified a series of negative outcomes that an organisation can suffer. Consequences such as disrupted operations and lost sales are predictable, but some of the factors possibly not considered by organisations in their risk management calculations include:

- investigation costs
- fall in stock price
- fines from regulatory bodies (especially in the
- case of data breaches)
- compensation payments to those affected by the incident
- extortion payments e.g. after ransom-related incidents
- reduced corporate goodwill
- loss of key staff and inability to recruit desired staff
- media scrutiny and reputational damage
- loss or suspension of accreditation or certifications
- reduced credit scores and ability to raise finance for investment and growth
- drop in staff morale and performance

London-based firm Tax Returned Limited was fined £200,000 by the ICO in 2018 for sending out millions of unsolicited marketing text messages.

Not all attacks result in material losses such as loss of data or assets that carry a financial cost. But where the attack does result in financial impact, the average cost is £22,300 for large businesses and £16,100 for medium businesses.

Other research has shown that 11% of businesses reported it cost them more than £50,000. Statistics show year-on-year rises, indicating the problem is getting worse and security measures are not always having the desired impact.

A global cyber attack in more than 150 countries in 2017 crippled the NHS and hit international shipper FedEx.

Legal Consequences

The above section outlines the consequences that are largely financial and reputational. But there are also legal consequences should the outcome of a cyber attack result in a data breach.

Data protection laws require that organisations manage the security of all personal data, for example information relating to customers and staff.

If this data is compromised, then the General Data Protection Regulations (GDPR) allow the Information Commissioner's Office (ICO) to fine organisations up to 4% of global annual turnover or 20 million euros - whichever is greater.

In addition, the ICO has a range of corrective powers and sanctions to enforce GDPR, including:

- issuing warnings and reprimands
- imposing a temporary or permanent ban on data processing
- ordering the rectification, restriction or erasure of data
- suspending data transfers to third countries

In summary, if the cyber attack itself does not do irreparable damage to your organisation, the ICO has the power to do so.

The NIS Directive

The Network and Information Security Directive is EU legislation, transposed into UK national law in 2018 as The Network and Information Systems Regulations 2018. It received considerably less media coverage than GDPR but is arguably more important to the integrity of cyberspace.

Its purpose is to create an overall higher level of cyber security in the EU. It does this by obliging each member state to have in place a national framework so that they are equipped to manage cyber security incidents. This will still apply to the UK after withdrawal from the EU.

It affects digital service providers (including search engines and cloud computing services) and 'operators of essential services' (including energy, transport, health, water and digital infrastructure providers).

Leadership

This all begs the question: why doesn't senior management take cyber security more seriously? Although three quarters of businesses (and over half of charities) say that cyber security is a high priority, just 30% of businesses (24% of charities) have a board member or trustee with responsibility for cyber security.

Cyber resilience - the ability to quickly detect attacks and return to normal operation with minimal downtime and minimum damage - is not front of mind for many organisations.

The ICO fined Uber £385,000 for failing to protect customers' personal information during a cyber attack which resulted in the records of 82,000 drivers based in the UK being taken.

As stated earlier, just over a quarter of businesses have a formal policy covering cyber security risks. That falls to one in five in the charitable sector.

There are a number of reasons why cyber security may not be given the priority it surely merits.

- Senior management and board-level executives' limited knowledge of cyber security means it does not get adequate attention
- It is difficult to forecast the likelihood of a cyber attack succeeding, and the potential losses, thus it is challenging to make a business case to invest in cyber security
- There is no legal obligation to manage this risk (although there are legal consequences for failure), as for example there is with health and safety
- The organisation has not to date suffered a seriously debilitating attack and so is unaware of the havoc that can be wreaked
- There is an assumption that the organisation is probably already adequately protected

Organisations too often take a piecemeal approach, reacting to issues as they arise, rather than adopting a planned, strategic approach that pre-empts incidents and provides a framework for managing incidents and handling the aftermath of an attack.

In other words, the board's focus should be on risk management just as much as risk mitigation. So, how does an organisation achieve this? How does cyber security become embedded in the culture and operational fabric of an organisation?

