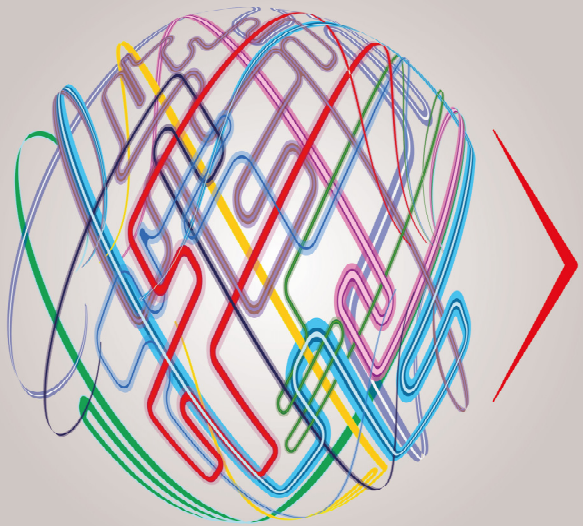
ICAEW KNOW-HOW
TECH FACULTY



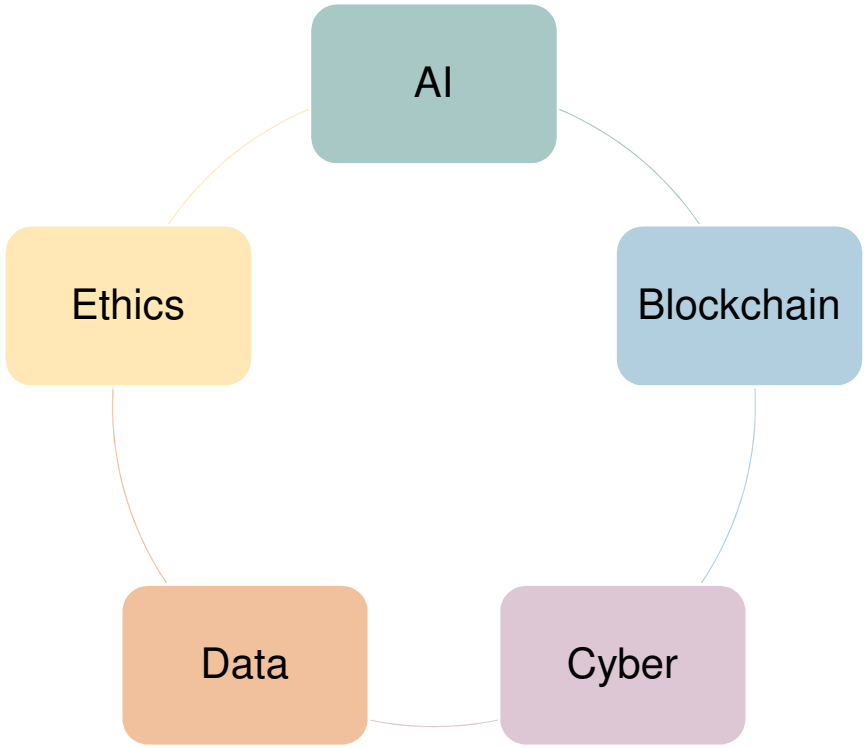
Five questions boards should ask about cyber security

