

# COMP3010

## Security Operations & Incident Management

### *Table of Contents*

Introduction .....	2
Acquisition .....	2
Identification .....	3
Preparation .....	4
Approach Strategy .....	5
Preservation & Collection of Evidence.....	6
Examination & Analysis.....	8
Evidence Presentation .....	13
Conclusion.....	14
References & Appendices .....	15
Appendix 1 – Acronyms/Abbreviations (in order of appearance).....	29

## Introduction

Unfortunately, online banks are no stranger to targeted cyber-attacks due to the high accuracy and consistency of customer and financial information. Concurrently, attacks on ATM's have been growing over the past decade (Kok, 2019) thanks to the reliance and interconnectivity of outdated or vulnerable software (Kumire, 2020). This is further compounded by the expansion of potentially vulnerable services (e.g. mobile top-up) ATM's offer (Cluckey, 2013). Cyber-attacks on bank's do not necessarily require an insider to open access from inside the ATM network (as seen in Figure 1). In summary, any one of these vulnerabilities could be an avenue to the DOS\* attack that devastated Local Banking Ltd\*. As an SME\*, they likely struggled financially to implement appropriate preparatory countermeasures (Ginovsky, 2014).

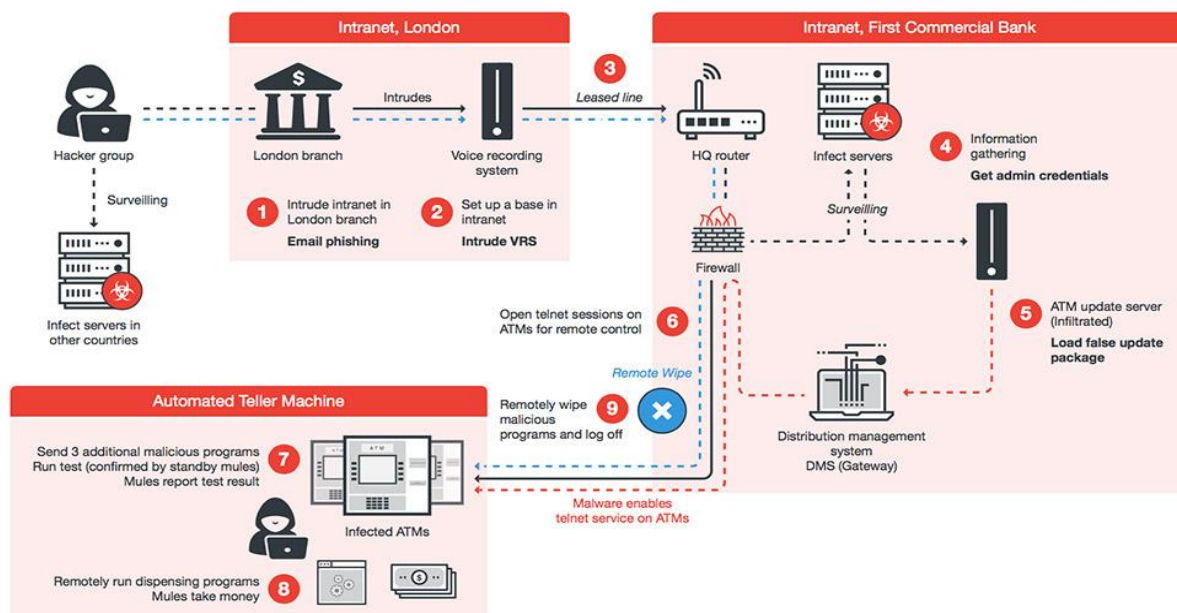


Figure 1: Taiwan network attack (Schwartz, 2017)

In this paper, I will be illuminating an ideal investigation strategy and initial countermeasure recommendations that will mitigate current and future attacks. Each section will be further divided down into short term (mitigation of existing breach damage) and long term (prevention of future breaches) timescales, as well as limitation factors and further options to show a broad spectrum of what will plausibly be deployed.

## Acquisition

The acquisition step is an initial preparatory step, utilising several phases of the ADFM\* framework (Saleem, et al., 2014) as shown in Figure 2. This framework is more useful than its predecessor (Digital

Forensics Model - DFM) thanks to the higher documentation quality, increased relevant phase count and suitability to situations where the attack has already occurred. This framework does not come without problems as efforts can be duplicated between the phases (Shrivastava, et al., 2012). The first phase of investigation will be obtention of evidence and identification of attack vectors and malicious actors (Yusoff, et al., 2011).