The answer is **third party certified management systems** that go right to the heart of the organisation and demand leadership from the top.

Part 2
The role of Certified Management Systems

Good Governance

The government's National Cyber Security Centre's advice for managing risk in cyberspace includes the following recommendations:

- Establish a governance framework - to enable and support a consistent approach to risk management across the organisation, with ultimate responsibility residing at board level
- Produce supporting policies - an overarching technology and security risk policy should be created and owned by the board to communicate and support risk management objectives, setting out the risk management strategy for the organisation as a whole
- Apply recognised standards - consider the application of recognised sources of security management good practice, such as the ISO/ IEC 27000 series of standards

All of the above is achieved through the implementation of appropriate BS and ISO standards. These management systems, if maintained and continuously developed, will enable the organisation to:

- manage risk - protect the organisation against attacks
- ensure mitigation - reduce the impact of attacks
- enable business continuity (disaster recovery) - facilitate swift recovery after an attack through an incident response plan

Facebook were hit with a £500,000 fine from the ICO in 2018 for serious breaches of data protection law.

What is a Certified Management System?

Management systems are the way in which an organisation controls the parts of its operation, and the relationship between those parts, to achieve its business objectives.

Some organisations operate in an informal way; others choose a more organised, formal approach with a recognisable system - usually documented - embedded into the fabric of the organisation.

Management systems (or 'standards') developed by ISO (the International Organisation for Standardisation) or BS (British Standards) provide frameworks - not rules - for an organisation to manage many facets of its business such as product and service quality, environmental performance, health and safety and of course, IT and many functions that relate to cyber security.

Most systems work on the Plan-Do-Check-Act principle that ensures continuous improvement. And whilst documentation, for example of policies and procedures, is more often than not a requirement, the amount of 'paperwork' is often considerably less than imagined.

Certificates that demonstrate compliance are issued by a network of officially accredited certification bodies across the world. They audit an organisation's management systems to ensure that they have been developed correctly and are implemented and functioning properly.

Benefits of Certified Management Systems

The advantages of implementing certified management systems - in whatever aspect of the business - are many and varied. Those who have achieved certification in any standard overwhelmingly report that a management system:

- provides evidence of capability to prospective customers
- instils organisational discipline
- facilitates easier management of complex systems
- makes implementation of change easier
- encourages early recognition of potential failings and opportunities
- enables swift recovery after incidents
- provides a framework for testing and continuous improvement
- helps introduce best practice through third party auditing
- improves the relationship between organisational functions
- helps win new business

With specific reference to cyber security, implementing the appropriate standards will additionally allow an organisation at a strategic level to:

- provide their customers with the assurance that they have the appropriate processes and systems in place to manage their data (i.e. are GDPR compliant)
- deliver confidence to investors/partners/shareholders that the business is managing all risk to prevent cybercrime

ISO 27001 – Information Security Management

Overview

An Information Security Management System (ISMS) is the starting point for a robust approach to cyber security and the most widely adopted of the ISO standards in this field.

It helps you to keep information safe and minimise the risk of security breaches. ISO 27001 also defines the very concept of security of information in a broader context – not just keeping information away from prying eyes but also mindful of the integrity and availability. After all, organisations hold information because it is of use to the proper functioning of the business.

Features and Benefits

- Embeds IT security best practice
- Improves defences against cyber attack - unauthorised access to information (including in a non-digital format) is protected
- Risks of breaches are thoroughly assessed and analysed
- Relevance and accuracy of stored information is effectively managed
- Information is stored and managed in a legally compliant way (supporting GDPR)
- Counters risk related to mobile devices
- Prevents identity theft
- Access and ability to modify information is effectively managed and authorised users appropriately vetted
- The impact of a breach is mitigated

What the Alcumus ISOQAR experts say:

"How many people in your organisation store files on USB sticks in their drawer? Do you carry a notebook and just leave it on your desk for anyone to pick up? Do colleagues email documents to their personal addresses so they can work on them at home? Do you give out the Wi-Fi password to anyone who asks? It's often these seemingly innocuous things that leave your organisation exposed and vulnerable to attack. ISO 27001 is the perfect framework for addressing everything from your strategic approach to data management to how often staff have to change their password."

