

**Bank of England**

# Sustainable and Resilient

## **Cyber Security Strategy 2024-2027**

October 2023

**Cyber Security Division**

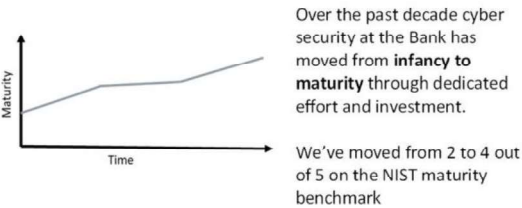


A Note from the CISO (p.2)



Our ambition is to create a future for cyber security at the Bank which is **sustainable and resilient**: built to last and growing stronger rather than weaker in the face of disruptions

Our maturing capability (p.3)



Ongoing pressures (p.3)

**Changing External Threats**

- Increasing commercialisation
- Geo-political tensions
- Wider proliferation
- CNI targeting

**An Evolving Technology Estate**

- New environments
- Commodity solutions
- Obsolescent controls
- Dependence on third parties

Sustainable and Resilient (p.5)

**Sustainable**



**People:** Building a pipeline of multi-skilled individuals and a security focused culture



**Consistency:** Ensuring a consistent maturity of capability regardless of environment



**Supportability:** Cost effective and operationally efficient controls

**Resilient**



**Assurance:** Pivoting from a system-centric to a business function view of assurance



**Recovery:** Focus on strengthening our ability to recover from successful cyber-attacks



**Secure-by-design:** Continuing to ensure security is an essential component of architectural decisions and project delivery

Executing Our Strategy (p.10)

**Funding**

**£3m**

A consistent investment in line with historic spend to keep pace with changing external threat

**2%**

A surcharge on Technology investment to ensure proportionate security improvement

**Delivery**

- A new 3 year Investment Programme
- Multi-year planning based around core outcomes and objectives vs. pre-defined deliverables
- Detailed benefits tracking

Measuring Progress (p.11)

Risk	Residual 2023	Target 2027
Data Loss	12	9
Denial of Service	9	6
Insider	12	8
Misconfiguration	8	4
Mobile Asset Loss	3	3
Nation-state high	5	4
Nation-state low	6	6
Patching	9	6
Phishing	9	6
Privilege escalation	8	4
Ransomware	12	8
Supply Chain	16	10

Delivery Risks (p.13)

Unexpected changes in the external threat landscape





A significant shift in our wider Technology strategy

A lack of required resourcing and investment



---

# Contents

---

<b>A Note from the CISO</b>	<b>2</b>
Scope of this strategy	2
<b>A Maturing Capability</b>	<b>3</b>
Changing External Threats	3
An Evolving Technology Estate	4
<b>Sustainable and Resilient</b>	<b>5</b>
Sustainable	5
Resilient	7
<b>Executing Our Strategy</b>	<b>10</b>
Funding	10
Delivery	10
<b>Measuring Our Progress</b>	<b>11</b>
<b>Delivery Risks</b>	<b>13</b>

# A Note from the CISO



**Jonathan Pagett**

CISO

A decade after we began the journey to improve our cyber maturity, I am proud to lead an award-winning division of experts committed to repaying the trust placed in us by the people of the United Kingdom to keep the Bank of England safe from cyber-attack.

And yet, with cyber we know that the journey is never over. As fast as we can implement controls and capabilities, attackers will create new ways to circumvent them.

Distilling the next three years of focus down to a few pages is never easy. But in short, this strategy outlines our ambition to create a future for cyber security at the Bank which is **sustainable and resilient**: built to last and growing stronger rather than weaker in the face of disruption.

Having built a capability to be proud of, now is not the time to rest on our laurels. The world changes so fast that all too soon we could see ourselves falling behind. Instead, we must ensure the systems and structures which keep us safe are not just designed to withstand change but to evolve alongside it.

## Scope of this strategy

This strategy covers the Bank's requirement to manage its own cyber security risks, including the people, processes and technology that enable the Bank to fulfil its mission.

It does not cover the Bank's regulatory role to oversee cyber security risks in the wider financial sector.

