Script

# Slide 2 - Introduction

This presentation is a critical evaluation of leadership within my organisation, the Bank of England. For practical reasons I have chosen to focus on the leadership of the Cyber Security Division only. This is due to the Bank being a large and complex organisation with numerous departments, divisions, and functions.

During the presentation I provide a brief introduction to the Bank and Cyber Security’s role and strategy within it. I will appraise the leadership of the Cyber Security Division, consider its current state, its strengths and weaknesses, and a desired future state. Finally, I will make recommendations to allow the division to achieve its leadership goals in line with Bank’s mission.

# Slide 3

The Bank of England, as the central bank of the United Kingdom, plays a crucial role in maintaining the country’s financial stability. It is responsible for the production of secure banknotes, overseeing payment systems, and works to keep the cost of living stable by managing the main interest rate in the UK. The Bank ensures that transactions can be conducted easily and securely through the creation, support, and maintenance of the Real Time Gross Settlement IT system, which helps to preserve the purchasing power of money.

Through the PRA the Bank regulates UK banks and other financial institutions to ensure their operational safety. The Bank of England also acts as the lender of last resort and as the custodian of the official gold reserves in the United Kingdom.

The Bank has an ambition, set out by Governor Andrew Bailey, for the Bank to be more human, humble and in step with a changing world. To achieve this a set of Bank Behaviours were launched in February 2023. The behaviours, Act Inclusively, Drive Growth, and Delivers Outcomes, are at the heart of all the Bank does and are instrumental to drive a culture that enables its people to thrive, invest in personal career development and focus on what matters in their role.

The Bank’s intranet states, “Everyone in the Bank should consider themselves as a leader” (Bank of England, 2023) supporting one of the strongest themes from the module; leadership should not be dictated by your position in a hierarchy, leadership can come from all levels.

# Slide 4

The Bank’s cyber security strategy has been created to allow the division to achieve its mission and covers the Bank’s requirement to manage its own cyber security risks. However, it does not cover the Bank’s regulatory role to oversee cyber security risks in the wider financial sector.

The strategy’s ambition is to create a future for cyber security at the Bank of England which is sustainable and resilient. It must be built to last and grow stronger rather than weaker in the face of disruptions.

The Bank’s ability to respond to threats and attacks is vital to the stability of the UK economy and to maintaining the public’s trust. Any failure to protect or minimise the impact of an attack on the Bank’s information systems, data, staff, or reputation would have a detrimental effect on its ability to achieve its mission. Due to the Bank’s high level of visibility both nationally and internationally, it is a target for numerous threat actors including novice hackers, organised crime gangs, and nation states. These continuous attacks require a resilient and robust set of controls that include people, processes, and technology.

To achieve the “people” element of the strategy, the cyber division looks to build a qualified, motivated, and experienced workforce. Today the division can be overly reliant on key individuals, whose segmented specialisation offers little resilience in the event of staff departures. Without the ability to compete for external staff on a purely financial basis, the Bank must be able to retain and grow its own talent, investing in skills through development.

The concepts of “T shaped” people and “key shaped” teams are spoken of regularly. However, these phrases are typically used in reference to technical skills and capabilities. An individual’s ability to grow in the use of a system or technology often overshadows any consideration of “softer” management skills. This in turn causes issues for the future of leadership.

# Slide 5

Like most organisations, cyber security at the Bank of England has become a major focus across all levels of leadership. Gone are the days when cyber security was perceived as ‘for IT teams only’, and CISOs now have board-level visibility and must promote cyber hygiene and improved digital resilience for all staff.

The Bank’s CISO reports directly into the Chief Information Officer and has a standing place on agendas for numerous board and committee meetings.

To support the CISO, the role has a personal assistant, and a senior leadership team made up of 8 managers. These managers align to functions or capabilities and consist of 21 teams, to make up a total of 91 staff. These teams typically operate in silos, and any large project or programme looking to engage with cyber security has various points of contact for requesting time and resources. This have become obvious due to the multiple projects created to migrate applications from “on premise” infrastructure to a cloud hosted solution.