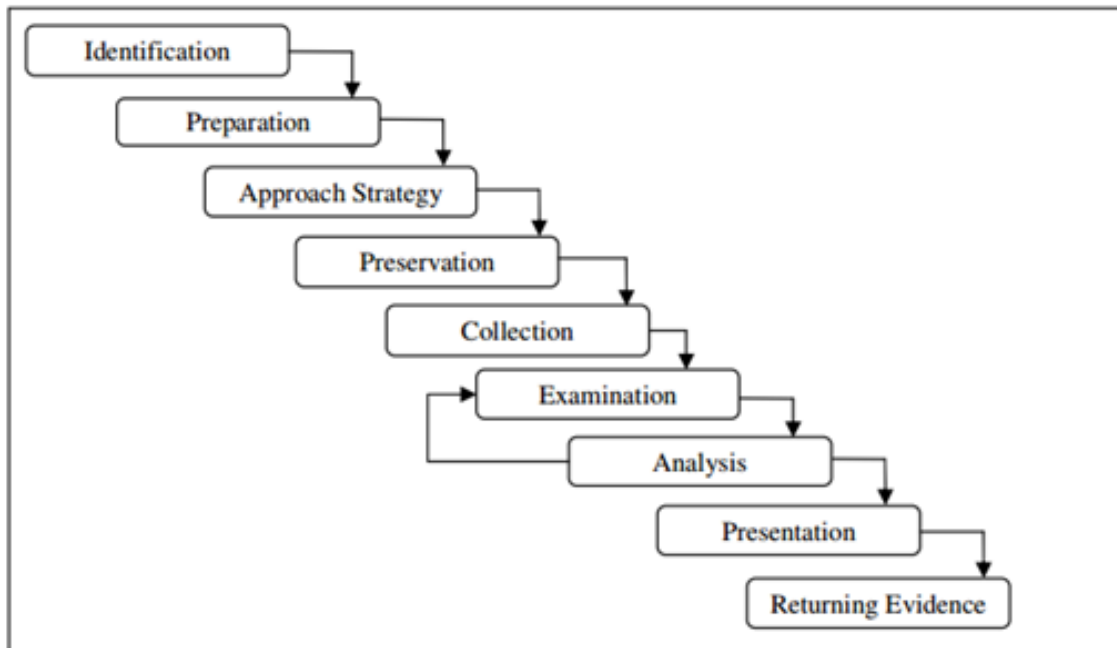


Figure 2: Abstract Digital Forensics Model (Tahiri, 2016)

## Identification

The first step would be to identify basic quirks of the breach, following fingerprints left behind by the antagonist to reveal which services, customers and employees are affected. Identification of an attack will not only determine the route of the inquiry but also at-risk assets (Reith, et al., 2002). Ideally, Local Banking should have an asset inventory (Corporate Finance Institute, 2021), defining digital and physical assets, and a risk analysis strategy (Rouse, 2020) exploring cyber-attacks on these assets (The Hartman Team, 2020). These will be deployed in the preparation phase, while also serving as a useful starting reference for identifying upcoming tasks to complete.

Although the initial view claims an infection of DOS seeding malware, it is possible the attack could be more sinister than that by advanced malware or a persistent insider. Short term, the investigation will need to uncover whether the bank was specifically targeted and the scope of said attack. A good start would be to examine Snort IDS network logs

and frequency of customer complaints to establish when and where the attack originated from (Gogoi & Mishra, 2018). If no logs exist/implemented (Murphy, 2021), that will summarily point to the malware being more advanced than initially thought, especially if high honeypot activity is present (Antonopoulos, 2010). Even from malware sources on the inside (snort IPS can be deployed on internal and external switches or firewalls (Koychev, 2015), see Figure 3). If logs reveal the incoming flood traffic was from an external IP(s), then the attack was unlikely to have been directly instantiated by malware on the ATM's and could be a DDOS\* attack if it came from multiple IP's.

```
alert icmp any any -> $HOME_NET any (msg:"ICMP flood"; sid:1000001; rev:1;
classtype:icmp-event; detection_filter:track by_dst, count 500, seconds 3;)
```

```
alert tcp any any -> $HOME_NET 80 (flags: S; msg:"Possible DoS Attack Type : SYN
flood"; flow:stateless; sid:3; detection_filter:track by_dst, count 20, seconds 10;)
```

*Figure 3: Snort rules to identify DOS attacks. The top rule detects ICMP\* flooding, the bottom detects SYN flooding. If either rule detects more request than it is 'count' option, an alert log will be triggered (Gogoi & Mishra, 2018)*

Logs would also be valuable for determining if the previously mentioned malware has propagated on the ATM network (King & Williams, 2014). Multifunctional malware is on the rise (Soni, 2018), banking trojans being in the top 3 proliferating malware types. So it is entirely possible that DOS is only one feature of the malicious program. Since user's occasionally do not have their cards returned, network data will be correlated for suspicious patterns to unknown IP addresses.

