THE CYBER SECURITY BOARD TOOLKIT[1]

GSC:	OFFICIAL	Version:	1-0
Owner:	Gary Brailsford-Hart Director of Information (CISO)	Date:	May 2019

[1] Content drafted and adapted from the NCSC

Table of Contents

Cyber Security Board Toolkit

About the Board Toolkit

The Board Toolkit is relevant for anyone who is accountable for an organisation in any sector. That could be a Board of Directors, a Board of Governors or a Board of Trustees. Additionally, technical staff and security practitioners may find it a useful summary of NCSC guidance, and can use the questions within the toolkit to frame discussions with the Board.

Scope and structure

Good cyber security is all about managing risks. The process for improving and governing cyber security will be similar to the process we use for other organisational risks. It is a continuous, iterative process and comprises three overlapping components, summarised below:

1. **Get the information we need to make well informed decisions on the risks we face.**
2. **Use this information to understand and prioritise our risks.**
3. **Take steps to manage those risks.**

Crucially in order for these steps to be effective, we need to **get the environment right,** this is broken down into three sections that explain how we do this.

Getting the Environment Right through:

A. Embedding cyber security in the City of London

B. Growing cyber security expertise

C. Developing a positive cyber security culture

Introduction to cyber security for Board members

As a Board member you need to understand enough about cyber security so you can have a fluent conversation with your experts.

What is cyber security?

Cyber Security is the protection of devices, services and networks - and the information on them - from theft or damage via electronic means.

What do I need to know about cyber security?

There are three common myths concerning cyber security. Understanding why they're incorrect will help you understand some key aspects of cyber security.

Myth #1: Cyber is complex, I won't understand it.

Reality: You don't need to be a technical expert to make an informed cyber security decision.

We all make security decisions every day (whether to put the alarm on, for example) without necessarily knowing how the alarm works. Boards regularly make financial or risk decisions without needing to know the details of every account or invoice. The Board should rely on its cyber security experts to provide **insight**, so that **the Board** can make informed decisions about cyber security.

Myth #2: Cyber attacks are sophisticated, I can't do anything to stop them.

Reality: Taking a methodical approach to cyber security and enacting relatively small changes can greatly reduce the risk to the City of London.

The vast majority of attacks are still based upon well-known techniques (such as phishing emails) which can be defended against. Some threats can be very sophisticated, using advanced methods to break into extremely well defended networks, but we normally only see that level of commitment and expertise in attacks by nation states. Most organisations are unlikely to be a target for a sustained effort of this type, and even those that are will find that even the most sophisticated attacker will start with the simplest and cheapest option, so as not to expose their advanced methods.

Myth #3: Cyber attacks are targeted, I'm not at risk.

Reality: Many cyber attacks are opportunistic and any organisation could be impacted by these untargeted attacks.

The majority of cyber attacks are untargeted and opportunistic in nature, with the attacker hoping to take advantage of a weakness (or vulnerability) in a system, without any regard for who that system belongs to. These can be just as damaging as

targeted attacks; the impact of WannaCry on global organisations - from shipping to the NHS - being a good example. If you're connected to the internet then you are exposed to this risk. This trend of untargeted attacks is unlikely to change because every organisation - including yours - will have value to an attacker, even if that is simply the money you might pay in a ransomware attack.

How do cyber attacks work?

A good way to increase your understanding of cyber security is to review examples of how cyber attacks work, and what actions organisations take to mitigate them. Reviewing incidents that have occurred within the City of London is a good place to start.

In general, cyber attacks have 4 stages:

- **Survey** - investigating and analysing available information about the target in order to identify potential vulnerabilities.
- **Delivery** - getting to the point in a system where you have an initial foothold in the system.
- **Breach** - exploiting the vulnerability/vulnerabilities to gain some form of unauthorised access.
- **Affect** - carrying out activities within a system that achieve the attacker's goal.

Defending against cyber attacks

The key thing to understand about cyber security defences is that they need to be layered and include a range of measures, from technology solutions to user education to effective policies. The infographic below gives examples of defences that will help the City of London to combat common cyber attacks. Our section on Implementing effective cyber security measures provides further detail and questions that you can use to understand more about our own organisation's defences.

As a Board member, you will be targeted

Senior executives or stakeholders in organisations are often the target of cyber attack, because of their access to valuable **assets** (usually money and information) and also their **influence** within the organisation.

Attackers may try and directly target our IT accounts, or they may try and impersonate you by using a convincing looking fake email address, click here to see an example. Once they have the ability to impersonate you, a typical next step is to send requests to transfer money that may not follow due process. These attacks are low cost and often successful as they exploit the reluctance of staff to challenge a non-standard request from someone higher up in the organisation.

Good cyber security awareness throughout the City of London, security policies that are fit for purpose and easy reporting processes will all help to mitigate this risk. It is also critical that Board members understand and follow the organisational security

policies, so that when an impersonator tries to circumvent them, staff can identify that something is unusual.

You should also consider how information about you that is publicly available could assist an attacker who is trying to impersonate you.

A.

Embedding cyber security into our structure and objectives

Cyber security is not just 'good IT' - it must enable the City of London digital activity to flourish.

