C-Cyber Incident Response – Policy Primer

Version 03. July 2020

Principal Author: Mark Brett
Contributions: Jonathan Read Hull City Council / YHWARP
Graham Jordan Gateshead Council / NE WARP

Background

Things go wrong in ICT systems, either accidentally, a wrong parameter or filename used or a deliberate act of maleficence, to cause harm to the system, such as an attack, often through the Internet which we now refer to as a Cyber Attack.

Modern computer networks and system, can be defended automatically to deal with the majority of low level attacks, where these attacks are mitigated and solved, they are referred to as events. Where an attack or event actually causes a physical outcome (System crash, malware infection etc.), that leads to an Incident. The overall monitoring systems for dealing with systems and networks is referred to as a SEIM (Security Event & Incident Monitoring) system.

Prerequisites

Before you can do anything, you must ensure your network have a consistent and stable network time source This is a requirement for the PSN code of Connection, as without it you cannot normalise data of correlate logfiles. The NCSC Logging Made Easy [14] will help with some of this work. The NCSC produce other Incident Management information [15] that should be read and adhered to. You must have up to date detailed and accurate network diagrams [16] and systems documentation. There are plenty of drawing tools to help you do so [17]. Without neither you or an external Network response company will be able to help you, valuable time and resources will be wasted. The NCSC has a scheme (Certified Incident Response CIR) and list of trusted companies that can help [18]. The Scottish Government has also published a Cyber Resilience and Response Guide [19]. There is also a Scottish Government Cyber Playbook that can be downloaded and customised [20]. Asset registers are critical to success and will be the subject of a future C-TAG guide.