## Preparation

The preparation phase is the preliminary step before the actual investigation, where resources and support will be gathered to investigate the breach, defining how to apply tools effectively without collateral damage. Providing planning space to countermeasure deployment, training staff and smarter defences will reduce breach severity escalation (Ellis, 2021) and future breach possibility (Rapid7, 2017). Without a preparatory step, further damage to network infrastructure could occur by delving into the bank's systems with poorly configured tools, little training in how to use them and without proper authority. All of which would be detrimental factors to our overall strategy (UK Government, 2021).

To deal with the current attack, one possibility is a 4-layer strategy to be devised (Sharifi, et al., 2019), consisting of 3 layers with an additional

preliminary resource obtention step. The initial operation and deployment costs would be extensive if using an outside company (Scott, 2014) but would likely only need to be done once if the infrastructure remains in place. Funding would need to be secured for this and likely insured in case the approach strategy fails (ABI, 2021). Insurance plans focussing on customer data would be a wise choice in the early steps to cover financially crippling exposure of data (itgovernance, 2018).

Long term awareness would be difficult to specialise due to the wide range of DOS types (Hamilton, 2018). As an SME, they are unlikely to have the technical expertise and resources available to train staff long term. Fortunately, there are companies who will outsource cyber training solutions (European Union Agency for Cybersecurity, 2021) until Local Banking has the capability to implement their own cyber awareness program. The training would be important as it would cover both what to do in the event of a breach (DOS or otherwise) and reduce avenues of entry to phishing malware.

### Approach Strategy

The approach strategy depicts how tools and techniques, gathered in the preparatory phase, will be applied following ISO27041 (SecAware, 2015) to gather evidence. ATM network logs, ATM maintenance personal whereabouts, ATM's accessed and other entities of any system interacting with the ATM network are key examples of evidence. To justify the need, consider consequences of a sloppy Snort implementation to generate alerts (figure 3). While useful for identifying incriminating fingerprints, outdated ATM's systems may suffer a self-inflicted DOS (Slattery, 2011). An approach strategy must ensure the investigation services are not further damaged, or staff impeded, (IPRR, 2009) while forcing a successful conclusion out of the investigation (James, 2015).

The possibility of an insider being present should be unearthed with caution. The low employee count works in the investigations favour, less users to examine and each employee is likely to have multiple control assets entrusted to them (Amrin, 2015). On the other hand, any investigation into employee's needs to be done as openly and sensitively as possible (Intersoft Consulting, 2018) to conform to local and international privacy regulations (e.g. Article 13, GDPR/Data Protection Act 2018), facing employee (Leccisotti, 2015) or legal consequences in

default. Visitor logs should see the same scrutiny and examination. Employee access to ATM, network and server assets should be reviewed and revoked if they do not need it. Furthermore, Login credentials should be available to at least one other employee to prevent system lockout (Watchguard, 2008). A permission hierarchy and appeal process could be setup to allow access levels to be granted or denied (Nominet UK, 2020) using appropriate technologies (such as the Thycotic Identity Bridge (Hunter, 2020)). To allow for compatibility and accessibility across multiple system types, a tailored roll out plan should be devised for separate teams. Finally, Local Banking should be backing up what data can be onto trusted servers per a Disaster Recovery Plan (Net Vault, 2020). Restoring from backup in this DOS instance would be a last resort due to the forementioned disruption to employee's.

Considering institution size, approach strategy will detail regular, easily planned, interchangeable training (Jones, 2020). Training will focus on top threats employees are likely to face (Witts, 2021) and banking related threats (e.g. fraudulent financial information requests). To further boost security awareness and ward off deliberate sabotage, a tailored security policy would be founded for employee's to be tested against (UK Domain, 2020).