Integrate cyber security into the City of London's objectives and risks

There's two reasons why this is so important.

Firstly, cyber security impacts on every aspect of the City of London. Therefore to manage it properly it must be integrated into organisational risk management and decision making. For example:

- Operational risk will likely be underpinned by cyber security because of the reliance on the security of digital services that we use (email services, bespoke software, etc.)
- Some legal risk will be tied in with cyber security risk (such as contractual requirements to protect data or partnerships, regulatory requirements to handle data in particular ways)
- Financial risk is impacted by cyber security (such as money lost through fraud enabled by cyber, revenue lost when services are taken offline by cyber attack)
- Good cyber security will also allow us to take some risk in using new technology to innovate. An overly cautious approach to risk can lead to missed business opportunities or additional (and unnecessary) costs.

Secondly, cyber security needs to be integrated for it to be successful. Good cyber security isn't just about having good technology, it's about people having a good relationship with security, and having the right processes in place across the organisation to manage it.

For example, in order to protect against an attacker accessing sensitive data (whilst ensuring that only those with a current and valid requirement can see it), we will need:

- a good technical solution to storing the data
- appropriate training for staff handling the data
- a process around managing the movement of staff, aligned with access management

Engaging with our experts

Consider whether our reporting structure enables the Board to have the engagement with cyber security that it needs. If the CISO reports to an intermediary to the Board who has a focus on only one aspect - be that finance or legal or technology - this can potentially hinder the ability for the Board to see cyber security's wider implications. In the majority of FTSE350 organisations the CISO now reports directly to the Board.

A good place to start on improving cyber security in the City of London is to consider the communication between experts and members of the Board. Getting the structure right can help, but we also often see a reluctance from both parties to engage, because:

- technical staff think that the Board won't understand them
- the Board think that the technical staff are unable to explain the issues in the context of the strategic aims of the organisation

Improving the communication between these two groups requires effort from both sides:

- **Boards** need a good enough understanding of cyber security that they can understand how cyber security supports their overall organisational objectives
- **technical staff** need to appreciate that communication of cyber risk is a core component of their job, and ensure they understand their role in contributing to the organisation's objectives

What does good look like?

The following questions are designed to generate productive discussions between the board and the security team. The aim is to identify what constitutes 'good' cyber security in terms of **embedding cyber security into our structure and objectives**.

Q1. As a Board, do we understand how cyber security impacts upon our individual and collective responsibilities?
Q2. As an organisation, who currently has responsibility for cyber security?
Q3. As a Board, how do we assure ourselves that the City of London's cyber security measures are effective?
Q4. As an organisation, do we have a process that ensures cyber risk is integrated with business risk?

B.

Growing Cyber Security Expertise

As the demand for cyber security professionals grows, we need to plan ahead to ensure the City of London can draw upon expertise.

Cyber skills are already in high demand, and the Global Information Security Workforce study estimates that by 2022 there will a shortfall of 350,000 appropriately trained and experienced individuals in Europe. Organisations must take steps now to ensure they can draw on cyber security expertise in the future.

Given the lack of suitably skilled individuals and an increasing reliance on digital services that need to be secured, organisations that do not embrace cyber security will soon fall behind.

1. Work out what specific cyber security expertise we need.
2. Establish how urgently we need these skills.
3. Consider how we might recognise professional cyber security skills.

Make the best use of the skills we have

The best way to make use of the skills we have is to identify and focus on the things that are unique to us (or the things that only people within the City of London are most qualified to do). This can be enabled by making use of established, commodity technologies. For example we might choose to allow cloud vendors to build and secure our infrastructure, which frees our experts to spend time exploiting the unique insight they have into our organistion.

Build our best workforce: equal, diverse and inclusive

Due to the cyber security skills shortfall, the City of London must draw and nurture talent from the largest possible pool. The cyber security industry is subject to the same skills challenges as all technology-focused industries. Organisations may find it hard to recruit and retain high-calibre staff from all demographic groups. In fact there are many talented women and minorities working in cyber security, but they are often less visible. They may experience hostile working environments that slow or stop their career, or avoid the industry altogether. Working together to overcome these challenges will give the City of London a competitive edge.

Look beyond technical skills

When designing job roles and desired candidate profiles, particularly at entry level, be imaginative. Protecting the City of London relies on bringing together many different skills, technical and non-technical, to deliver security that aligns with the organisation's objectives. Recruit for broader business skills, aspiration and potential as much as for current technical skills.

Look after our existing talent

When trying to make the City of London more diverse and inclusive, we often focus on bringing in **new** talent, while ignoring the issues that prevent our **current** staff staying and thriving once they are in. The talent available may be beyond our own direct control, but we **can** control how much cyber security talent we lose because of difficult policies and processes, and unwelcoming workplace cultures. As much as strong *security* cultures, we should focus on fully *inclusive* workplace cultures.

Train, buy-in, or develop for the future

Broadly there are 3 options to increase cyber expertise within the City of London.

Train existing staff

Don't just consider the staff who are already in security-related jobs. The NCSC has had huge success training staff from a variety of backgrounds, skills and experience. After all, there are many different aspects to cyber security and someone who is expert at designing a network architecture might have a very different skill set to the person working with staff to make sure security policies are practical and effective.