KLAVS HENRIKSEN, LEADER AUDITOR, ALCUMUS ISOQAR

ISO 22301 - Business Continuity

Overview

Prevention is better than cure but sometimes, even with the best planning, things go wrong.

A Business Continuity Management System (BCMS) is not just about disaster recovery or incident response. There is more to ISO 22301 than handling the aftermath of an IT catastrophe.

Indeed, ISO 22301 focuses on the full range of issues from unexpected disruptions and inconveniences to business, all the way to full on disaster. It does not just relate to cyber issues although an organisation may restrict the scope of the system for just this purpose. A BCMS supports an organisation in the event of any disruptive incident, for example, fires, power outages and flooding.

Features and Benefits

- Instils a risk management approach
- Requires an organisation to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of, prepare for, respond to, and recover from disruptive incidents when they arise
- Compels an organisation to establish well thought out contingency plans
- Requires the organisation to establish
- Maximum Acceptable Outage (how long should normal service be out), also what is the restoration point (Recovery Point Objectives)
- Establishes protocols for internal and external communication in the event of an incident: who to tell, how much to disclose and how to communicate it

What the Alcumus ISOQAR experts say:

"In some respects, ISO 22301 is the ultimate risk management tool. It's more grounded in the real world and more useful than ISO 3100 which also centres on risk management. There's nothing out there that helps an organisation to assess the potential for incidents and the associated cost (and not just financial) and deal with the aftermath of incidents in quite the same way as this standard. When it comes to incident response and minimising disruption, there really is nothing that can replace a well thought out documented system to get a business back on its feet. I have seen many instances of ISO 22301 certified organisations who count their blessings that they adopted the standard."

STEVE STUBLEY, TECHNICAL DIRECTOR, ALCUMUS ISOQAR

ISO 20000 - IT Service Management

Overview

ISO/IEC 20000, usually referred to as just ISO 20000, is the international standard for IT Service Management (ITSM). Its broad aim is to help organisations deliver more effective IT services (within your business and/or to external customers) including the management of cyber security.

It is applicable to any organisation in any industry - it's not just for large businesses and it's not just for those in the IT sector. The standard was developed to mirror the best practices described within the IT Infrastructure Library (ITIL) framework.

Features and Benefits

- Specifies requirements for establishing, implementing, maintaining and continually improving a service management system
- Forms the hub in a collection of management systems to help establish strong cyber security defences
- Supports the management of the service lifecycle, including the planning, design, transition, delivery and improvement of services
- Brings IT into the sphere of governance
- Helps control cost of IT

What the Alcumus ISOQAR experts say:

"Many at board level are often intimidated by the subject of IT. It's odd that people are so happy to profess ignorance of the subject of IT in a way they would never admit for subjects like maths or English! ISO 20000 is ideal for putting IT on the agenda. In basic terms, it helps a board get the big picture of whether the IT function is operating as it should, delivering the right service in the right way to meet the business goals, and whether it's providing value for money. It's at the heart of any organisation that takes cyber security seriously."

TOM MARTIN BALL, INFORMATION SECURITY SECTOR MANAGER, ALCUMUS ISOQAR

BS 10012 - Personal Information Management

Overview

This is a British Standard (rather than one that has been adopted by ISO) and outlines the specification for a Personal Information Management System (PIMS).

It is particularly useful in helping organisations comply with data protection laws such as the GDPR (General Data Protection Regulations).

Features and Benefits

- Ensures a focus on data privacy management
- Requires a risk-based approach to data privacy
- Integrates well with ISO 27001
- Provides the ultimate reassurance that you take GDPR seriously (Article 42 of the GDPR encourages use of independent certification)

What the Alcumus ISOQAR experts say:

"This standard takes a lighter touch than ISO 27001, which provides a framework for a much broader approach to information security. BS 10012 is narrower in that it just focuses on the management of personal data. It was in fact updated to ensure it aligns with the requirements of GDPR. So for some organisations, particularly smaller ones who don't want the extra workload, BS 10012 may be a more appropriate choice."