# A Maturing Capability

---

Over the past decade cyber security at the Bank has moved from **infancy to maturity** through dedicated effort, investment, and organisational support. While we are building on these strong foundations maintaining our current levels of capability requires us to tackle the dual challenges of **an evolving cyber security threat** and **transformations to the technology we need to protect**.

Beginning with the Information and Infrastructure Security (IIS) Programme (2014-2017), through Cyber 2020 (2017-2020) and the most recent Cyber Defence Programme (2021-2024) cyber security has been an investment and organisational priority for the Bank. Over the past ten years the c.£45 million spent on improvement initiatives has created over 100 new security roles and vastly strengthened our core controls, from better network segregation to a monitoring and response capability.

We have tracked our cyber maturity throughout and remain on track to finish the current Cyber Defence Programme with an overall National Institute of Standards and Technology (NIST) rating of 4 out of 5, an almost 100% improvement since our journey began. As well as this independent benchmarking, we engage regularly with peers across the globe and have been recognised repeatedly for our capabilities (see box 1). However, maintaining such maturity over time requires tackling two distinct but inter-related forces: changing external threats, and the evolution of our own technology estate.

## Box 1: An award-winning division

This year the Cyber Security Division at the Bank were recognised with the Financial Services award of the year at the National Cyber Awards. This followed previous award wins for individuals within our Cyber team at the WeAreTechWomen and Women in IT Awards, and Central Banking's Best Cyber Resilience Initiative.

## Changing External Threats

As the Bank matures, so too do the capabilities of the varied threat-actors who seek to disrupt our services and compromise our information.

**Increasing commercialisation:** The monetisation of ransomware attacks (extorting money through operational disruption and/or data theft) and Business Email compromise (deceiving organisations into making fraudulent payments), paired with the anonymity provided by cryptocurrencies, have seen the scale of cybercrime grow dramatically. Ransomware-as-a-Service (RaaS) offerings have moved the ability to compromise an organisation from the hands of skilled individuals to within reach of anyone with an ability to pay. As commercial cybercrime proliferation expands the numbers of those able to mount sophisticated attacks, we will likely see incident numbers grow.

**Wider proliferation:** technological developments also have the potential to reduce the technical barrier to entry for those mounting attacks. The dramatic growth of Artificial intelligence (AI) in recent months will almost certainly increase the volume and value of successful compromises. While the National Cyber Security Centre (NCSC) believe that it will still take several years for the tooling to drive a paradigm shift



in existing attack techniques publicly and commercially available AI and Large Language Models (LLMs) are already improving attackers' ability to profile, select and socially engineer their targets.

**Geo-political tension:** Hostile nation states who have historically lacked sufficient sophistication may also increasingly use legally available tools to buy the capabilities needed to pose a threat to the Bank (see box 2). Such states may use such services for espionage or disruptive demonstrations of power, rather than financial gain; particularly amidst a backdrop of geopolitical tensions which the NCSC believe "will take decades to settle". The Russian invasion of Ukraine, the war in Israel/Palestine, heightened tensions with China and acrimonious elections in India and the USA continue to put the current world order under increasing strain.

### Box 2: NSO Pegasus

Pegasus spyware, developed by cyber-arms company NSO group, is designed to covertly gather information from mobile phones. Marketed as a tool for fighting crime and terrorism, there have been numerous reports of the product being used to surveil governmental officials including Boris Johnson and other 10 Downing Street staff.

**CNI targeting:** Amidst such tensions earlier in 2023 NCSC, alongside Five Eyes partners (USA, Canada, Australia, and New Zealand), issued two advisories in unusually quick succession specifically highlighting an emerging threat of cyber-attack to critical national infrastructure organisations from state-aligned groups.

## An Evolving Technology Estate

**New environments:** Within the Bank, programmes such as Real Time Gross Settlement (RTGS) Renewal, Cloud, and Data Centre Migration have brought their own transformations to our technology. A Central Bank Digital Currency (CBDC), if pursued, could represent an even greater shift. We are also about to embark on a multi-year programme to tackle an obsolescence challenge which has been years in the making and will represent another dramatic period of technological change.