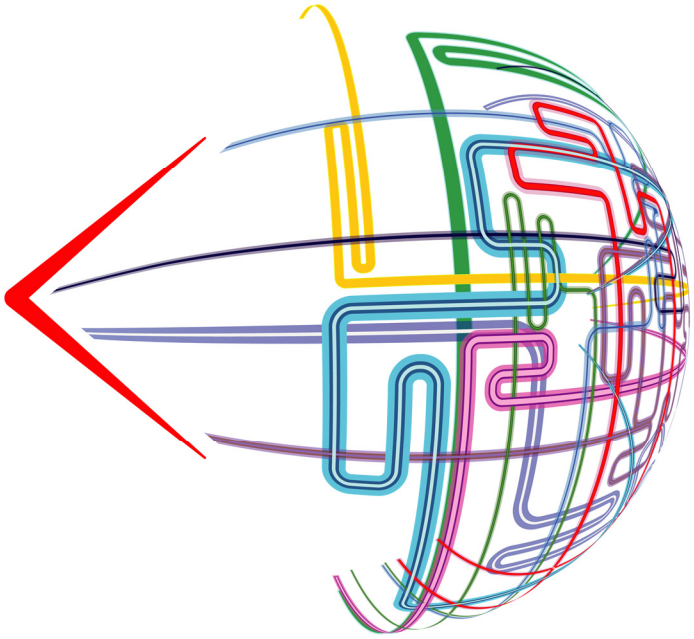
26 JUNE 2020

NCSC

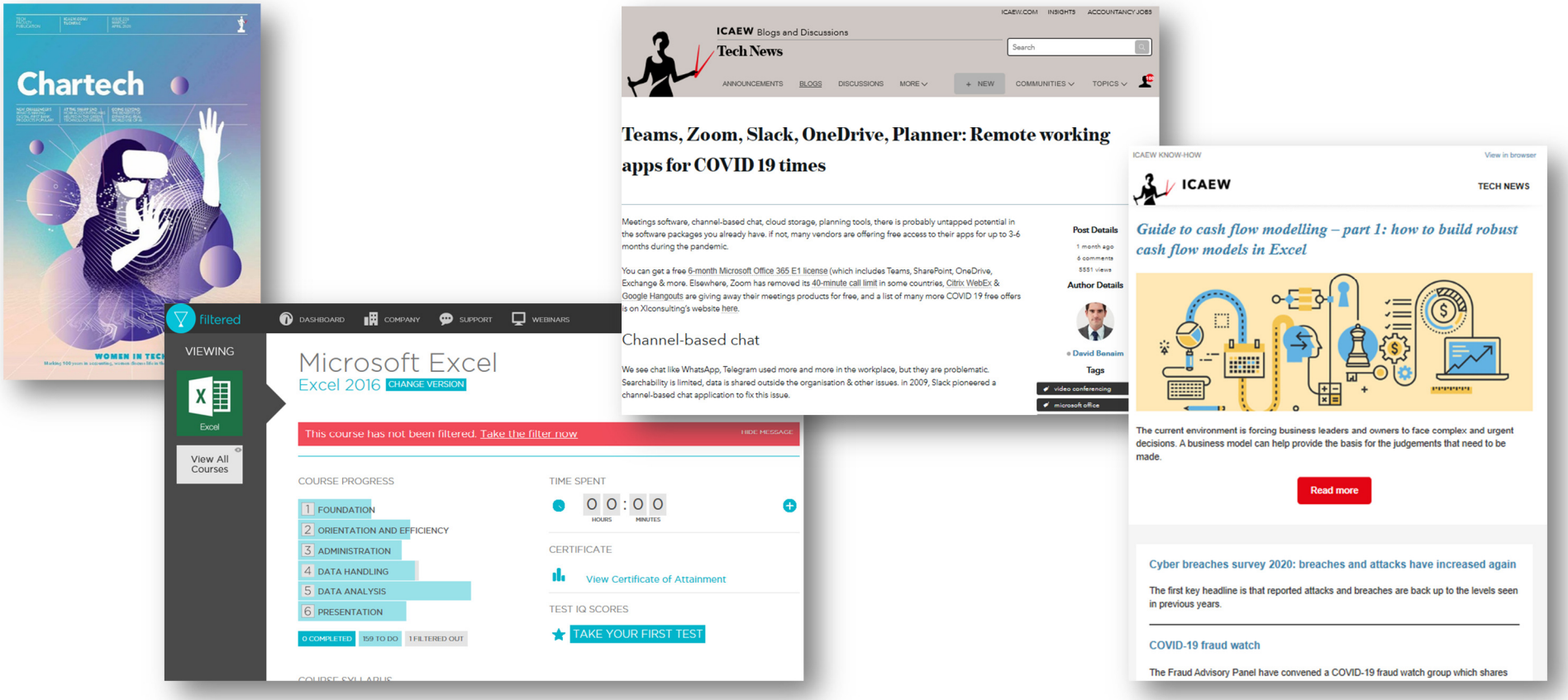
GREG SWIFT, GRANT THORNTON UK

ICAEW Tech Faculty – insight and guidance on tech





ICAEW Tech Faculty – insight and guidance on tech



icaew.com/jointechfac

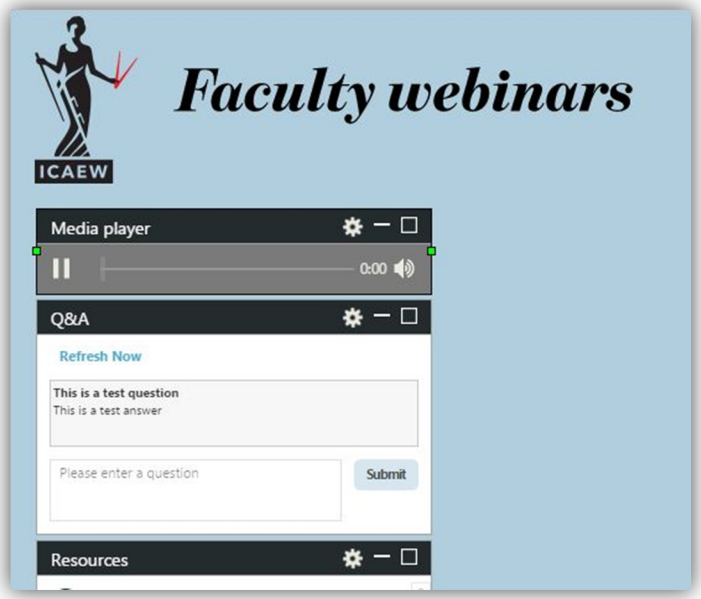
Today's presenters

National Cyber Security Centre
a part of GCHQ

Representative from NCSC

Greg Swift
National Director for Information Systems, Grant Thornton UK LLP

Ask a question or download resources



Audio problems?
ENSURE YOUR VOLUME IS TURNED ON
If you experience poor sound quality you may benefit from refreshing your page

Ask a question
Type your question into the question box then click submit.

National Cyber Security Centre
a part of GCHQ

Helping board members get to grips with cyber security:

Introducing The Cyber Security Toolkit for Boards

Hannah H
NCSC
Hannah.h@ncsc.gov.uk
26th June 2020

National Cyber Security Centre
a part of GCHQ

So what is cyber security?

Cyber security is how individuals and organisations reduce the risk of cyber attack.

Cyber security's core function is to protect the **devices** we all use (smartphones, laptops, tablets and computers), and the **services** we access - both online and at work - from **theft** or **damage** via electronic means

It's also about preventing **unauthorised access** to the vast amounts of personal information we store on these devices and online.

National Cyber Security Centre
a part of GCHQ

The NCSC: Helping to make the UK the safest place to live and work online

- **understands** cyber security, and distils this knowledge into practical guidance
- **responds** to cyber security incidents to reduce the harm they cause to organisations and the wider UK
- uses industry and academic expertise to **nurture** the UK's cyber security capability
- **reduces** risks to the UK by securing public and private sector networks

National Cyber Security Centre
a part of GCHQ

Why does cyber security matter to boards?

- Because cyber security is **a board level responsibility**

- Why?