DONN HOULDSWORTH , AUDIT TEAM MANAGER, ALCUMUS ISOQAR

Cyber Essentials/ Cyber Essentials Plus

Overview

This is a UK government scheme which provides low cost certification for organisations who meet criteria to demonstrate their cyber security credentials. It involves the implementation of technical controls designed to protect an organisation.

Cyber Essentials is based upon an online selfassessment tool. Cyber Essentials Plus is more demanding and requires an additional series of vulnerability tests e.g. PEN (penetration) testing.

Features and Benefits

The guide offers five technical controls explaining how to:

- secure your internet connection
- secure your devices and software
- control access to your data and services
- protect from viruses and other malware
- keep your devices and software up to date

What the Alcumus ISOQAR experts say:

"Cyber Essentials is quite basic. That said, for small businesses, it's an excellent first step in ensuring you have the essentials in place to provide at least a minimum level of security. In fact the government often insists upon it if you are bidding for government contracts. It's recommended but not the total answer, especially for larger organisations."

HELEN JONES, MD, ALCUMUS ISOQAR

BS 10012 - Personal Information Management

Overview

This system creates a framework for an organisation to lead on not just the technical issues but also the cultural and behavioural aspects of the approach to cyber security.

Features and Benefits

- Make informed investment decisions regarding cyber security
- Improve effectiveness
- Identify and mitigate cyber security risk in the organisation

What the Alcumus ISOQAR experts say:

"It's not an ISO standard and that's perhaps one of the reasons it isn't widely adopted. It's more focused on outcomes, so isn't quite as practically useful as other standards. It is however useful as a tool to assess the performance of security initiatives at a broad level. I would recommend that organisations consider this once they have achieved the holy trinity of ISO 27001, ISO 20000 and ISO 22301."

KEVIN GROOM, LEAD AUDITOR, ALCUMUS ISOQAR

Part 3
How safe is your organisation?

Questions to ask yourself
Your organisation's management of cyber security is not something that can readily be assessed in a simple checklist. However, there are questions you can ask yourself about your overall approach to encourage you to think about your organisational preparedness, resilience and ability to bounce back in the event of a cyber attack.

- [ ] Do you have a board member or trustee with responsibility for cyber security?
- [ ] Is the board member appropriately and regularly briefed?
- [ ] Is cyber security a standing agenda item at board level?
- [ ] Do you have a formal policy?
- [ ] Do you have an identified budget for cyber security?
- [ ] Do you have appropriately qualified staff (or an outsourced supplier) to manage cyber security and do you/they have a training plan to keep skills up to date?
- [ ] Do you have a training plan for all staff to ensure they are regularly briefed?
- [ ] Have you identified your key information assets and assessed their vulnerability to attack?
- [ ] Have you performed a risk management analysis to establish the impact of an attack on your organisation (including operational consequences, damage to reputation, share price etc.)?
- [ ] Do you regularly review who may be targeting your company, their methods and their motivations?
- [ ] Does your staff handbook make it clear what the expectations of staff are and that breaches could result in disciplinary action?
- [ ] Do you have a BYOD (Bring Your Own Device) policy that sets out rules for staff using their own devices?
- [ ] Do you have robust, third party certified management systems in place?

If your answer to any of the above questions is 'No', then you should act now.

Part 4
Glossary of Cyber Attack Terminology

Bot / Botnet
A computer connected to the internet that has been compromised with malicious code and is under the control of a remote administrator. A 'botnet' is a collection of similarly compromised computers.

Bug
A relatively small and unexpected defect in an information system or device.

Cyber Attack
An attempt to gain unauthorised access to systems and data or to cause damage.

Cyber Security
The convergence of people, processes and technology to protect the integrity, confidentiality and availability of hardware, networks, software and data from attack, damage or unauthorised access.