NIST Category	Technology	Aws (Amazon)	Azure (Microsoft)	Google Cloud Platform (GCP)
Identify Asset Management Risk Assessment Risk Management Strategy etc.		AWS Compliance Center,AWS Resource Tagging, AWS Config, AWS Config Rules, AWS Cloud Formation, AWS CloudTrail, AWS CloudWatch Logs, Customer Responsibility, AWS Best Practices	Azure policy, Azure AD registered devices, Cloud app Security, Microsoft Compliance Manager, Microsoft Security center, Microsoft Intelligent Security Graph, Microsoft Threat Modeling Tool, Customer Responsibility, Azure Best Practices	Security command center, GCP Resource Manager, Cloud Deployment Manager, Cloud Asset Inventory, Customer Responsibility, GCP Best Practices
Protect Access Control Awareness and Training Data Security Protective Technology etc.	**Access control**	AWS Single Sign-On, AWS Directory Service,AWS IAM, AWS Cognito, AWS MFA, AWS Config, AWS ConfigRules, AWS Cloudwatch, CloudWatch Logs, CloudTrail, VPC Flowlogs, Customer Responsibility, AWS Best Practices	Microsoft Azure Active Direcory, Microsoft Identity Manager, Azure AD app proxy, Windows security baselines,Azure Privileged Access Workstation, Azure Active Directory B2C, Customer Responsibility, Azure Best Practices	Cloud IAM, Security Key enforcement, Cloud Identity, Policy Intelligence, Identity-Aware Proxy, Titan Security key, Access Transparency, Customer Responsibility, GCP Best Practices
	privileged access management	3rd party	Microsoft Azure Active Directory privileged identity management (PAM), Enhanced Security Administrative Environment, Azure Privileged Access Workstation	3rd party
	Awareness and training	Customer Responsibility	Customer Responsibility	Customer Responsibility
	data security	AWS Trusted Advisor, AWS CloudFormation, AWS Config, AWS ConfigRules, AWS CloudTrail, AWS GuardDuty, AWS Macie, AWS Security Groups, AWS SNS , AWS VPC, AWS Secret manager, Customer Responsibility, AWS Best Practices	Azure Bitlocker, Azure VPN, Azure ExpressRoute, gateway,Microsoft Intune, Azure Security center, Windows security baselines, Azure Information Protection, Customer Responsibility, Azure Best Practices	Cloud Armor, VPC Firewall, Shielded VMs, VPC Service Controls, Customer Responsibility, GCP Best Practices
	Key management	AWS KMS, AWS HSM	Azure Key Vault, Azure HSM	Cloud HSM, Cloud KMS
	DLP	AWS Macie	Azure Information Protection, Azure DLP	Cloud Data Loss Prevention
	Encryptions	Elastic block storage (AWS EBS), efs mount, AWS Encryption Services, AWS Secrets Manager	Azure storage encryption, Azure Bitlocker, Azure SQL server encryptions	Built in, Cloud External Key Manager, Secret Manager
	backup	AWS Best Practices, Aws Backup, Customer Responsibility, AWS Best Practices	Azure Backup, Azure Site Recovery, Customer Responsibility, Azure Best Practices	Data Exporting and Importing service, Cloud Storage for data archiving, Customer Responsibility, GCP Best Practices
	Firewall	AWS Access lists, AWS Security groups, AWS Firewall manager	Azure Network Security groups, Azure Firewall	Cloud armor, VPC Firewall, Google Cloud Firewall
	IPS / IDS	Amazon GuardDuty	Microsoft Threat Protection	Security Command Center, Event Threat Detection (beta)
	Antimalware	3rd party	Microsoft Antimalware, Windows Defender ATP	Chronicle
	WAF	AWS Waf	Azure Application gateway	Cloud armor, Web Risk API
	Ddos Protection	AWS Shield	Azure Ddos Protection	Cloud armor
	Certificate Manager	AWS certificate manager	3rd party	Secret Manager
	Endpoint Protection	3rd party	Windows Defender ATP	3rd party
	Mail protection	AWS SES best practice, 3rd party	Office advanced threat protection	3rd party
	Network Protection	AWS VPC, AWS privateLink, Customer Responsibility, AWS Best Practices	Azure virtual network, Azure ExpressRoute, Azure Network Security, Customer Responsibility, Azure Best Practices	Virtual Private Cloud (VPC)
	API Management	Amazon API Gateway	Azure API Management	Apigee (Api Management)
	Load Balancer	Elastic load balancer, Cloudfront	Azure load balancer	Cloud Load Balancing
	VPN	VPC Customer gateway	Azure vpn gateway	Hybrid Connectivity
	SSL Decryption	AWS Elastic load balancer	Azure application gateway	Https Load Balancing
	Vuln Assessments	Inspector, Trusted Advisor	AZURE Security Center	Cloud security scanner
Detect Anomalies and Events Security Continuous Monitoring Detection Processes		aws security hub, AWS Cloudwatch, CloudTrail, VPC Flowlogs, AWS Config, AWS Organizations, AWS Firewall Manager, AWS PrivateLink, AWS Systems Manager, Amazon Macie, AWS Managed Services, Amazon SNS, Customer Responsibility, AWS Best Practices	Azure monitor, Microsoft azure audit log management, Azure Log analytics, Azure AD Auditing, Azure Anomaly Detection, Azure Advanced Threat Analytics, Microsoft Cloud App Security, Azure Security Center, Azure Log Integration, Azure Active Directory risk detections, Customer Responsibility, Azure Best Practices	Cloud Audit Logs, Stackdriver logging and monitoring, Network Intelligence Center, Network Telemetry, Cloud Logging, Cloud Monitoring, Cloud Trace, Error Reporting, Service Monitoring, Kubernetes Engine Monitoring, Access Transparency, Customer Responsibility, GCP Best Practices
Respond Response Planning Analysis etc.		CloudFormation,amazon sns, amazon ses, AWS Cloudwatch, CloudTrail, VPC Flow Logs, AWS Firewall Manager, Customer Responsibility, AWS Best Practices	Microsoft Incident Response and Recovery Process, Windows Defender ATP, Azure Firewall, Azure Notifications Hub, Azure Service Bus, Customer Responsibility, Azure Best Practices	Incident Response and Management, Cloud Armor, Chronicle, Cloud Scheduler, Google Cloud firewall, Customer Responsibility, GCP Best Practices
Recover Recovery Planning Improvements		Aws Backup, Customer Responsibility, AWS Best Practices	Azure Backup, Azure Site Recovery,Customer Responsibility, Azure Best Practices	Google storage backup, object versioning, Data Exporting and Importing service, Cloud Storage for data archiving, Customer Responsibility, GCP Best Practices