1. Nearly all organisations depend on digital technology to **function**
2. The potential **cost** of remedying a cyber incident can be significant
3. The risk of **reputational damage**

Cyber security is therefore **essential** and needs to be understood as an **enabler**

National Cyber Security Centre
a part of GCHQ

Cyber security myths

1. Cyber security is too complex for me to understand

2. Cyber attacks are sophisticated – we can't stop them anyway

3. Cyber attacks are highly targeted – our organisation is unlikely to be interesting / valuable enough

National Cyber Security Centre
a part of GCHQ

Introducing the Cyber Security Toolkit for Boards

- **Guidance** to support board members **get up to speed** on a topic they may not be familiar with
- Designed primarily for **corporate** boards - but messages relevant to any board in any sector
- Aims to encourage crucial conversations to take place between the board and its technical experts
- Available online - pdf can be downloaded for those who prefer hard copy

National Cyber Security Centre
a part of GCHQ

Resources designed to encourage essential cyber security discussions between the Board and their technical experts.

IN THIS GUIDANCE

National Cyber Security Centre
a part of GCHQ

Toolkit structure

1. Introduction to cyber security

2. Nine core modules introduce key topics

Appendices with reference material:

- Cyber security regulation
- Help with incidents
- About the NCSC

National Cyber Security Centre
a part of GCHQ

Toolkit modules

1. Embedding cyber-security into organisational objectives
2. Growing cyber security expertise
3. Developing a positive cyber security culture
4. Establishing your baseline and identifying what you care about most
5. Understanding the cyber security threat
6. Risk management for cyber security
7. Implementing effective cyber security measures
8. Collaborating with suppliers and partners
9. Planning your response to cyber incidents

National Cyber Security Centre
a part of GCHQ

The questions

Each module concludes with questions

Designed to *apply* the information discussed and to help prompt discussion at board level

Questions are asked of three different audiences:

1. individual **board members**
2. the **board** - more strategic issues
3. the **organisation** – what board members might want to seek **assurance** on

Questions don't always have simple answers

Testing shows the questions are the most popular part of the toolkit

National Cyber Security Centre
a part of GCHQ

9 Planning your response to cyber incidents

Cyber incidents can have a huge impact on an organisation in terms of cost, productivity and reputation. Being prepared to detect and quickly respond to incidents will help to prevent the attacker from inflicting further damage, so reducing the financial and operational impact. Handling the incident effectively whilst in the media spotlight will help to reduce the impact on your reputation.

Questions for board members

Q1

Do I understand my role during an incident and have I had training to equip me?

Consider:

- Do I have the understanding required to make decisions potentially out of hours and under time pressure?
- Do I need training to support my specific role in an incident, e.g. understanding relevant regulation, or dealing with the media?

Questions for the board

Q2

Do we know who leads on an incident and who has the authority to take any decisions?

This will depend on your organisational structure. Responsibility might sit with one member of the board, or one of the executives, or it might be divided out across different roles.

Ideally you should:

- Specify exactly who is able to take decisions on which aspects of incident management
- Have back-up plans in place if those decision makers are unable to fulfil that duty (for example, out of hours)
- Test this decision-making process, with a focus on potential areas of overlapping responsibility.

Questions for the organisation

Q3

Do we have an incident management plan, and how do we ensure it is effective for cyber incidents?

A basic plan should include:

- Identifying the key contacts (incident response team or provider, senior management, legal, PR, and HR contacts, insurance providers etc).
- Clear escalation routes (for example to senior management) and defined processes for critical decisions.
- Clear allocation of responsibility (specifically whether this is for normal working hours or 24/7).
- Basic flowchart or process for full incident lifecycle.
- At least one conference number which is available for urgent incident calls.
- Guidance on regulatory requirements such as when incidents need to be reported and when to engage legal support.
- Contingency measures for critical functions.

Q4

How would we know when an incident occurred?

This incorporates two aspects; what are the triggers that can tell us an incident has happened, and how do we then share that information within the organisation?