Depending on the City of London's needs and our staff, training could take the form of on-the-job training, professional qualifications or placements. Do remember that developing cyber security expertise is no different to many other professional areas: staff will require continuous investment, training and development opportunities to hone their expertise and also to keep up with changes in the industry.

- There are many companies who offer cyber security training.
- We could also offer time for study on an NCSC certified degree, or time for a placement on the Industry100 programme.

Buy in expertise

There are several complementary routes available for introducing external expertise. A larger organisation will probably take advantage of all of them.

1. Recruit a skilled non-executive director to the Board.
2. Employ a consultant to provide specific cyber security advice.
3. Identify specific cyber security services which can be fulfilled by a 3rd party.
4. Recruit employees who already have the skills we need.

Recruiting expertise externally can provide a quick solution where there's a lack of specialised cyber security knowledge. However, be sure to identify someone who can adapt cyber security principles to **the City of London**. 'One size fits all' is rarely applicable in terms of cyber security, and someone who just applies an out-of-the-box solution may not be significantly improving our cyber resilience.

Develop future staff: sponsorship, apprenticeships and work experience

Supporting young people to pursue an education in cyber security can be a brilliant way of ensuring a future pipeline of employees with the right skills. There are many schemes aimed at school and university-age students and almost all of them involve some industry participation or support, including apprenticeships, site visits and speaker opportunities.

What does good look like?

The following questions are designed to generate productive discussions between the board and the security team. The aim is to identify what constitutes 'good' cyber security in terms of **growing cyber security expertise**.

Q1. As an organisation, what cyber expertise do we need, and what do we have?
Q2. As an organisation, what is our plan to develop what we don't have?
Q3. As a Board member, do I have the right level of expertise to be accountable for cyber security decisions?
Q4. As an organisation, are we building an equal, diverse and inclusive workforce to tackle our cyber security skills challenges?

C.

Developing a positive cyber security culture

Board members should lead by example to help promote a healthy cyber security culture.

Establishing and maintaining a healthy culture, in any part of the business, is about putting people at the heart of structures and policies. However, when it comes to cyber security, there is sometimes a tendency to focus almost exclusively on the technical issues and to overlook the needs of people and how they really work.

This rarely results in success. We know, for example, that when official policy makes it hard for someone to do their job, or when a policy is no longer practical, that people find workarounds and 'unofficial' ways of carrying out particular tasks.

Without a healthy security culture staff won't engage with cyber security so we won't know about these workarounds or unofficial approaches. So not only will we have an inaccurate picture of the City of London's cyber security, but we will also miss the opportunity for valuable staff input into how policies or processes could be improved.

The board leading by example

They set the tone when it comes to cyber security. Lead by example and champion cyber security within the City of London.

We often hear stories of senior leaders ignoring security policies and processes, or of asking for 'special treatment' in some way (such as requesting a different device to those issued as standard). This tells everyone else in the organisation that perhaps we don't consider the rules fit for purpose, and/or that it is acceptable to try to bypass them.

If policies *don't* work for you as a Board member (that is, if you find yourself doing something different to get our job done more easily), then there is a good chance they aren't working for others either. If it seems that the policy is having a detrimental effect on the organisation, work with policy makers to adapt it.

Culture takes time and concerted effort to evolve. Don't assume that because the Board has endorsed a security posture that it will automatically cascade down throughout the organisation.

Putting people at the heart of security

Ultimately, the role of security should be **to enable the City of London to achieve its objectives**. It follows that if our cyber security measures aren't working for people, then our security measures aren't working.

Some organisations fall into the trap of treating people as the 'weak link' when it comes to cyber security. This is a mistake. Effective security means balancing all the different components, not expecting humans always to bend to meet the technology. More importantly, the organisation can't function with people, so staff should be supported so they can get their job done as effectively and securely as possible.

Security and leadership need to make the most of what people's behaviour is telling them. Whilst technical monitoring can look for anomalies, people can act as an early-warning system and intuitively spot something that looks unusual. Ensuring staff know who to report any concerns to can save the organisation a huge amount of time and money in the long run. If staff are working around a set procedure, this may highlight a particular policy or process that needs reviewing.

Develop a 'just culture'

Developing a 'just culture' [1] will enable the organisation to have the best interaction with staff about cyber security. Staff are encouraged to speak up and report concerns, appropriate action is taken and nobody seeks to assign blame. This allows staff to focus on bringing the most benefit to the organisation rather than focusing on protecting themselves.

What does good look like?

The following questions are designed to generate productive discussions between the board and the security team. The aim is to identify what constitutes 'good' cyber security in terms of **developing a positive cyber security culture**.

Q1. As a Board member, do I lead by example?
Q2. As an organisation, do we have a good security culture?
Q3. As an organisation, what do we do to encourage a good security culture?

1.

Get the information we need to make well informed decisions on the risks we face

Establishing our baseline and identifying what we care about most

Understanding what technical assets we have, and how they're critical to the City of London's objectives, are both key to effective risk management.