Data breach/loss/spill/theft/ leak/ exfiltration
The loss or theft of information to a party usually outside the organisation who has gained unauthorised access.

DoS (Denial of Service) Attack
Where the perpetrator prevents a user from accessing a computer network.

DDoS (Distributed Denial of Service) Attack
Where multiple compromised systems (such as a botnet or those infected with a Trojan) target a single system resulting in a Denial of Service.

Keylogger
Software (or possibly hardware) that secretly monitors keystrokes on keyboards.

Macro Virus
Malicious code that attaches itself to documents and uses the macro programming of software (such as Excel or Word) to execute a sequence of actions.

Malicious Applet
A small application program usually inadvertently downloaded which performs unauthorised functions.

Malicious Code
Code within software that results in damage to the system or security breaches.

Malicious Logic
Software, firmware or hardware that is inserted in a system to perform unauthorised functions.

Malware
Catch-all term for malicious software that performs unauthorised operations in a system.

Phishing
Attempts to fraudulently collect sensitive information such as passwords, credit card details through emails, telephone and text messages posing as legitimate sources.

Ransomware
A type of malicious software that threatens to publish the victim's data or block access unless a ransom is paid.

Spam

The abuse of email and other electronic communication systems to indiscriminately bulk broadcast unsolicited messages.

Spoofing

Various techniques from malicious parties using fake sending addresses (and IP addresses) to indicate that the message is from a trusted host to deceive computer systems or users and gain unauthorised access.

Spyware

A form of malware that is secretly installed without the user's knowledge and captures sensitive details such as passwords and bank details.

Trojan horse

A program that is disguised as legitimate software by offering useful functions but also has malicious, hidden functions to bypass security and gain unauthorised access.

Virus

A program that can infect a computer without the user's permission or knowledge and, with a host program, infect another computer.

Worm

Similar to a virus but which is capable of replicating itself and spreading to other computers, in contrast to viruses which require a host program or human intervention to propagate.

Part 5
References and Resources

Cyber Security Breaches Survey 2018.
(Department for Digital, Culture, Media and Sport, 2018)

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018

Wholesale Banks and Asset Management Cyber Multi-Firm Review Findings. (Financial Conduct Authority, 2018)

https://www.fca.org.uk/publications/multi-firm-reviews/wholesale-banks-asset-management-cyber-multi-firm-review-findings

A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate.
(Ioannis Agrafiotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, David Upton, 2018)

https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288

10 Steps to Cyber Security. (National Cyber Security Centre)

https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

Adhering to Data Protection Legislation With BS 10012:2017.
(Tom Martin Ball, 2018)

https://www.alcumusgroup.com/blog/november-2018/data-protection-legislation-bs-10012-2017

Cyber Crime Costs Projected to Reach $2 Trillion by 2019.
(Steve Morgan, Forbes, 2017).

https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019

About Alcumus ISOQAR

We help organisations create better workplaces through a huge range of common and sector-specific standards and compliance assessments, allowing them to demonstrate to their customers, competitors, suppliers and staff, that they are committed to being the best that they can by minimising risk, delivering change, driving improvement and winning more work.

As one of the UK's largest UKAS accredited certification bodies we can audit, certify and train organisations across multiple sectors.

We work worldwide, so we can help businesses gain a competitive edge anywhere they need us.

About Alcumus

Alcumus is a leading provider of software-led risk management solutions providing clients with advice, expertise and support to help them identify and mitigate risks, navigate compliance and keep people safe. It supports both UK and International clients – many of whom are on the FTSE 100 index - with a wide range of risk management services. This includes products across Supply Chain Management, EHSQ Software, UKAS Accredited Certification and HR and H&S support services.

Our people are at the heart of our business, building strong relationships with our clients to understand their needs, minimise risks and navigate compliance through our in-depth knowledge of your sector, regulations and challenges.

E: info@alcumus.com
T: 0333 920 8824
W: alcumus.com

Alcumus®
Safer, Healthier, Stronger