Defining Incident Response

We've discussed events and what leads to an incident. When an incident happens, the first thing that needs to happened is to actually be aware of the attack. Some attacks can go undetected for months. This is why we ensure that systems are secure by design, this is the who purpose of Information Assurance and Risk Management. The only objective of Incident Response is to get to the make safe point, where the unwanted systems / network behaviour is stopped in its tracks. Once at make safe, the next and longer phase is Incident Recovery. The objective of the recovery phase itself is to get the system / network back to a stable state, that is how the network or system was at the point the incident happened. Incident recovery is not about improvement. Both Incident response and Incident recovery have clearly defined boundaries.

An incident can be thought of as a fast time resource intensive project. and if thought of as such, with a start, middle and end it becomes far easier to know when and incident is concluded. Open ended Incidents are not good practice and allow non-incident related issues to be introduced, causing complications and additional complexities.

Where to start?

Planning

There is an ISO standard for Incident response ISO 27035 [1] as with all standards, it details an approach and linked nicely with ISO 27001, ISO 27035 with it's five stage approach;

1. **Plan and prepare:** establish an information security incident management policy, form an **I**ncident **R**esponse **T**eam *etc.*
2. **Detection and reporting:** someone has to spot and report "events" that might be or turn into incidents;
3. **Assessment and decision:** someone must assess the situation to determine whether it is in fact an incident;
4. **Responses:** contain, eradicate, recover from and forensically analyze the incident, where appropriate;
5. **Lessons learnt:** make systematic improvements to the organization's management of information risks as a consequence of incidents experienced.

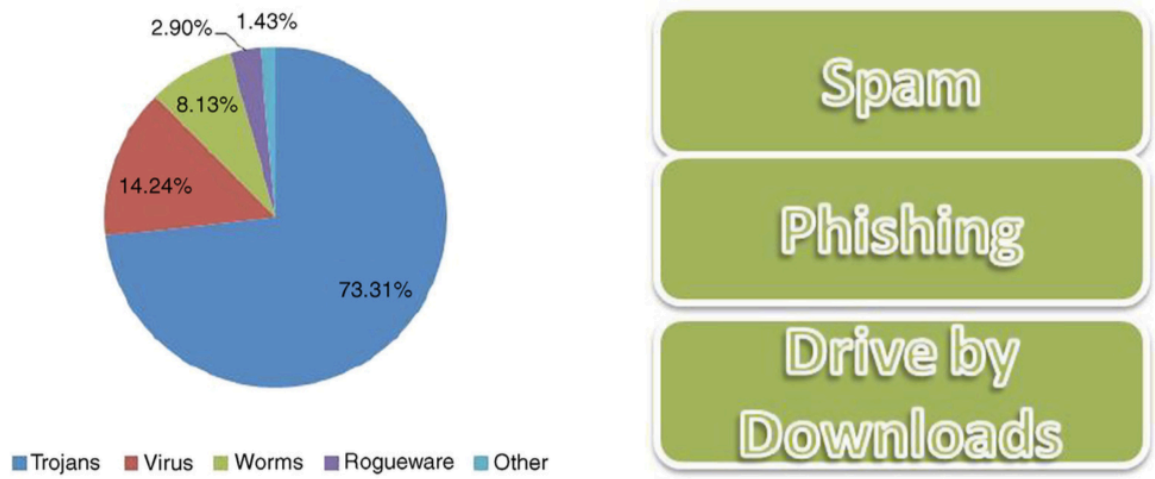


Fig. 2. Types of malware and mediums to spread them [101].

Source: Ref [22]

The figure above shows the types of attack vectors, how the malicious code / data gets into the network / system.

There's also the American NIST Incident handling guide [2] NIST SP800-61 revision 2. This dates back to 2012, but does contain a lot of useful advice and guidance. For specific cloud related guidance the Cloud Security Alliance has an incident response guide [26].

The NIST approach discusses;

- Preparation (Planning)
- Detection and Analysis (Response)
- Containment (Make safe)
- Post-incident action (Recovery)
-

The Erez Dasa table above shows how these can map across to technologies in the cloud.