There are two tasks in this section, but we examine them side-by-side as the results of one will impact on the other, and vice versa. The two tasks are:

- working out which components of our 'technical estate' (that is, our systems, data, services and networks) are the most critical to the City of London's objectives
- understanding what our technical estate comprises, so that we can establish a baseline which will inform both our risk assessments and the deployment of our defensive measures

Whilst these two tasks have separate purposes, we will need to have some baseline of our technical estate in order to understand which parts of it are mission critical. At the same time, we will need some way to prioritise which areas to baseline, as doing this for our entire technical estate would be a very resource intensive task.

Work out what we care about the most

As with any other business risks, the City of London will not be able to mitigate **all** cyber security risks at **all** times. So the Board will need to communicate key objectives (it might be 'providing a good service to customers and clients', for example) in order for the technical security experts to focus on protecting the things that ensure these objectives are fulfilled.

The Board should also consider what is most valuable to the organisation. For example, the Board might know that a specific partner is crucial to the organisation and that a compromise of their data would be catastrophic. This should be communicated to technical security teams, so that they can prioritise protecting these 'crown jewels'.

It is **critical** that this is an active and ongoing discussion between Boards and their experts:

- Boards will have business insight that security teams may not have (such as which particular partner relationship must be to be prioritised)
- technical teams will have insight into the enablers for key objectives (such as which networks or systems do particular partners rely upon)

Only by bringing these two **together** can we get a full picture of what is important to protect. Once we have this picture it is likely the Board will still need to prioritise within that list. This understanding will not only help focus the aim of our cyber security, but will also inform the assessment of the threat the City of London might be facing.

> **What are our crown jewels?**
>
> Our crown jewels are the things most valuable to the City of London. They could be valuable because we simply couldn't function without them, or because their compromise would cause reputational damage, or it would incur financial loss. Some examples could be:
>
> - bulk personal data
> - corporate systems
> - our public-facing website
> - operational systems

Work out where we are starting from

This provides information that underpins our risk decisions in two ways.

Firstly, it influences the options we have. Knowing which systems are connected to each other, who and what has access to particular data, and who owns which networks are all critical to setting good defences. This information will also be required in an incident to make an assessment of the damage an attacker could be inflicting, or the impact of any remedial actions we might decide to take.

Secondly, it might influence our risk assessment. Sometimes a risk comes not from a threat to an important asset, but from a vulnerability in the City of London's systems. Many incidents are the result of vulnerabilities in older, legacy systems, and the incidents arise not because the vulnerability can't be defended against, but because the organisation didn't have a good enough understanding of their systems to realise they were exposed.

Understanding the **entirety** of our estate can be a daunting, or impossible, task - especially for organisations whose networks and systems have grown organically - but even a basic understanding will help and a good understanding of our priorities can help focus this task.

Identify critical technical assets

Based on the Board's priorities we need to identify what parts of the technical estate are critical to delivering those top-level objectives. This could be systems, data, networks, services or technologies. For example, maintaining a long term customer base may be a priority objective. There are lots of ways that good cyber security could enable this. It could be:

- securing a customer database to protect their data

- ensuring resilience of the order processing system to ensure deliveries go out on time
- ensuring availability of the website so that customers can contact us easily

It can sometimes be difficult to identify these dependencies as they are such an integral part of our operation that they can be taken for granted, but the questions below can help. Doing this in conjunction with baselining our technical estate will also help to potentially identify assets that we weren't even aware of, and are actually critical to providing certain services.

What does good look like?

The following questions should be used to generate productive discussions between the board and our security team. The aim is to identify what constitutes 'good' cyber security in terms of **establishing our baseline and identifying what we care about most**.

Q1. As an organisation, do we have a clear understanding of how technical systems, processes or assets are contributing to achieving our objectives?
Q2. As a Board, have we clearly communicated our priority objectives and do we have assurance that those priorities guide our cyber security efforts?
Q3. As an organisation, how do we identify and keep track of systems, data or services that we are responsible for?

Understanding the cyber security threat

Organisations face different types of threat, so each Board's approach to cyber security will vary hugely.

The type of threat faced is shaped by the nature of the organisation and the services an organisation provides. For example, the vast majority of organisations won't be targeted specifically by nation states and so may focus on the threats posed by cyber criminals. However, organisations who form part of, or are providing services to, our Critical National Infrastructure and defence sector may be at risk from nation states.

Understanding the threats faced by the City of London, either in its own right or because of who we work with, will enable us to tailor the City of London's approach to cyber security investment accordingly. We need to consciously make the decision about what threat we are trying to defend against, otherwise we risk trying to defend against everything, and doing so ineffectively.

Get an understanding of the threat

An understanding of the cyber security threat landscape will be key to helping the Board make well-informed governance decisions. For example, we may prepare differently for partnering with a company if we know that they provide important products or services to Critical National Infrastructure and therefore may be a target for a nation state. The Board will already have insight into the threats or challenges facing their sector. This should be complemented by an awareness of the motivations of attackers, and a mechanism for staying up to date with key cyber security developments (for example, the growth of ransomware).

