Nationwide Building Society

Ref	Question	Response
1.1	Have you learnt any lessons from the COVID-19 pandemic and related cyber activity that will contribute to your cyber incident response and recovery practices?	We have noticed a significant shift in the use of the C19 topic in Phishing attacks, however the broad attack vector remains the same.
1.2	To whom do you think this document should be addressed within your organisation?	Head of Cyber Security
1.3	How does your organisation link cyber incident response and recovery with the organisation's business? Does your organisation follow international standards or common frameworks? If so, which international standards or common frameworks?	The Security Strategy is aligned to and designed to specifically support the Nationwide Building Society Strategy. The Security Business Plan defines and tracks how Security will achieve the aims set out in it's Strategy. The Security Strategy is, at least annually refreshed and board approved. The Security Business Plan is a living document. This includes the main framework used by Security is ISF Standard of Best Practice (encompassing, ISO207001, PCI-DSS, NIST).
1.4	Does your organisation structure its cyber incident response and recovery activities along the seven components set out in the FSB toolkit? Please describe any additional components your organisation considers.	Nationwide Building Society use a multi-layer Incident Management escalation process. Cyber Security Incidents are managed locally within the SOC, with more significant incidents being managed within a Security Incident Process. Above that Nationwide uses an industry, Gold, Silver, Bronze approach to manage incidents and crisis events, according to risk appetite and supported by Nationwide's Risk Management Framework.
1.5	Based on your organisation's experience, please provide any additional effective practice(s) for any of the tools. Please list the number of the tool (e.g. Tools 1 – 46) and describe the effective practice(s).	Nothing further to add
1.6	Based on your organisation's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6).	Nothing further to add
1.7	What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?	Through the current Financial Services Information Exchange (FSIE)working group hosted by the UK National Computer Security Centre (NCSC), Cybersecurity Special Interest Group (CSIG) which is an operational knowledge sharing forum and direct engagement with UK National Crime Agency (NCA), UK Government Communications Headquarters (GCHQ), there is already good support from central authorities. Calling Financial Sector Cyber

		Collaboration Centre (FSCCC) meetings in response to an serious incident is already exercised regularly.
1.1	To what extent does your organisation designate roles and responsibilities as described in Tool 3? Does your organisation identify these roles by business line, technology application or department?	Nationwide Building Society operate a tiered Incident Management Process to reflect the severity of an incident. Gold is the highest whereby a Senior Management Nominee will run an Incident supported by business and operational teams. Nationwide Building Society has a Incident Management team who coordinate all management aspects including Comms and Scribe. All Media Communications are issued through the external Communications team and specific Teams are responsible for Secretariat functions (Documentation, Minutes, Action Management etc). Subject Matter Expert Teams and Senior Relationship Owners (SROs) are engaged as and when required. The SRO is the accountable representative of Nationwide Building Society with responsibility for the end-to-end relationship with a specific Third Party across the Society, including suppliers that may contain multiple services.
1.2	How does your organisation promote a non-punitive culture to avoid “too little too late” failures and accelerate information sharing and CIRR activities?	Pride Values; Annual Speak Up and Whistle Blowing Training are mandatory.
2.1	What tools and processes does your organisation have to deploy during the first days of a cyber incident?	We have a dedicated internal Forensics team, which can be increased through an external Incident response retainer with 3rd Party to support Operational Teams. Tooling includes Encase Endpoint Tool, McAfee technology stack, Microsoft Advanced Threat Protection (ATP) Defender suit, ARBOR F5 DDoS, Splunk Security Incident Event Management (SIEM) platform
2.2	Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months.	Regular exercising from table top run throughs to full testing of our Gold SIM processes.