### Preservation & Collection of Evidence

Once the approach strategy has been improved, it is enacted upon to the standards of 4 principles (see Figure 4). Principle 1 (approach strategy) has already been alluded to so principle 2 (only investigators gather evidence and little interference from upper management is encountered) and principle 3 (preserving and signing off data in as original a format as possible) will be the focus here (media, 2016). The preservation phase will be the prelude of the collection phase, concerning the securement and processes of

#### Four principles are involved:

##### Principle 1:

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

##### Principle 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

##### Principle 3:

An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

##### Principle 4:

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

*Figure 4: Principles of preserving and collecting electronic evidence that the approach strategy will apply to the situation (Association of Chief Police Officers, 2021)*



security incident evidence. The evidence will be both physical and digital, likely with different privacy access levels, so there is an expectation for this phase to take the longest. Especially if the access level requires board approval and background checks (KPMG, 2018). Arguably, preservation of obtained evidence can be easily overlooked by the more practical phases due to the rapid pace of the investigation (DFLabs, 2019). This is even more true for Local Banking, where the size of the investigation will be relatively small and quick compared to larger corporations. However, it is no less important than the practical phases since corrupted or lost evidence would be extremely demoralising for the small investigation. The malware itself will likely contain rootkits and other tools to obscure it from the investigation detection sweeps, especially if it has propagated to the bank's cloud resources (Park, et al., 2012). The first responder to the attack should ensure a systematic investigation is undertaken on the bank's network (should be possible considering the size of the organisation) for these hidden dangers. A first responder to the investigation should also ensure the collection of evidence is prioritised by volatility downwards, maximising collection (Veber & Smutny, 2015). Furthermore, preservation is imperative for insuring evidence examination is accurate and for establishing the scope of the DOS attack. How they should do this will depend on the final approach strategy and incident standards such as ISO27037 (Cloud Security Alliance, 2013). Of note, different systems in the bank will have different quirks and incompatibilities with each other (e.g. old ATM Windows operating systems mentioned earlier would be incompatible with UNIX powered servers). Therefore, the corruption of data could occur if it is altered on one system and loaded on another. To complicate matters further, evidence on different systems will be in separate locations to one another. For example, mobile devices are utilised heavily in today's advancing world and a lot of Local Banking employee's will be likely to possess at least 1 such device at work (Silver, 2019). A malicious or oblivious insider that possess an infected mobile device could have, theoretically, connected to the bank's wireless network (or a terminal with Bluetooth) and uploaded malware to Local Banking (Kaspersky, 2020). As such, the investigation may also have to delve into mobile forensic analysis and evidence collection on device metadata (Benkhelifa, et al., 2016). Extrapolating the data can be difficult due to the lack of affordable knowledge (Writers, 2016) and political freedom, especially considering previously referenced legal ramifications. But, if Local Banking can accept or work through these

problems before they can occur, they may find that extraction tools will be able to automatically dump evidence files straight to the investigator (Efe & Akyol, 2019). There are also standards that specifically related to mobile forensic examinations that would need to be complied to throughout the investigation (Ayers, 2017). For example, CFT-IM-10 (Mukasey, et al., 2008) asserts “tools must be able to present acquired data elements in a human readable format”. CFT-IM-10 would need to be referenced when examining executable and binary applications and files for evidence of malicious software that could relate to Local Banking’s cyber incidents.

In the long term, it may be true that malware on the systems is more advanced than initially thought, requiring a digital forensics expert. Furthermore, physical evidence potentially relating to the malware’s installation is likely spread across the bank chain’s multiple locations (Osbourne, 2021). To ensure tracking integrity of evidence is upheld, digital and physical evidence gathered should be documented and securely stored appropriately based on its type. Mostly conducted for a scenario where said digital forensics expert would need to be contracted to investigate the breach, it is also done to ensure volatile evidence (e.g. ATM RAM, live access records) is not put in jeopardy (SecAware, 2021). Afterall, this is a criminal investigation as much as an internal one (under the Computer Misuse Act 1990) meaning the police and judges would also need to view evidence in its original form (National Crime Agency, 2021). The preservation of all gathered evidence in the long term would be crucial to this end (IDRISSI, 2019). LTDP\* of key evidence including but not exclusive to:

- Access and activity logs on networks linked to the ATM system, prioritising the most volatile locations and initial ‘ground-zero’ site where the breach was first detected.
- Snort alerts and Wireshark activity monitoring correlating user logs to significant events.
- Historical security reports and file integrity records conducted on the system within the past year (Exabeam, 2017).
- Employee incident history that may indicate employees who would be more likely to have caused the attack.