Collaborate on security

One of the best sources of information on good practice and relevant threats can be our sector peers. Attackers often target a number of organisations in the same sector in a similar manner. Cultivating these collaborative relationships on security has two major benefits. Firstly, it can help make our own organisation more resilient, through early warning of threats and improved cyber security practice. Secondly, it helps make the sector as a whole more resilient, which can reduce the appeal to potential attackers.

Cyber Security Information Sharing Portal

The NCSC's Cyber Security Information Sharing Partnership provides a secure forum where companies and government can collaborate on threat information. Access to CISP not only provides the opportunity to securely share intelligence with trusted partners in our sector, but also gives access to sensitive threat reports and the full breadth of NCSC advice.

Assess the threat

Working out the 'threat actors' (the groups or individuals capable of carrying out a cyber attack) relevant to the City of London can help us make decisions on what we

are **actively** going to defend against. Whilst investing in a good baseline of cyber security controls will help defend the City of London from the most common threats, implementing effective defences against a more targeted or sustained attack can be costly. So dependent on the likelihood and impact of that threat, we may decide that it is not worth that additional investment.

Ongoing discussion between the Board and experts will help us to prioritise the threats to actively defend against. The experts will have an in-depth understanding of the threat, and the Board will be able to identify the features of the organisation that might make it an attractive target to attackers. It is also critical to have this discussion in advance of any decision that will significantly change the threat profile of the organisation, in order to give technical staff the time to suitably adapt the organisation's cyber security.

> **Working with suppliers and partners**
>
> When assessing the threat, we should consider not only the value that we might have as a standalone organisation, but also the value we may represent as a route into another, possibly larger organisation. For example, we may supply important services to an organisation involved in Critical National Infrastructure, in which case, a nation state may want to attack the City of London in order to access their ultimate target.

Don't underestimate the impact of untargeted attacks

An untargeted attack is where an attacker uses a 'scattergun' approach to reach thousands of potential victims at once, rather than targeting a specific victim. Attackers often use automated, widely available tools that scan public-facing websites for known vulnerabilities. This same tool will then, once a vulnerability has been found, exploit that website automatically, regardless of who it belongs to. This could have just as much impact on the City of London as a targeted attack. A good baseline of basic cyber security controls and processes will protect our system from the majority of these attacks.

Obtain good intelligence - and use it

We will need different types of threat intelligence for different purposes. A good overall threat picture is needed for governance decisions and timely threat intelligence for day-to-day and tactical decisions. Many industry and government partners offer threat intelligence, from annual reports on general trends, right down to highly technical reports on a specific type of malware. We therefore need a mechanism for identifying what intelligence the City of London needs, for what purpose and for sharing that intelligence internally. Critically we then need to **use** that intelligence to inform business decisions, including procurement, outsourcing, training, policy and defence of our networks.

We can also gather threat intelligence internally. We will likely have experience of attacks on our own organisation which can provide strategic insight into activities of

threat actors, as well as tactical details on the methods of the threat actors. These specific details will likely come from logging or monitoring within the City of London.

What does good look like?

The following questions should be used to generate productive discussions with the board and our security team. The aim is to identify what constitutes 'good' cyber security in terms of **understanding the cyber security threat to the City of London**.

Q1. As an organisation, which threats do we assess are relevant to the City of London, and why?
Q2. As an organisation, how do we stay up to date with the cyber threat?
Q3. As an organisation, how do we use threat intelligence to inform business as usual (BAU)?

2.

Using information to understand and prioritise our risks

Risk management for cyber security

Good risk management will help us make better, more informed decisions about our cyber security.

Most organisations will already be taking steps to assess and manage their cyber security risk. However it is worth considering what the **driver** is for that activity. Often, organisations conduct risk management exercises for 'compliance' reasons, which could include:

- obligations from external pressures (such as regulatory requirements)
- customers' demands
- legal constraints

When done for these reasons, there is a danger of risk management becoming a tick-box exercise. This can lead to organisations believing they have *managed* a risk, when in reality they have merely *complied* with a process which may have (albeit unintended) negative consequences.

Compliance and security are **not** the same thing. They may overlap, but compliance with common security standards can coexist with, and mask, very weak security practices. **Good risk management should go beyond just compliance**. Good risk management should give insight into the health of the City of London and identify opportunities and potential issues.

Integrate cyber security into organisational risk management processes

Many of our organisational risks will have a cyber component to them. Cyber security risk should therefore be integrated with our organisational approach to risk management. Dealing with cyber security risk as a standalone topic (or considering it simply in terms of 'IT risk') will make it hard for us to recognise the wider implications of those cyber security risks, or to consider all the other organisational risks that will have an impact on cyber security.

The role of cyber security should be to *support and enable the business,* and it should do this by managing its risks **without** blocking essential activities, or slowing things down, or making the cost of doing business disproportionately expensive.

Don't make reducing risk levels the measure of success

It can be difficult to measure the success of the City of London's cyber security efforts. A typical output of good cyber security is the absence of a failure, which can be hard to measure, and since cyber security is still a relatively new field there aren't yet many established metrics to draw on.