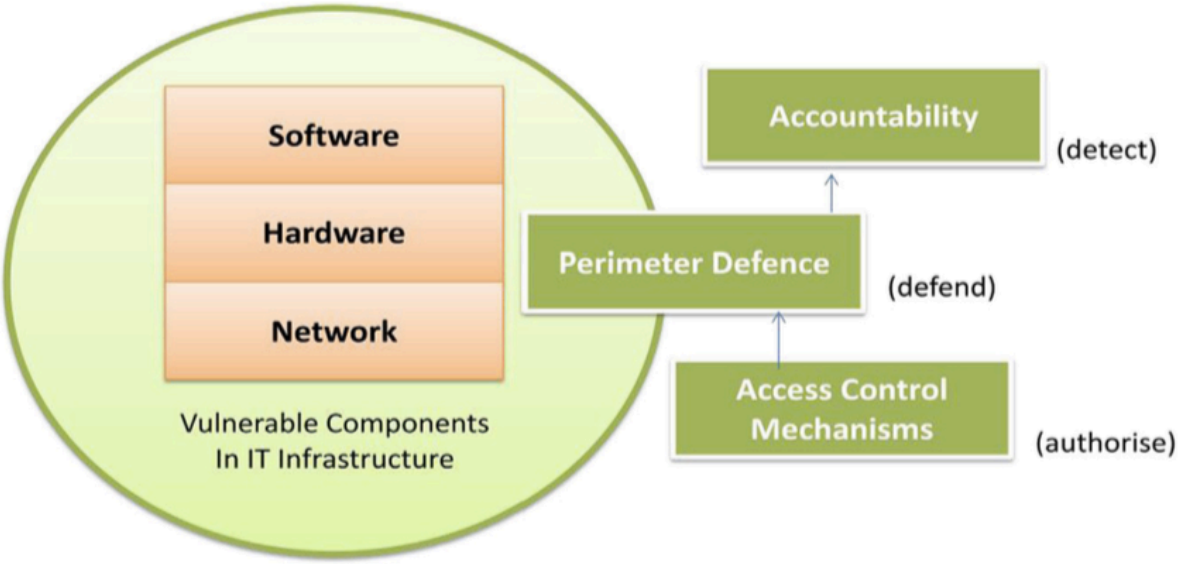


Fig. 1. Vulnerabilities and defense strategies in existing systems.

Source: Ref [22]

Some very good examples of incident playbook (think of plans or recipes as we're in a cook book), can be found here [3] the approach is very good. Whilst Forensics are out of scope for this paper, there is an excellent primer and source of information from SANS to be found here [4]. Sans also produces an incident handlers guide that can be found here [5].

Exercising

We have discussed exercising, the MHCLG Pathfinder programme delivered a number of Cyber Exercises [6]. The NCSC have produced the Exercise in a box suite, that can be freely downloaded and contains all of the materials needed to plan and run a successful cyber exercise [7]. For really in depth guidance the Mitre Exercise planning guide is a comprehensive and authoritative guide [8].