**Obsolescent controls:** Our defences must transform in line with the estate they aim to protect. Traditional physical hardware controls will not be fit to defend an increasingly virtualised environment; and reliance on an impenetrable enterprise boundary will not meet the challenge of growing data flows and third-party dependencies while allowing us to reap the opportunities these offer.

**Commodity solutions:** Bespoke home-grown systems are increasingly being replaced with standardised solutions or developed from multiple commodity components. While often benefitting from the higher security budgets of providers and reducing operational obsolescence challenges, the ubiquity of such software makes it a more likely target for attackers, increasing the importance of good cyber hygiene practices such as patching. During the transition, where we depend on integrations between legacy systems and fast changing replacements, the higher patching cadence of the latter will pose an operational challenge.

**Dependence on third parties:** An embrace of commercial-off-the-shelf (COTS) systems also deepens our reliance on third party vendors. The Renewed RTGS has more than double the number of registered third-party engagements to support its operations than its predecessor. Increasingly, elements of the technology on which we depend are run and secured by those outside of our organisation. The Bank is not alone in making this shift, and attackers are all too aware of these potential backdoors.

# Sustainable and Resilient

Having built up defensive capabilities we must now ensure that the Bank's cyber security is **sustainable and resilient** in the face of change.

To ensure sustainability we will focus on our **people, consistency of maturity and supportability of our services**. To strengthen our resilience, we will **broaden our assurance practices, invest in our recovery capabilities, and continue embed security by design**.

## Sustainable

*Attackers will never stop targeting the Bank. We can never become complacent as to our capabilities, let down our guard or stop evolving our protections. We must ensure we maximise the impacts of our investment, strengthening our core foundations and making the most of available resources. Over the next three years we will do this through a focus on:*

### **People: Building a pipeline of multi-skilled individuals and a security-focused culture**

Building a qualified, motivated, and experienced workforce remains one of the largest challenges for any cyber security organisation. Today we are overly reliant on key individuals, and segmented specialisation offers us little resilience in the event of departures. Without the ability to compete on a purely financial basis, we must be able to retain and grow our own talent, investing in skills and development.

In the coming years we will focus on evolving our operating model around T-shaped individuals and key-shaped teams (see box 3), supporting lateral movement, and actively promoting and rewarding cross-skilling. We will build out career pathways and development plans across the division with a focus on creating more junior roles and growing expertise through both experience and qualifications. We will strengthen our partnerships across the sector and look to create greater opportunities for talent rotation. In all cases, we will continue to work closely with the People Directorate, tailoring the Bankwide employee value proposition to the specifics of cyber-careers.

#### **Box 3: T-Shaped People and Key Shaped Teams**

The vertical bar of a T represents an individual's depth of skills in a specific field or technology. The horizontal bar is the ability to apply knowledge to areas beyond these primary skills. T-shaped people display both breadth and depth and can work on tasks outside of their core domain. Expanding the concept to 'key shaped' teams encourages a focus on creating multi-skilled teams with varied expertise and greater resilience and flexibility.

Beyond the Cyber Security Division, we will continue to reinforce a security focused culture across the Bank, whereby all colleagues understand and demonstrate the required behaviours to safeguard our assets. We will learn from behavioural science to use just-in-time 'nudges' to make it easier for our people to recognise potential cyber security risks and mitigate them in the moment.

Recognising the challenges introduced by remote working, as well as changing staff attitudes, we will use a data-driven approach to personalise messaging, creating a compelling narrative for security awareness at all stages of the employment lifecycle. Our senior leadership will remain pivotal to setting a strong security tone from the top, and we will support them with appropriate risk-based reporting, exercising, tailored briefings and communications.