It is common for risk assessments to deliver some kind of assessment level, be that high medium low, or a number, and so it could be tempting to use this as a performance metric for our cyber security efforts. However, they are a poor metric of our internal security efforts as they are influenced by external factors that are outside of our control - factors which change extremely rapidly. New vulnerabilities are being discovered every day and the number of actors seeking to use cyber means to achieve their aims is increasing.

Driving performance through reduction of a number associated with the cyber security risk will likely incentivise risk assessors and reviewers to underestimate the risks, leading to less informed decisions. Some considerations on what 'good metrics' look like is provided in the “Implementing effective cyber security measures” section of this document.

Be realistic about the risks

Similar 'good practice' risk management principles will apply for managing cyber risk as they would for managing any other organisational risk. However there are two things to bear in mind.

Firstly, solutions and technologies in cyber security are advancing so quickly that it is easy to get caught out using outdated assessments of cyber risks. So we may need to review cyber security risks more regularly than other risks.

Secondly, because cyber security is still a relatively new field, the organisation won't have as intuitive an understanding of cyber security risks, as it might for say, financial risk. As new technologies emerge, there might not be a huge evidence base to draw on to form a risk assessment. This is worth bearing in mind when considering the confidence we have in an assessment of cyber security risk, especially if that assessment is going to be directly compared to assessments of more well-established risks.

A good example of this is cloud security. Many organisations are hesitant to use cloud services because they intuitively assume it is high risk, informed mainly by the belief that storing something valuable with a third party is more risky. In reality, the third party (so in this case a cloud service provider) may have better security measures within their data centres than our own on-site storage. So the *overall risk* may actually be lower. A decision to adopt recent technologies - like cloud storage - would need to be based on a comprehensive understanding of all the risks, rather than an intuitive assessment.

What does good look like?

The following questions should be used to generate productive discussions with the Board and our security team. The aim is to identify what constitutes 'good' cyber security in terms of **managing cyber security risk**.

Q1. As an organisation, do we have a process that ensures decision makers are as well informed as possible?
Q2. As an organisation, do we have a process that ensures cyber risk is integrated with business risk?
Q3. As an organisation, do we have an effective and appropriate approach to manage cyber risks?
Q4. As a board, have we clearly set out what types of risks we would be willing to take, and those which are unacceptable?

3.

Take steps to manage those risks

Implementing effective cyber security measures

Put in place defences that will protect our critical assets against the biggest threats.

Implementing good cyber security measures is not only a key part of meeting our regulatory requirements but will also help reduce the likelihood of a significant incident. Implementing even very basic cyber security controls will help reduce the chance of an incident.

The Board - Get a little bit technical

Having a basic understanding of cyber security can help us to ask the right questions to seek assurance about the City of London's cyber resilience - just as we would need to have a certain level of understanding of finance to assess the financial health of the City of London. A good place to begin is to discuss our existing cyber security measures with our experts, and the questions below under 'What does good look like?' suggest a starting point for what to ask.

Start with a cyber security baseline

Attackers often use common methods to attack a network. A lot of these methods can be mitigated against by implementing basic cyber security controls. There are several frameworks that outline what good cyber security controls look like. These include the NCSC's 10 Steps to Cyber Security, ISO/IEC 27002 and the NIS Cyber Security Framework.

Tailor our defences to our highest priority risks

The basic cyber security controls will help mitigate against the most common cyber attacks, but once we have that baseline in place, we then need to tailor our defences to mitigate **our** highest priority risks. Our measures will be tailored both to our technical estate (protecting the things we care about the most) and to the threat (protecting against methods used by specific threat actors).

Guidance can help us address these priorities. For example, if we know that one of our critical systems has external connections, we might consider the specialised government guidance on how to safely import data into that system.

Layer our defences

As with physical and personnel security, cyber security can make use of multiple measures which (when implemented simultaneously) help reduce the chances of single point of failure. This approach is commonly referred to as 'defence in depth'.

Each measure provides a layer of security and deployed collectively, greatly reduce the likelihood of a cyber incident. Once we have our cyber security baseline in place we can focus on layering our defences around those things that are most important to us - or particularly valuable to someone else.

Defend against someone inside our network

Defences do not stop at the border of our network. A good defence assumes that an attacker will be able to access our system and works to minimise the harm that they can do once they are inside it. One of the key things we can do to limit the damage they can inflict is to restrict their movement and access. Effectively managing user privileges and segregating our network are common approaches. Identifying an attacker inside our system as soon as possible will also help limit the damage they can do. Monitoring and logging are key to being able to spot any signs of malicious activity.

These measures will also help mitigate the threat from a malicious insider; somebody who has legitimate access to our systems but then uses that access to do harm. This threat ranges in capability and intent, from a disgruntled employee through to corporate espionage.

Review and assess our measures

Good cyber security is a continuous cycle of having the right information, making informed decisions and taking action to reduce the risk. We will need to be continuously assessing and adapting our defences as the needs of the City of London and the profile of the threat changes. To do this it's important to have some way to assess whether our defences are effective.

There are several mechanisms available to technically assess the effectiveness of our security controls. This may include things like testing the security of our networks (pen-testing) through to certification of products or services. We may want to use a combination of internal mechanisms and objective assessment provided by an external source.