Responding

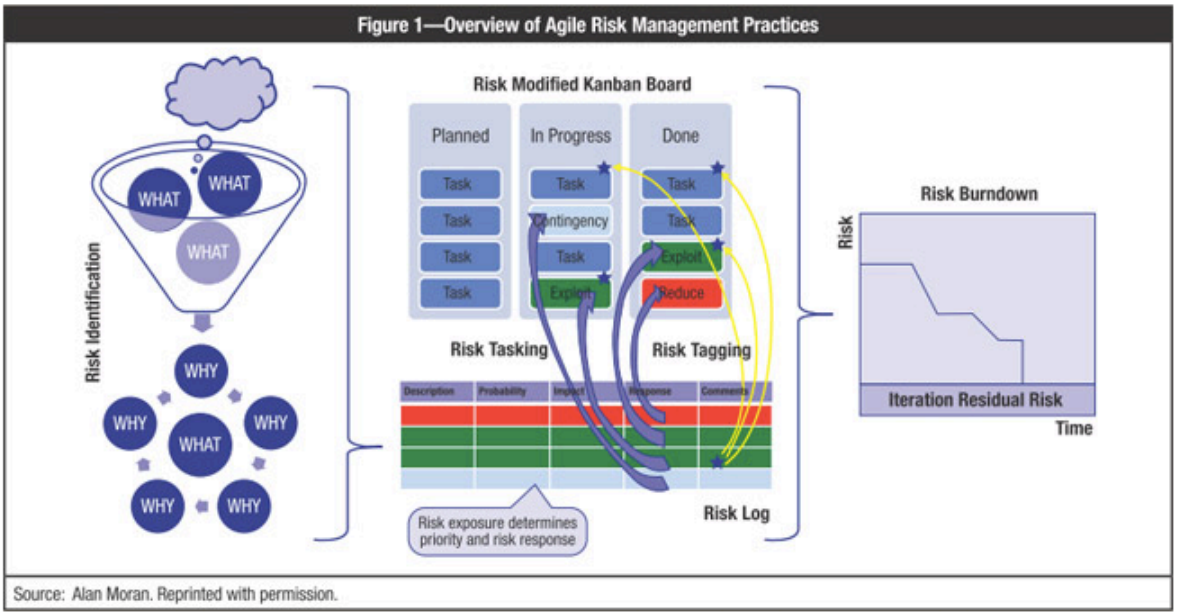
Responding to Cyber incidents will always be different to what you've planned for. The idea of planning is more about trying to understand the decisions, line of communications and the team

building experience. Plans make you think about scenarios, which can be exercised. All incidents will need resources. The FT produced a useful report "Surviving a Cyber Incident" containing a lot of sage advice [9]. For information, have a look at the Golden Hour Guide which is described in the Cyber Incident Framework [10] the paper also contains a number of useful case studies and other information.

The guide also discusses the NLAWARP / Silverthorn SIRO Risk framework © , with it's six stages, mapping

1) Identify and map out key systems / services /suppliers
2) Identifying how we get assurance for key systems services / suppliers
3) Identifying Key Information Risks (to develop Key Risk Indicators (KRIs)
4) Articulating Information Risk Statements (Risk / Threat/ Vulnerability/Exploit)
5) Defining Risk Appetite [25] (Taking 1-4 above identifying assurance gaps).
6) Articulating a Risk Appetite (Using business language [User Stories] [23])

User stories are incredible powerful for Risk Management, Cyber Exercising and for testing assumptions. Risk Poker [24] is another useful way to articulate the risks.



Source Isaca [23]