The wider Technology department within the Bank has committed to moving 80% of our in-house applications to the cloud by 2030. This excludes any payment systems that are part of the Critical National Infrastructure, such as the Real-Time Gross Settlement system, known as RTGS, but requires a large amount of collaboration across business areas and Technology departments.

In the next 6 years the budget for cloud services and infrastructure is set to grow rapidly. As a direct result of this, the budget for securing this new IT estate must also grow. This budget will be required to build a new set of skills for cloud technologies and support a new way of thinking about the Bank’s systems and cyber security.

# Slide 6

As mentioned, the cyber security division of the Bank is led by the Chief Information Security Officer supported by 8 senior managers with each manager aligning to a function within the department. All managers are centrally located at the Bank’s head office in Threadneedle Street in London. All cyber security staff sit together, but this is in an area that is physically separate from other technology teams which can limit collaboration.

The Bank of England is committed to diversity and inclusion, and the cyber security division supports the organisation in its aim to reflect the society they serve. The Bank has staff-run networks including Age, Bank of England Ethnic Minorities (BEEM), Christian Union, and disAbility Network to name a few. The Bank encourages diverse ideas, open debate and perspectives that challenge their current ‘norms’. The senior leadership team is made up of 6 men and 3 women; all members are white British or Irish; 80% have higher education degrees; the age of team members ranges from 30 to 52; and the average time at the Bank is 9 years (however, this is high due to one member of staff being at the Bank of over 30 years).

All members of the senior leadership have specialised technical skills with 2 thirds holding at least one industry-recognised certification, however, only 2 out of the 9 leaders have any formalised management or leadership training. Generic Bank-wide behaviours are supported, promoted, and regularly communicated by all members of the cyber security leadership.

Due to the nature of cyber security, there are regular incidents that require some level of crisis management. The leadership team appear to work well together through collaboration, however, only 1 third regularly engage with other business units or technology departments not within their area of responsibility. The cyber strategy covered earlier was created through collaboration across teams and input was taken from all levels.

There is a strong leadership culture within the division, but the senior team can often be seen as a closed group with decisions being made and communicated downward without a well-defined feedback process.

# Slide 7

Any organisations strength comes from its people, and the cyber security division at the Bank of England is no exception. As mentioned, the average length of service for cyber security’s senior management is 9 years, with one individual having been at the Bank for more than 30 years. These long periods of service provide a large amount of tacit knowledge that can be drawn upon.

However, these long periods of service can also be seen as a weakness. Those in leadership positions tend to be people who have been at the Bank for a long time and become “accidental” leaders without any formal leadership training. However, I feel that the leaders are less “accidental” and more “circumstantial” due to being in the right place at the right time during periods of high staff turnover. These leaders are typically highly technical but lack advanced leadership skills.

The teams within the cyber security division are effective in collaborating with other cyber security teams, but fail to work across boundaries including, Horizontal - Across functions and expertise; Stakeholder - beyond their immediate area; and Geographic - across offices and locality.

Retention of staff is a challenge for the whole Bank of England organisation, and it can be observed that two groups of staff exist; those that join and stay for more than 10 years, and those that leave for other opportunities after 3 years. Internal surveys regularly refer to issues of remuneration, however, the Bank is unable to compete with commercial businesses and attempts to rely of other initiatives which are not attractive to younger members of staff.

Cyber security’s increased level of visibility at board level can provide a great opportunity for improvement, and with every cyber incident that appears on the news, increased funding for cyber activities is seen as a vital area of the budget.

Due to the Bank’s function and reputation, it has the ability to collaborate with every financial institution in the UK, as well as groups such as the NCSC (National Cyber Security Centre) and central banks around the world. This could provide opportunities to share information and learnings around cyber security.

A major issue for all Cyber Security teams is the lack of qualified applicants for open positions which is due to the recent trend of over-inflated salaries in cyber security due to a massive skills shortage. The Bank, due to its reputation and capabilities must take the opportunity to build talent internally, and provide a work environment that is attractive to staff.

The largest threats to the leadership within the cyber security division is CISO burnout. In a recent Nominet survey, of 800 CISOs interviewed, 88% reported being “moderately or tremendously stressed” with 90% stating that they would be willing to take a pay cut if it would reduce stress levels. This creates a worrying trend were the average tenure for a CISO is only 26 months.