Engaging with staff will also help us gain a more accurate picture of the City of London's defences. It will also give us the opportunity to get valuable staff input into how policies or processes could be improved. Metrics or indicators can also tell us where we need to change our approach or adapt to new circumstances. Understanding exactly what an indicator is telling us may require further investigation of the situation. An example is the trend in people reporting suspicious emails. A decline in the number of people reporting can either mean fewer malicious emails are getting through to people's inboxes, or it could mean fewer people are reporting any concerns because they don't receive feedback when they do, and therefore believe nothing is ever done afterwards.

What does good look like?

The following questions should be used to generate productive discussions with the Board and our security team. The aim is to identify what constitutes 'good' cyber security in terms of **assessing the City of London's cyber security measures**.

Q1. As an organisation, how do we assure ourselves that our measures are effective?
Q2. As an organisation, what measures do we take to minimise the damage an attacker could do inside our network?
Q3. As an organisation, do we implement cyber security controls to defend against the most common attacks?

Collaborating with suppliers and partners

Cyber attacks on our suppliers can be just as damaging as an attack on our own networks.

There are four reasons why cyber security is a key consideration when collaborating with suppliers and partners:

1. We increase the number of routes and external touchpoints in the City of London. So if any of them are compromised, we are also at risk.
2. We may be targeted as a way into the organisation we are supplying.
3. Our suppliers may be targeted as a route into the City of London.
4. We may be sharing sensitive or valuable data or information that we want suppliers to protect.

Being able to demonstrate a good level of cyber security is increasingly a key component of supplier and provider contracts, and is already a requirement for many government contracts.

Build cyber security into every decision

All organisations will have a relationship with at least one other organisation, be that the provider of our email service, or the developers of the accounting software we use, through to our traditional procurement supply chain. Most organisations will be reliant on multiple relationships. Each of these relationships will have a level of trust associated with them, normally some form of access to our systems, networks or data. There are three key things we therefore need to ensure:

1. That this access doesn't provide a route for an attacker to gain access to the City of London, either through deliberate action or unintentional consequence.
2. That any partner or supplier is handling any sensitive data appropriately and securely.
3. That any product or service we buy has the appropriate security built in.

Cyber security risk should be a key consideration in any decision on new relationships or collaborations. This includes decisions on suppliers, providers, mergers, acquisitions and partners.

Identify our full range of suppliers and partners, what security assurances we need from them, and communicate this clearly

Review our current supply chain arrangements to ensure we are setting out our security needs clearly and identifying the actions we need to take as a result. If we ourselves are a supplier, ensure you meet the security requirements set for you by the customer as a minimum.

Ensure that the security requirements we set are justified and proportionate and match the assessed risks to our operations. Also be mindful of the current security status of our suppliers to give them time to make the necessary improvements. It might be useful to include references to the following government guidance that can help to establish a baseline of cyber security:

- 10 Steps to Cyber Security
- Small Business Guidance
- Cyber Essentials

The following government guidance can help **us** to assess our own security needs from suppliers:

- Supply chain guidance
- Cloud services guidance
- Software as a Service guidance

Get assurance

Security should be built into all agreements from the start, and we should have confidence that our security needs are being met. Dependent on our relationship with the supplier or provider and our resources, we could seek assurance of this through testing, auditing or adherence to accreditation standards.

Consider the implications if our supplier is compromised

No matter how comprehensive our security agreements with our partners are, and no matter how well they implement their controls, we should assume that our partners **will** be compromised at some point. We should plan the security of our networks, systems and data accordingly with this assumption in mind. This is also worth considering in our security agreements; what are we expecting of them and their response? Do they have to notify you? Do they have to assist us if we are consequently also compromised?

What does good look like?

The following questions can be used to generate productive discussions with our technical team. The aim is to identify what constitutes 'good'cyber security in terms of **supply chain security**.

Q1. As an organisation, how do we mitigate the risks associated with sharing data and systems with other organisations?
Q2. As an organisation, how do we ensure that cyber security is considered in every business decision?
Q3. As an organisation, are we confident that we are fulfilling our security requirements as a supplier?
Q4. As a Board, do we have a clear strategy for using suppliers, and have we communicated it?

Planning our response to cyber incidents

Good incident management will help reduce the financial and operational impact when they do occur.

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 our reputation.

Ensure we have a plan

1 in 10 organisations don't have an incident management plan. If you're one of these organisations, then we should address this immediately.

Understand your role in incident management

Incidents often occur at inopportune moments and most people's decision making is compromised in times of crisis. For these reasons, **everyone** must have a clear understanding of **their role** and the organisational response in advance, especially Board members who would likely be representing the organisation in the media.

The Board also needs to be explicit about who it is willing to devolve authority to (especially outside core working hours), and exactly what that authority covers. For example, does that cover calling in a contracted incident response company, or taking down a public facing website? The Board also needs to be explicit about when it wants to be informed of an incident, both in terms of at what stage of the incident, and in terms of what significance of incident they need to know about.