When considering what might trigger an incident, you need to consider:

- What monitoring is in place around critical assets (like personal data) that would have an impact if compromised, lost or changed?
- Who examines the logs and are they sufficiently trained to identify anomalous activity?
- What reporting mechanisms are there for staff to report any suspicious activity?
- Are the thresholds for alerts set to the right level – are they low enough to give suitable warning of potential incidents and high enough that the team dealing with them are not overloaded by irrelevant information?

When considering how an incident will be communicated internally, consider:

- What constitutes an incident?
- Who has the authority to make that decision?
- Who needs to know the details of the incident?
- Has the board explicitly conveyed the threshold for when it wants to be informed of an incident?

9 Planning your response to cyber incidents (cont.)

Questions for the organisation

Q5

Do we know where to go for help in an incident?

This might include:

- Incident response providers (you might want to consider NCSC **Certified Incident Response**[6] companies)
- NCSC **Incident Management**[7] team, or if you think you have been the victim of online fraud, Action Fraud[8].
- Intelligence sharing groups, for details of other companies experiencing the same incident: for example, you might be a member of **CISP**[9], the NCSC's Cyber Security Information Sharing Partnership.

Q6

How do we learn from incidents and near misses?

It's important to learn lessons from incidents as well as from 'near-misses'. These will give you valuable insight into the threat you're facing, the effectiveness of your defence, and potential issues with your policies or culture. A good organisation will use this insight to respond better to future incidents, and not seek to apportion blame.

The board may decide it doesn't need to know the details of every incident, just the most significant lessons learned from the incidents experienced.

6 https://www.ncsc.gov.uk/information/cir-cyber-incident-response

7 https://www.ncsc.gov.uk/section/about-ncsc/incident-management

8 https://www.actionfraud.police.uk/

9 https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

National Cyber Security Centre
a part of GCHQ

Cyber security toolkit for boards: Five Starter Questions

Q1: How do we defend our organisation against **phishing** attacks?

Q2. How does our organisation control the use of **privileged IT accounts**?

Q3. How do we ensure that our **software and devices are up to date**?

Q4. How do we make sure our **partners and suppliers** protect the information we share with them?

Q5. What **authentication methods** are used to control access to systems and data?

National Cyber Security Centre
a part of GCHQ

Coming soon…

Podcasts and videos for each module

New content: researching additional topics

Developing training packages

Responding to feedback: Hannah.h@ncsc.gov.uk

Grant Thornton
An instinct for growth™

Cyber Security Toolkit for Boards

Greg Swift
National Director
Information Systems

Cyber Security Toolkit for Boards

As with many organisations Grant Thornton UK LLP relies on its digital technology to function. This has been critically positively demonstrated in the current Corona Virus pandemic. Good cyber security protects that ability to function, and ensures that we can exploit the opportunities that technology brings.

The National Cyber Security Centre (NCSC) has published its “Cyber Security Toolkit for Boards” to enable Senior Management Teams to have informed discussions with its Subject Matter Experts (SME’s), service organisations and the wider public. As part of the Toolkit the NCSC have published five questions to act as a primer for this expected dialogue.

In expectation of these questions being asked of the Grant Thornton UK Senior Leadership Team (SLT) by regulators or clients we instigated a dialogue and approach adopted in the subsequent slides, together with the controls in place within our organisation to respond to them.

A glossary of common terms in Appendix B.

Q1): How do we defend our organisation against phishing attacks?

Phishing describes a type of social engineering where attackers influence users to do 'the wrong thing', such as disclosing information or clicking a bad link. The link could install malware on our system, or direct our people to a fake website that asks for sensitive information (such as logon credentials or bank details).

We filter or block incoming phishing emails using a third party solution, providing Targeted Threat Protection and URL Protection software. This makes an attack less likely to happen and reduces the amount of time spent checking and reporting suspicious emails.

We use a third party solution to ensure incoming email is marked as external. This facility helps our people make better judgements about how they should treat the email, and any requests it makes.