### **Consistency: Ensuring a consistent maturity of capability regardless of environment**

In recent years the Bank's estate has undergone dramatic shifts: we have gone from one environment to multiple, each with their own native capabilities and providing significantly different homes for the applications that run on them. These include our Azure cloud platform, the new CNI enclave which houses the renewed RTGS, as well as our legacy enterprise estate. While embracing the benefits these differences can offer, we have more to do to ensure consistency of maturity with regards to the security controls in place and our operational confidence in running them. Incident data shows us that good cyber hygiene remains the key to protecting against most cyber security threats. After a period of significant change, we need to carve out the appropriate time and resources to make sure that each of our core operational capabilities are uniformly matured across our environments.

We need to be able to continue to manage our security posture, having an overarching view of the software components and versions we are running in each environment, so that we can identify where patches and configuration changes are required. Strong operational processes, such as exist in the enterprise estate today, should ensure we can deploy these changes with speed and regularity, and without the risks of operational disruption as a result. In newer environments such as the Cloud, we need to ensure we can give vulnerabilities the requisite context so we can quickly understand the true risk they posed by assessing component criticality and exposure.

With dedicated investment and attention in previous years we have built a strong centralised access management capability. However, not all our systems are currently integrated. Continuing to coalesce around a single toolset alongside consistent processes will improve our ability to administer access and make it easier for approvers like line managers to understand and control the privileges which their staff need.

Finally, we need to ensure that our ability to monitor for and respond to incidents is consistent regardless of where in the estate these occur. We will need to build our operational experience, ensuring we have equal confidence in identifying and navigating anomalous activity in newer environments as we have on the enterprise.

### **Supportability: Cost effective and operationally efficient controls**

In a resource-constrained environment we must ensure that we can secure a growing technology estate without dramatically increasing the size, costs, and complexity of our security teams. To ensure our people are focused on doing what matters most, we will embrace the benefits of automation; streamlining and challenging processes which do not offer genuine benefits.

We will make use of newer support models such as Software-as-a-Service where appropriate (see box 4) and consider where overlapping or competing controls create operational inefficiencies which offset any benefit of coverage or redundancy. Where it makes sense we will consolidate tools with fewer vendors, with whom we will form truly strategic partnerships. When we do introduce new vendors or



controls, we will do this across all environments unless there is a strong reason not to do so. This should reduce the likelihood of inconsistencies being re-created as the estate continues to change.

### Box 4: A New Model of Support

Vendors are increasingly offering tools under the Software-as-a-Service (SaaS) model, and indeed in some cases insisting upon this. SaaS models are reliant on centralised hosting (overwhelmingly via the Cloud) and therefore may not be appropriate in all cases. However, in many situations such a model will allow for easier and faster provisioning and scaling and shift the burden of hardware and network maintenance to the vendor.

## Resilient

*The last decade has proven that shocks to our ways of working must be expected: from Covid-19 which moved the organisation to almost universal remote-working overnight, to the largest armed conflict in Europe since the Second World War. In line with our growing requirements and expectations of firms, over the next three years we will strengthen an internal focus on our own cyber security resilience by:*

### Assurance: Pivoting from a system-centric to a business function view of assurance

We will pivot our model of assurance away from ensuring system compliance against tightly defined controls. Instead, we will focus on assessing the cyber security risks to functions, including both systems and the business processes (see box 5) which surround them. Moving forward we will prioritise consideration of the 14 business critical functions, driving conversations with business owners that consider the exposure of these functions to cyber risks such as Ransomware or Insider Threat.

### Box 5: Business Critical Functions

Current security assessments are scoped to a specific system, e.g., T24 or Openlink, which are then reviewed against defined controls. In future we will instead consider critical functions in the round, such as the **operation of the RTGS system, including provision of intra-day liquidity and ensuring that note supply and notes operations continue, in order to facilitate public access to sufficient, high quality, secure banknotes in a range of denominations.**

We will streamline our accreditation processes, building on existing tiering to recognise the areas of key importance for business colleagues, and of most significant risk. For those lower tier processes we will adopt automated and self-serve models which will free up our teams to invest far more into the areas of greatest concern.