Get involved in exercises

The best way to test these processes and thresholds (and to get a good understanding of the Board's role) is through exercising the incident management plan. If we would be involved during a real incident, then we should be involved in an exercise. Doing this in conjunction with operational staff can also help to highlight issues around authority for critical decisions. Even if we do not have a direct role in responding to an incident, running an exercise can be a good way to understand the realities of how an incident would impact on the City of London.

Drive a 'no blame' culture

Post-incident analysis provides insight that can help us reduce the likelihood of incidents occurring in the future and reduce their potential impact. Crucially in order to get this insight we need to be able to be honest and objective about what has happened. This can only happen in a no blame culture, such as we would use when investigating health and safety incidents. Critically for the Board, new regulation, such as GDPR, is clear that responsibility for incidents or data breaches sits with the organisation and not an individual. Therefore the Board is ultimately responsible for

any cyber security incident as the governing body. Apportioning blame to a specific individual within the organisation will be treated as poor cyber security practice.

Work out what an incident would look like

One of the most common things overlooked is being able to identify what constitutes an incident. There's two aspects to this:

1. Working out how we would spot an event in the first place.
2. Working out at what point an **event** (something happening on our networks or systems) becomes an **incident**.

How would we spot an event?

Depending on their motives, an attacker is unlikely to tell us when they have successfully compromised the City of London, so we need our own methods to identify an intruder or an attack. This normally takes the form of monitoring. Monitoring refers to observing data or logs collected from our networks or systems to identify patterns or anomalies that could indicate malicious activity. Even if we don't have monitoring to identify the incident, it is still useful to collect system or network logs (especially those relevant to our critical assets) so that we can retrospectively review them once we know an incident has occurred.

When does an event become an incident?

This is often not a clear cut decision. We can try and gather as much information as possible to inform our assessment of an 'event', but we probably won't have a complete picture of what has happened. Beginning an incident response might have implications for cost, reputation and productivity, so we will want to consider who has the authority to make this decision, and what the thresholds are for an incident **in advance**.

What is a cyber security incident?

A breach of the security rules for a system or service - most commonly:

- attempts to gain unauthorised access to a system and/or to data
- unauthorised use of systems for the processing or storing of data
- changes to a systems firmware, software or hardware without the system owner's consent
- malicious disruption and/or denial of service

Use the information we already have

All the information we have previously gathered on what's important to protect, the threat and our technical estate will provide critical insight in two key areas:

- It will give us insight into the impact of incident. If the attacker has accessed a particular user device, what could they access? Could they access those things we care about the most?
- It will help us determine our operational response. If the attacker is on a specific network can we isolate that network? If we can, what would the impact be on the City of London?

Take pre-emptive measures

Put measures in place to help reduce the harm that an attacker could do. This could be:

- introducing measures that restrict their movement once they are inside our network
- pre-emptively reducing the impact of attacks (for example, backing up our data will help to reduce the impact of a ransomware incident)

As with any other defensive measures, these should be focused on protecting what is most important to you.

Make an Incident Management plan

Cyber Incident Response is a complex subject as no two incidents are ever the same. However, as with all business continuity planning, we can develop a plan that will outline the key elements of our response. Our plan should not only cover the technical elements, but also:

- the people and process elements such as media, customer and stakeholder handling
- reporting to regulators
- dealing with legal actions

For more common incidents (such as DDOS) it may be helpful to develop a specific 'playbook' setting out the City of London response.

Test our plan

Rehearsing our response to different scenarios is key to ensuring our plans are effective and remain current. There are various exercising packages we can use. This will be a critical part of the role for any staff involved directly in incident management, but every Board member also needs to understand their specific area of responsibility during an incident.

Learn lessons

An often overlooked aspect of incident management is the post-incident review. An incident can provide valuable insight into our cyber readiness, including:

1. The **threat** the City of London faces.

- Who carried out the attack and was it targeted?
- Did they go about it in the way we expected?
- Did they go after the things we expected?

2. The effectiveness of our **defensive measures**.

- What did our defences protect against?
- What didn't they?
- Could they be improved?

3. The effectiveness of our **incident response measures**.

- What would we have done differently?
- Did our response help to reduce the impact of the incident?
- Did it make some aspects worse?

> **Working with suppliers and partners**
>
> Our plan should also consider how we mitigate the impact on any partners or customer organisations if we were compromised. When do we inform them? What mechanisms are in place to limit the damage it could do to them? We should also consider what we would do in the event that a supplier is compromised; we may not have control over how they deal with the incident. What would we be able to do independently to reduce the impact on the City of London? The best way to mitigate this risk is to have a collaborative approach to our security with our partners and suppliers.

What does good look like?

The following questions should be used to generate productive discussions with the Board and our security team. The aim is to identify what constitutes 'good' cyber security in terms of **responding to cyber incidents**.

Q1. As an organisation, do we have an incident management plan and how do we ensure it is effective for cyber incidents?
Q2. As an organisation, do we know where we can go for help in an incident?
Q3. As an organisation, do we learn from incidents and near misses?
Q4. As an organisation, how would we know when an incident occurred?
Q5. As a Board, do we know who leads on an incident and who has the authority to take any decisions?
Q6. As a Board member, do I understand what's required of my role during an incident, and have I had training to equip me for that role?