We stop attackers 'spoofing' our emails through the management of controls such as SPF (Sender Policy Framework) and DKIM (Domain-Keys Identified Mail). Additionally, our Anti-Virus software is installed on all assets and is updated automatically when updates are released by the vendor.

We train our people regularly on how to identify phishing emails and provide regular security updates. All our people are required to conduct IT Security training at least three times a year, as minimum.

Q2. How does Grant Thornton control the use of privileged IT accounts?

Privileged accounts such as “Global” and “Domain” administrator have high levels of access to data and functions. If these are compromised an attacker can gain elevated access to the network and cause significant damage and disruption.

We use 'least privilege' when implementing admin accounts. The IS Team, and other people with elevated levels of access, are provided with enough system privileges and rights required to perform their role. System privileges are carefully controlled, reviewed on a regular basis and revoked as people leave or change roles within the firm.

Additionally, multi factor authentication (MFA) is applied to account credentials

We have a strong account creation and management process that is linked to our ISO20000 Service Management certification.

Q3. How do we ensure that our software and devices are up to date?

Patching is the process of applying the updates that suppliers and vendors regularly issue to all hardware and software. From servers and routers to smartphones and laptops, patching enhances functionality and also fixes security bugs or vulnerabilities.

We have defined processes, reviewed and approved through our ISO2000 certification, to identify, rank, and remediate any vulnerabilities within our network. Critical security updates are applied as soon as practicable, and we conduct monthly vulnerability scanning and annual penetration tests, to identify and remediate vulnerabilities. Additionally, we utilise the 'Bitsight' continuous monitoring service to identify any threats to our network perimeter.

We monitor the versioning and support of all our software and implement "technical refresh" plans for any resource that is nearing the end of its support. All IS assets are managed and monitored through our IS team processes and strategic plans ensure that appropriate support is in place.

We utilise 3rd party and cloud services as part of our strategic service delivery. All service providers are subject to our appointment and security validation processes.

Q4. How do we make sure our partners and suppliers protect the information we share with them?

Service providers, such as cloud data hosting, are an extended part of our infrastructure and must be carefully selected and managed to ensure that data security is maintained.

We conduct reviews of all our service partners through the use of the IT Security Questionnaire process prior to appointment. All suppliers must meet a “de minimis” standard of ISO27001, Cyber Essentials Plus or similar and be able to prove the maturity of their IT Security framework.

Service partner access to the Grant Thornton network is limited to the minimum required and any variation is subject to review and control.

Suppliers are required as part of their contract to notify Grant Thornton as soon as possible of any security issues. Upon notification an assessment will be made of the risk and appropriate steps taken (e.g. suspending access to the network) to mitigate any risk whilst maintain service operability.

Q5. What authentication methods are used to control access to systems and data?

All of our people must “authenticate” (log-in) to the Grant Thornton network, either in the office or via the Virtual Private Network (VPN) when using their GTUK supplied laptop remotely to access our data and services. That process must be secure but not overly onerous to provide the optimum level of practicality and security.

We use Multi Factor Authentication (MFA) to authenticate all users to the network. Additionally, all users receive mandatory security training which must be completed.

We have defined a Grant Thornton Password policy, detailing best practice, as part of the IT Security Policy framework. All users must attest that they have read and will comply with the policy as part of the Annual Declarations process.

Conclusion

We have implemented strong technical controls to protect ourselves and our clients data. In addition to those mentioned in the previous slides;

Our Security Operations Centre, operated in conjunction with the Cyber Security Services Team, utilises Security Incident & Event Management (SIEM) software to provide a 24/7 monitoring and threat response capability.