### Recovery: Strengthening our ability to recover from successful cyber-attacks

When we began building our cyber capabilities, our focus was firmly on reducing the likelihood of a successful attack. In more recent years we have improved our ability to respond to such attacks. However, in the event of a major cyber incident we will be equally judged by how quickly we are able to restore our critical services. Building on the work of business continuity teams we need to strengthen this ability. This will mean acknowledging both the differences and commonalities between cyber security and broader technology incidents, ensuring that colleagues feel better prepared for tackling the likely realities of a deliberate and destructive attack scenario.

Critically, we will continue to focus on a culture of reflection. Strong feedback loops will allow us to use incidents, against both ourselves and others, to strengthen and improve rather than just recover to a previous state. Penetration tests, internal exercising, near misses and live incidents all provide invaluable learning, but only if we ensure an environment that seeks to understand and grow rather than blame and chastise.

This shift is in line with a wider industry trend for organisations who have reached our level of preventative and response capabilities. Newly introduced recovery frameworks will help us to identify gaps in our abilities to both restore service and to learn from an attack. With a focus on Tier 0 services and business critical functions we will work with wider Technology teams to ensure we feel confident in our abilities throughout all stages of a potential incident.

### **Security-by-Design: Continuing to ensure security is an essential component of architectural decisions and project delivery**

Given the volume of changes to the technology estate with major programmes such as Obsolescence (see box 6), it is vital that security principles continue to be a core factor in architectural decision making. The more we can ‘shift security left’ and embed secure and consistent design patterns from the outset, the more we can ensure an ability to deliver securely at scale. Implications of design choices on either the costs (both to deliver and support) of appropriate security, or the additional risks these may create need to be made clear to all up-front. This will allow both business and technology teams to appropriately factor them into decisions.


#### **Box 6: Overcoming Obsolescence**

Protecting an ageing estate is a significant challenge. A strategic focus on tackling our technical debt will undoubtedly make the Bank safer and provide better foundations for a sustainable and resilient model of cyber security in the long-term. However, as with any large-scale change, we will need to ensure our cyber capabilities can keep pace and consequently would expect cyber investment to grow to match the scale of this transformation in the short term.

As the Bank continues to introduce new development practices such as Agile, security will need to be embedded as both a cultural priority and as critical acceptance criteria. Automated and continuous testing will ensure we are building securely from the outset, while a transformed accreditation process will ensure that any minimum viable product always includes appropriate security controls and corresponding support models.

Figure 1: A plan for sustainable resilience

# Sustainable




**People: Building a pipeline of multi-skilled individuals and a security focused culture**

- A commitment to building T-shaped people and key shaped teams
- A targeted L&D strategy with a compelling employee value proposition
- A security-focused culture with just-in-time nudges and personalised narratives



**Consistency: Consistent maturity of capability regardless of environment**


- Security Posture Management
- Access controls
- Monitoring and response



**Supportability: Cost effective and operationally efficient controls**


- Greater automation and process optimisation
- Use of delivery models such as SaaS which shift the burden of support
- Simplified vendor and control estate

# Resilient




**Assurance: Pivoting from a system-centric to a business function view of assurance**

- Shift from validating system controls to protecting end-to-end business services against holistic cyber security risks
- Build upon our existing control validation to provide insightful cyber security risk assessments of critical business functions



**Recovery: Focus on strengthening our ability to recover from successful cyber attacks**

- Scenario-driven runbooks and exercising to support disaster recovery and business continuity planning
- A culture of reflection and improvement which learns from incidents and near misses
- Targeted recovery assessments on Tier 0 services



**Security-by-design: Continuing to ensure security is an essential component of architectural decisions and project delivery**

- Consistent and predictable design patterns to support security at scale
- Greater security integration with development teams and practices

---

# Executing Our Strategy

---

To fulfil our ambition, we need the right model for **funding and delivery**. The **changing technology estate and evolving external threat** are fundamentally different pressures, and our proposed investment model will recognise this. Learning from the previous decade, we will continue to use the **Programme delivery approach** for major change.