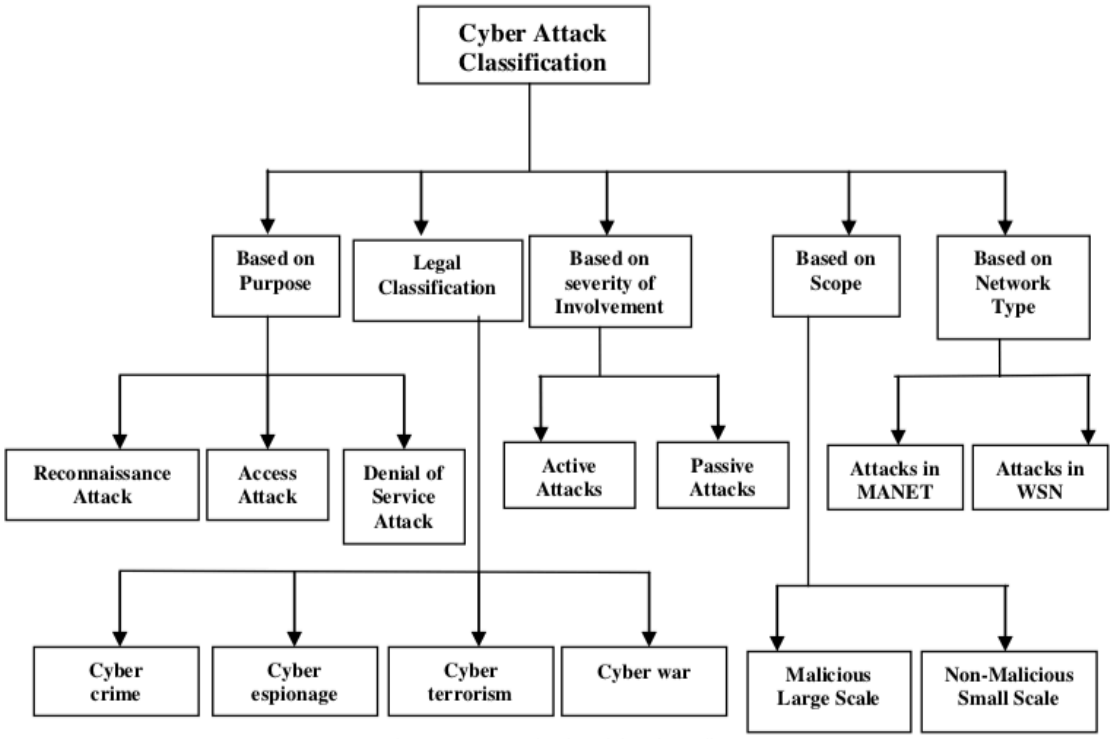


Figure 1: Attack classification diagram

Source: Figure 1 above and table below; Cyber Incidents: Uma, M. and Padmavathi Ganapathi. "A Survey on Various Cyber Attacks and their Classification." *I. J. Network Security* 15 (2013): 390-396. Ref [21]

Table 1: Different types of attacks

Name of the Attacks	Description	Examples
Reconnaissance Attacks	Type of attack which involves unauthorized detection system mapping and services to steal data	a) Packet sniffers, b) Port scanning, c) Ping sweeps and d) DNS(Distributed Network Services) Queries
Access Attacks	An attack where intruder gains access to a device to which he has no right for access	a) Port trust utilization b) Port redirection c) Dictionary attacks d) Man-in-the-middle attacks e) Social engineering attacks and Phising
Denial of Service	Intrusion into a system by disabling the network with the intent to deny service to authorized users	a) Smurf b) SYN Flood c) DNS attacks d) DDos(Distributed Denial of Services)
Cyber crime	The use of computers and the internet to exploit users for materialistic gain	a) Identity theft b) Credit card fraud
Cyber espionage	The act of using the internet to spy on others for gaining benefit	a) Tracking cookies b) RAT controllable
Cyber terrorism	The use of cyber space for creating large scale disruption and destruction of life and property	a) Crashing the power grids by al-Qaeda via a network b) Poisoning of the water supply
Cyberwar	The act of a nation with the intention of disruption of another nations network to gain tactical and military advantages	a) Russia's war on Estonia (2007) b) Russia's war on Georgia (2008)
Active Attacks	An attack with data transmission to all parties thereby acting as a liaison enabling severe compromise	a) Masquerade b) Reply c) Modification of message
Passive Attacks	An attack which is primarily eaves dropping without meddling with the database	a) Traffic analysis b) Release of message contents
Malicious Attacks	An attack with a deliberate intent to cause harm resulting in large scale disruption	a) Sasser Attack
Non Malicious Attacks	Accidental attack due to mis-handling or operational mistakes with minor loss of data	a) Registry corruption b) Accidental erasing of hard disk
Attacks in MANET	Attacks which aims to slow or stop the flow of information between the nodes	a) Byzantine Attacks b) Black Hole Attack c) Flood Rushing Attack d) Byzantine Wormhole Attack
Attacks on WSN	An attack which prevents the sensors from detecting and transmitting information through the network	a) Application Layer Attacks b) Transport Layer Attacks c) Network Layer Attacks d) Multi Layer Attacks

Recovering

Do not underestimate the amount of time a Cyber attack will take to resolve. As we said earlier the incident part only goes as far as “Making Safe”, (Containment). The hard works starts with the recovery phase. It could take weeks, months or years to completely get back to normal. You need to plan for that and have that as a “Planning Assumption”. The NCSC list some helpful context about planning assumptions in dealing with suppliers [11]. You need to undertake Horizon scanning [12] and a Risk Assessment with a Threat analysis, the UK space Agency has produced a useful Cyber Toolkit which explores these areas [13]. so that you can prioritise your planning assumptions.