This stress is also experienced by those that support the CISO and leads to concerns around succession planning. Those being lead can often see the potential of a senior manager role but acknowledge the lack to support through training and comparatively low remuneration.

# Slide 8

There are several changes in desired qualities, behaviours, and culture of a future leadership team.

The leadership team of the future should allow managers to be aligned with cyber security functions but ensure that they have the support to be more agile and resilient when faced with new and emerging technologies. Technologies such as cloud computing will require new skills and require strong collaboration across boundaries.

As cyber security threats increase in regularity and complexity, a greater diversity in age, race, culture of origin, and experience would lead to opportunities for a wider range of diverse thinking.

There should no longer be any “accidental” or “circumstantial” leaders as all senior members of staff have had the opportunity to participate in formal leadership training and a scheme of coaching and mentoring would provide greater support.

Senior leaders must be encouraged to cross vertical, horizontal, demographic, and geographic boundaries and engage with staff for better collaboration. Stronger, more open networks result greater opportunities, and more success.

All senior managers must be seen to display the ethics and values of the Bank of England and promote them within the division and across the organisation. Building a strong, shared identity will re-enforce awareness training to create better behaviours and more resilient culture.

# Slide 9

My recommendations focus on people, skills, and behaviours.

[People]

The creation of the Deputy CISO role will allow for clearer delegation of duties. If the CISO is unavailable, due to illness, vacation, or other reasons, a Deputy CISO can step in and ensure that critical functions are still being performed without interruption.

Establishing a Deputy CISO role will also support the process of succession planning. However, this should not be limited to only the highest levels of the management structure, and leaders at all levels should be encouraged to identify and support those that will be our future leaders.

Due to the effort and resources being invested into cloud technologies, a senior leader whose responsibilities and accountability align directly with these work streams should be appointed. A dedicated senior leader for cloud will take work from other leaders creating an increase in their capacity to focus on their primary responsibilities.

[Skills]

To combat the creation of future “accidental” leaders, a training programme should be established across the department and division. This training should be made available to staff at all levels, each with tailored resources, and should include Senior Leadership Apprentice programs and MBA courses.

Create a culture of self-development by arranging a series of talks, discussions, and presentations around leadership within the Bank. This will allow aspiring or existing leaders to get knowledge and insight into how the Bank’s leadership act, work, and learn, and will help them grow in their own leadership adventure.

In a constantly changing world that presents us with challenges every day, an effective workforce needs to be resilient, but understand the importance of their own well-being. The stress put on to a CISO can be excessive and could be alleviated through the option of condensed working hours. This would allow managers to complete their working hours in 4 days, instead of 5. However, this would only be possible if the “people” recommendations are implemented.

[Behaviours]

Mentoring is a beneficial scheme for an organisation to have, however, I feel that coaching can provide greater value. Both current and future leaders should know what is expected of them, be supported in meeting those expectations. They should be held accountable for their behaviours, while being given the space to fail and grow from experiences.

Bill Joiner in his white paper “Leadership Agility: From Expert to Catalyst” describes 3 levels of leaders. Joiner describes “Expert” leaders as tending to operate within silos with little emphasis on cross-functional teamwork and improvements being mainly tactical and incremental. Providing opportunities for staff to engage and operate across boundaries, both vertical and horizontal, will allow them to grow from “expert” to “achiever”. They will operate with greater system-centric thinking and be able to work towards strategic objectives.

Gaining feedback on their actions is vital for a leader’s growth and improvement. Currently feedback is only gathered formally using a “360 degree” process, however, due to the overhead of administration, this process is only made available to managers every few years. A behaviour of asking for honest and open feedback in a more informal manner should be encouraged and supported organisation wide. Only by understanding what we are doing well, and were we can improve, can leaders learn.

# Slide 10

This presentation was delivered to the senior leadership team of the Cyber Security Division at the Bank of England in December 2023. Feedback from the presentation included a desire from the leadership team to undertake a horizon scanning activity to more accurately estimate the anticipated effort around cloud migration projects and the potential need for another senior leader.