## Funding

The Bank does not have the ability to influence the investment our attackers are making into developing their own skills and capabilities; we must simply keep pace. Based on analysis of historic spend, and taking into account our current non-investment budget, we estimate the costs of doing this are **c.£3m per annum**. This number may change beyond inflation in the face of seismic events, such as a declaration of war against a hostile state, and we will review them annually, however the previous decades' experience provides us confidence that in broad terms attacker capabilities rise relatively consistently over time.

The extent of changes to the Bank's technology fluctuates more significantly year-on-year. Based on prior years' spending we estimate the investment required to keep centralised security controls in line with changing technology is **c. 2% of total technology change costs**. By calculating cyber security spend as a surcharge on wider investment we will introduce greater transparency to the cost; allowing the organisation to understand the true cost of such change without increasing cyber security risks and reducing relative maturity. The surcharge will not mean that individual programmes can disregard their own obligation to deliver change securely but will fund the requisite central capability improvements.

## Delivery

Over the last decade we have become practiced at delivering security change. Previous cyber programmes have consistently delivered on time, on budget, and in line with stated benefits. Given this, a fourth programme will be established in March 2024. This will be managed in line with standard Bank governance, and we will seek the benefits of a continuous delivery model where it makes more sense to embed delivery within operational teams.

Recognising that detailed deliverables-based planning makes it harder to respond with agility to an unpredictable external threat landscape we will focus on outcomes-based planning. Detailed benefits playbacks will support our regular discussions with the Operations & Investment Committee (OIC) and with the Audit and Risk Committee (ARCo).

# Measuring Our Progress

---

While NIST has enabled us to benchmark ourselves against recognised best practice, the key to good measurement is its ability to **support good discussions and decisions** with regards to the Bank's cyber risk management.

Moving forward we will increasingly focus on assessing **the Bank's resilience to the key cyber risks which it faces**: to anticipate, monitor, respond and learn from them. Our strategy will be built around reducing the likely HARM of these risks, either lessening their likelihood through bolstering sustainable and consistent controls, or their impact through consolidated focus on resilience.

Under the current Cyber Defence Programme, we have worked with internal and external experts to define a list of core cyber risks facing the Bank. This is a manageable and proportionate list which is meaningful to business colleagues. We have further worked to indicatively map these against the Bank's HARM table.

These mappings are an imperfect average and mask the maturity inconsistencies we recognise exist between environments like enterprise and cloud. As we develop our understanding, individualised HARM scoring by environment or business-critical process, will be used to provide greater accuracy for the relevant business owners.

Wider external factors will impact risks position against the HARM table over time; while a destructive attack by a nation-state is considered unlikely today, if the United Kingdom were to become more actively engaged in the situations in Israel/Palestine or Russia/Ukraine, then this may change quickly. The list of core risks may also change as attackers continue to use novel methods to harm organisations. The risks of decryption caused by quantum computing, or advanced social engineering through AI, are not considered sufficiently pressing to make this group today, but this may change as the technology develops. Without mitigations, and continued investment to maintain these, each of these risks would tend towards their inherent risk states of high likelihood and impact, severely outside of tolerance.

Accordingly, while we have set out here our ambitions for the risk scores in 2027, this will be an evolving picture. We will undertake a full review of the risks on an annual basis and use these risks as the frame for our regular reporting to ARCo, and in outlining the objectives and benefits of investment under a future Programme.

In all cases, the key focus is on enabling business owners and our cyber experts to have meaningful conversations about the realistic nature of the cyber security risks which the organisation will continue to face, and the impacts and limitations of mitigating actions. This will support better investment decisions and allow us to track the impact of improvement projects more usefully.

This shift is in line with the recommended risk management approach of NCSC. However, given that it will not offer us the opportunities for benchmarking which NIST has been able to provide, we will continue to use broader maturity frameworks including NIST and the government's CAF as and where these are appropriate and relevant.