Procuring help to recover from an incident (NE WARP Case study)

our objectives:

- To have a ready-to-go incident response service to hand for whenever required
- To have the option of annual readiness check in terms of required documentation etc. that would be requested by an incoming response service

options:

- procure up front and have on standby
- procure at the time of need

- use CCS (Crown Commercial Services) dynamic purchasing system for cyber which includes NCSC CIR (Cyber Incident Response) providers
- conduct a local procurement

In the event of a critical incident requiring incident response it is likely emergency procurement would be possible. However, we'd still need to find and identify potential suppliers, explain our situation and what we think we need, enquire of their availability and costs.

Preferred route – CCS DPS

CCS DPS has minimum 10-day turnaround, clearly not appropriate for Incident Response at the time of need. NE WARP is looking to discuss with suppliers to agree to reduce this.

Buyers would need to follow the DPS buying process, complete necessary documents and be happy with the 'legal basis'- this would require procurement resource at the time of need - however templates etc could be developed. This is something that needs to be factored in to the planning assumptions.

References

1 ISO 27035: https://www.iso27001security.com/html/27035.html
2 NIST Incident Handling Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

3 Incident Playbook examples: https://www.incidentresponse.com/playbooks/

4 Sans Forensics Planning Guide: https://www.giac.org/paper/gcfa/283/forensic-investigation-plan-cookbook/108356

5 Sans Incident Handlers Guide: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

6 MHCLG PAthfinder Programme: https://www.local.gov.uk/cyber-pathfinder-training-scheme

7 NCSC Exercise in a box: https://www.ncsc.gov.uk/information/exercise-in-a-box

8 Mitre Exercise Planning Guide: https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

9 FT Guide to Cyber Incident Survival: https://ig.ft.com/sites/special-reports/cyber-attacks/

10 Cyber Golden Hour Guide: https://www.researchgate.net/publication/336400438_Cyber_Incident_Approach_Framework_for_Local_Government_-_Cyber_Incident_Approach_Framework_for_Local_Government

11 Cyber Planning Assumptions: https://www.ncsc.gov.uk/collection/board-toolkit/collaborating-with-suppliers-and-partners

12 Horizon Scanning Toolkit: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674209/futures-toolkit-edition-1.pdf

13 UK Space Agency Cyber Toolkit: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885869/Space_cyber_toolkit_final_v4.pdf

14 NCSC Logging Made Easy: https://www.ncsc.gov.uk/blog-post/logging-made-easy

15 NCSC Incident Management guidance: https://www.ncsc.gov.uk/section/about-ncsc/incident-management

16 Network Diagrams blog: http://networkdiagram101.com/

17 Network Diagram tools: https://www.lucidchart.com/blog/network-diagramming-best-practices

18 NCSC Certified Incident Response Companies: https://www.ncsc.gov.uk/information/cir-cyber-incident-response

19 Scottish Government Guide: https://www.gov.scot/binaries/content/documents/govscot/publications/advice-and-guidance/2019/10/cyber-resilience-guidance/documents/cyber-resilience-resource-toolkit/cyber-resilience-resource-toolkit/govscot%3Adocument/Cyber%2BResilience%2BResource%2BToolkit.pdf

20 Scottish Govt Cyber Playbook template: https://www.gov.scot/binaries/content/documents/govscot/publications/advice-and-guidance/2019/10/cyber-resilience-incident-management/documents/cyber-incident-response-denial-of-service-playbook/cyber-incident-response-denial-of-service-playbook/govscot%3Adocument/Cyber%2BCapability%2BToolkit%2B-%2BCyber%2BIncident%2BResponse%2B-%2BDenial%2Bof%2BService%2BPlaybook%2Bv2.3.pdf

21 Catergorising Cyber Incidents: Uma, M. and Padmavathi Ganapathi. “A Survey on Various Cyber Attacks and their Classification.” *I. J. Network Security* 15 (2013): 390-396.

22 Emergent Cyber Threats: https://reader.elsevier.com/reader/sd/pii/S0022000014000178

23 Risk in user stories: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-2/risk-management-in-agile-projects

24 Risk Poker: https://www.tmap.net/wiki/risk-poker

25 Articulating Risk Statements: https://www.ascentor.co.uk/2015/07/10-top-tips-writing-information-risk-appetite-statements/

26 Cloud Security Alliance Incident response: https://cloudsecurityalliance.org/research/working-groups/cloud-incident-response/