2.3	How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)?	Nationwide Building Society Procurement operate a central process where services are risk assessed for consideration by key internal departments. Contracts are then written in association with those key areas. Under the Operational Vendor Management Policy, SROs are responsible for management of those contracts. At Contract renewal the process is re-engaged. Nationwide Building Society also operate Third Party Controls Testing function to regularly assess the controls operated by Third Parties on behalf of Nationwide Building Society.
3.1	Could you share your organisation's cyber incident analysis taxonomy and severity framework?	Evidence can be provided
3.2	What are the inputs that would be required to facilitate the analysis of a cyber incident?	We have access to Logging and Monitoring tools, forensic tools and endpoint tooling we can use to conduct analysis
3.3	What additional tools could be useful to analyse the effectiveness of cyber incident response and recovery activities and the severity, impact and root cause of cyber incidents?	Nothing further to add
3.4	What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation?	Nationwide Building Society receive and share threat intel through the following partners: SecureWorks, Microsoft, Commercial Partners, CSIG, CDA, Open Sources, Group 2, FSIE, Advanced Persistent Threat (APT) Malware Joint Working Group (JWG), DDoS Joint Working Group, Cyber Security Information Sharing Partnership (CiSP), UK NCSC , UK NCA, MK FSCCC, MWR InforSecurity Ltd (F-Secure), Internal Sources, The Royal United Services Institute Cyber Security Research Programme (RUSI) and HaveIBeenPwned (HIBP).
4.1	Besides reducing impact to business and system security, what are other considerations that need to be taken into account during mitigation?	Member and Customer Impact, nothing without Members / Customers.; how can we serve their needs through other means; i.e.. improved home working experience, and ensuring we remain compliant with any central or sector specific regulatory requirements

4.2	What tools or effective practices does your organisation have related to mitigating the impact from: (i) data breaches (ii) loss of data integrity and (iii) ransomware events?	(i) - We have Data Loss Prevention (DLP) tools to detect data loss incidents and we are applying Security Classification tooling to all out MS documents. (ii) - We have database logging to detect changes to data held in critical databases. (iii) - We have Encase and we are in the process of deploying increased Endpoint, Detection & Response (EDR) to detect Ransomware on the network. We also have Network Access Controls where we can quarantine or remove a device from the network to prevent propagation.
4.3	What tools or practices are effective for integrating the mitigation efforts of third-party service providers with the mitigation efforts of the organisation?	We have an Incident Response retainer with certain 3rd Parties to supplement our in house teams.
4.4	What additional tools could be useful for including in the component Mitigation?	Nothing further to add
4.5	Are there situations in which effective practices for mitigation and restoration activities of the organisation are the same or overlap substantially? If yes, please provide examples.	Nothing further to add
5.1	What tools and processes does your organisation have available for restoration?	On line back ups for critical systems are captured and maintained at a suitable period of time to support our Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). Offline backs up a re also kept again for an agreed period of time.
5.2	Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?	We have tiered our Services in terms of business criticality and back up and restoration plans support this.
5.3	How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?	Periodicity of backup reduces the loss of data between service outage and last known good back up. These timescales are taken to allow us to remain within appetite.
6.1	What are the most effective types of exercises, drills and tests? Why are they considered effective?	Desk top reviews allow us to flex and test what we know needs greater focus.
6.2	What are the major impediments to establishing cross-sectoral and cross-border exercises?	Scale of the sector and having such a massive variation in the size, scale and maturity of organisations within the sector. IF its too high level, organisations that are mature don't get any value, too granular and many organisations will be underprepared or find they are not able to contribute.

6.3	Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery?	Encase , Endpoint Detect and Respond tooling, CISCO Identity Services Engine and McAfee Network Access Control tooling, WireShark and Netflow for network traffic, Splunk and ServiceNow for incident management
7.1	Does your organisation distinguish “coordination activities” from broader “communication” in general? If yes, please describe the distinct nature of each component.	We have Incident Management teams who are responsible for the response, containment and recover activities. We have a dedicated Incident Communications cell who action all internal and external communication and messaging.
7.2	How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident?	For our members, Nationwide Building Society is engaged in a wide range of communication channels, traditional and more innovative (i.e.. Facebook, Twitter . . .).
7.3	Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities?	Nothing further to add.