Table 1: Key Cyber Risks

Risk		Residual 2023		Target 2027		Approach
<b>Data Loss</b>	Confidential or protected information exposed to unauthorised parties	L: 3 I: 4	12	L: 2 I: 4	8	Reduce likelihood through information governance controls and increased DLP through expanded technical insider detection
<b>Denial of Service</b>	Disruption because of denial-of-service attacks	L: 3 I: 3	9	L: 3 I: 2	6	Ensure appropriate DoS defences across the stack and improve monitoring techniques to limit disruption opportunity and increase early detection rate
<b>Insider</b>	Bank personnel misuse authorised access	L: 3 I: 4	12	L: 2 I: 4	8	Reduce likelihood through improved and consistent cyber hygiene across all environments and expanded technical insider detection
<b>Misconfig.</b>	Bank services disrupted by the misconfiguration of security controls	L: 2 I: 4	8	L: 1 I: 4	4	Reduce likelihood through improved and consistent cyber hygiene across all environments, strong posture management and continued cyber-safety culture
<b>Mobile Asset Loss</b>	Loss information or inappropriate access gained through lost physical hardware	L: 1 I: 3	3	L: 1 I: 3	3	Continue to ensure a low impact of lost physical hardware through comprehensive device encryption
<b>Nation-state high</b>	A nation state launches a cyber-attack using destructive techniques	L: 1 I: 5	5	L: 1 I: 4	4	Reduce impact through improved recovery capabilities
<b>Nation-state low</b>	A nation state launches a cyber-attack using non-destructive techniques (e.g. espionage)	L: 2 I: 3	6	L: 2 I: 3	6	Continue to ensure low likelihood of nation-state espionage through consistent cyber hygiene across all environments and fundamentals such as patching
<b>Patching</b>	Vulnerabilities in software are exploited by cyber-attack techniques	L: 3 I: 3	9	L: 2 I: 3	6	Reduce likelihood through consolidated obsolescence investment and simplification of the estate. Reduced impact of exploited vulnerabilities through improved recovery capabilities
<b>Phishing</b>	Bank people or services are compromised by phishing techniques	L: 3 I: 3	9	L: 2 I: 3	6	Reduce likelihood of successful phishing through continued investment in email controls; reduce impact of a successful phish through improved recovery capabilities
<b>Privilege escalation</b>	Unauthorised escalation of privilege to gain inappropriate access to data	L: 2 I: 4	8	L: 1 I: 4	4	Reduce likelihood through improved, consistent access management controls across all environments, reduced user privileges, and expanded technical insider detection
<b>Ransomware</b>	Information is lost or services disrupted by ransomware-type cyber attack	L: 3 I: 4	12	L: 2 I: 4	8	Reduce likelihood through improved and consistent cyber hygiene; reduce impact through improved recovery capabilities
<b>Supply Chain</b>	Bank's supply chain is used to launch a cyber-attack on the Bank	L: 4 I: 4	16	L: 3 I: 3	9	Reduce likelihood through better supplier vetting, triage, and assurance; reduce impact through improved recovery capabilities

# Delivery Risks

The strategy is based on several key assumptions regarding the **threat landscape**, **Bank technology and resource availability**. If these prove false, then we may not be able to deliver as anticipated.

The critical risks to our ability to deliver against the strategy as intended are:

- **Unexpected changes in the external threat landscape**

While the strategy is built to around the expectation of a changing external environment, it broadly assumes these changes will remain at the scale seen over the previous decade. Events which would cause a true step-change in the threat, either because of geo-politics, technological advances, or something else, may require us to re-evaluate the resources needed to deliver, especially if they require a diversion from long-term change to operational response activities.

- **A significant shift in our wider Technology strategy**

Technology's strategy, operating model, and target architecture are all currently evolving. This strategy is built to adapt to this evolution but is predicated on key assumptions around existing plans. If these are to change dramatically then this may necessarily require us to revisit our own strategy and priorities. As a division within the wider Technology Directorate, Cyber is well-placed to ensure we have influence and involvement in any such changes.

- **A lack of required resourcing and investment**

The scope of our ambitions and the extent to which we can reduce residual cyber-risks will remain dependent on our ability to secure appropriate resourcing. This includes requests for investment through the upcoming budget round, the maintenance of existing BAU funding at broadly consistent levels and our ability to secure and retain key skills and talent both within Cyber and in wider areas of Technology.