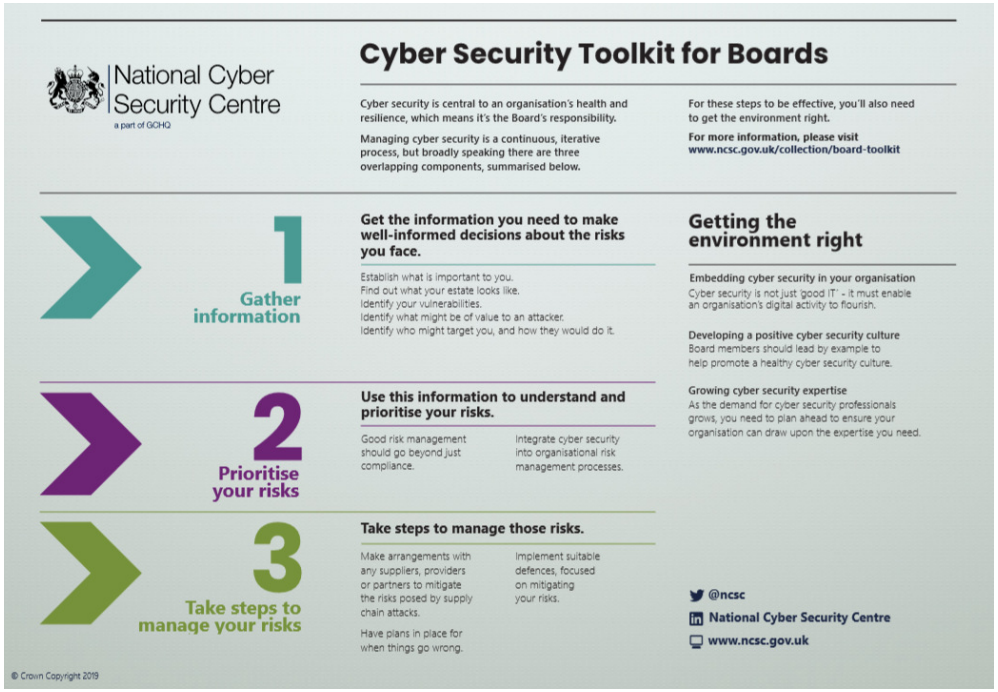
We have implemented Azure Information Protection, a function of the Microsoft Office 365 platform, to provide data classification and leakage prevention capability.

We support a comprehensive cyber security training programme that is available through the Business School, and monitored through the firm-wide reporting.

Our commitment to Information Security is evidenced through our ISO27001 and Cyber Essentials Plus certifications which we have held for the past 5 years.

We also take an active lead in working with our International organisation to develop security policies and assurance processes

Appendix A Cyber Security Infographic



Link to NCSC Board Toolkit - https://www.ncsc.gov.uk/collection/board-toolkit

Appendix B Glossary

AIP	Azure Information Protection - cloud-based solution for classifying and protecting documents and emails by applying labels
BitSight	Continuous scanning tool used by Grant Thornton International Limited to monitor the GTUK network and compare to other member firms
ISMS	Information Security Management System – management framework for IT Security function within Grant Thornton, requirement of ISO27001 certification
NCSC	National Cyber Security Centre – central Government IT and information security organisation
Office 365	Microsoft cloud based platform for Office, email and data processing
SIEM	Security Incident & Event Management – application for collating, analysing and reporting security alerts from across the network
SOC	Security Operations Centre – Grant Thornton Cyber Security Services partner that operates security tools and services on a 24/7 basis to alert the of any problems or incidents. Also extends to Threat Analysis

grantthornton.co.uk

Questions

Thank you for attending

Please take the time to fill out our short survey

Contact the Tech Faculty

Phone: +44 (0)20 7920 8526

Email: techfac@icaew.com

Web: icaew.com/techfac

This webinar is presented by the Tech Faculty. Tech Faculty membership gives you access to exclusive premium resources including our regular magazine, webinars, discount on events and conferences and extensive online resources to support your career.

For more information about faculty membership and our latest joining offers, please visit icaew.com/jointechfac or for more information about Faculties Online, please visit icaew.com/subscribefo.