## **Examination & Analysis**

Now that evidence has been identified, gathered, planned and collected in a secure manner, analysis can begin on both the evidence and



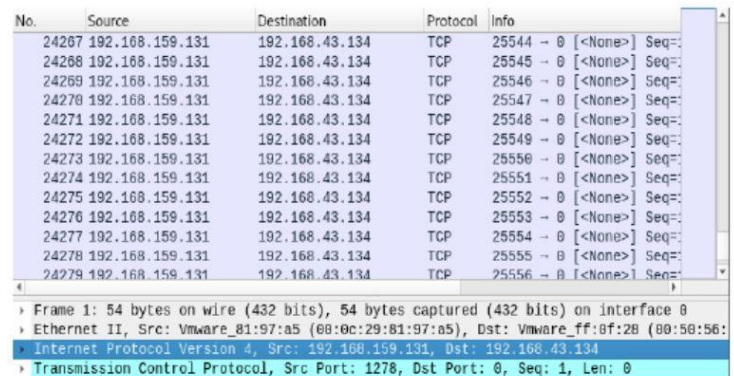
procedure. Establishing a retrospective of both the incident and investigation will foster more efficient and effective responses in the future (Ghafur, et al., 2019). Such analysis comes with caveats in the form of interpretation by different parties, along with how the organisation itself responds to incident. Without a qualified CERT\*, the examination & analysis would need to ensure it honours ISO27042 (Marshall, 2015) to please all evidence-doubting parties. Other standards include ISO27043 (SecAware, 2015) which shall be touched upon when analysing the worth of examined evidence.

There are several tools and techniques that will be used to investigate both the evidence:

#### ❖ Network analysis

##### ○ Wireshark

- Used to attempt to tie back DOS streams back to an initial user account or machine (Iqbal & Naaz, 2019). The logs gathered in the previous phases will indicate high counts of superfluous requests, even if they have been blocked by Local Banking's firewall.



No.	Source	Destination	Protocol	Info
24267	192.168.159.131	192.168.43.134	TCP	25544 → 0 [<None> Seq=
24268	192.168.159.131	192.168.43.134	TCP	25545 → 0 [<None> Seq=
24269	192.168.159.131	192.168.43.134	TCP	25546 → 0 [<None> Seq=
24270	192.168.159.131	192.168.43.134	TCP	25547 → 0 [<None> Seq=
24271	192.168.159.131	192.168.43.134	TCP	25548 → 0 [<None> Seq=
24272	192.168.159.131	192.168.43.134	TCP	25549 → 0 [<None> Seq=
24273	192.168.159.131	192.168.43.134	TCP	25550 → 0 [<None> Seq=
24274	192.168.159.131	192.168.43.134	TCP	25551 → 0 [<None> Seq=
24275	192.168.159.131	192.168.43.134	TCP	25552 → 0 [<None> Seq=
24276	192.168.159.131	192.168.43.134	TCP	25553 → 0 [<None> Seq=
24277	192.168.159.131	192.168.43.134	TCP	25554 → 0 [<None> Seq=
24278	192.168.159.131	192.168.43.134	TCP	25555 → 0 [<None> Seq=
24279	192.168.159.131	192.168.43.134	TCP	25556 → 0 [<None> Seq=

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
 Ethernet II, Src: Vmware\_81:97:a5 (08:0c:29:81:97:a5), Dst: Vmware\_ff:ff:ff:ff:ff:ff (08:00:00:00:00:00)  
 Internet Protocol Version 4, Src: 192.168.159.131, Dst: 192.168.43.134  
 Transmission Control Protocol, Src Port: 1278, Dst Port: 0, Seq: 1, Len: 0

Figure 5: SYN Flood attack in Wireshark (Iqbal & Naaz, 2019)

- By filtering packets by protocol and flags, logs will usually be able to identify what DOS type (Imperva, 2021) it is and where it is coming from to block the requests (see Figure 5 for an example DOS SYN flood attack in Wireshark) using a NIPS. Local Banking will likely wish to avoid blocking legitimate IP address (if the source IP of the packets has been spoofed), so a migration to IPv6 for the bank's network might be suitable as it provides additional packing crafting stages that will make IP spoofing harder (Kaspersky, 2018).
- A migration to IPv6 will not be easy or quick (Internet Society, 2017), especially for an SME (Tarzey, 2012) with outdated software. On the other hand, Wireshark would be a valid investigational tool as it is free software that only requires access to the network to function.

- Snort or alternative system
  - This really should tie more into the analysis side of the investigation, but some parts of Snort would be useful for the initial examination.
  - Network (ATM network) and host (ATM machines) intrusion prevention systems, when used in combination, are effective methods of stopping DOS attacks in progress (Harris, 2006). The HIPS would limit monlist() and other DOS abusable API calls on the ATM's themselves (FortiGuard Labs, 2019) where NIPS can intercept DOS incoming or outgoing DOS streams on the ATM network.
  - Local Banking will need to consider both the limitations and human factors of these systems. HIPS needs to be watched for regressions on OS upgrades and system performance problems, while NIPS can suffer from the same DOS effects as the system it is installed to watch (Paquet, 2009)! Outsourcing management of such systems can reduce the human workload but this brings in financial concerns of such a move (Secureworks, 2011).
  - For example, the generic intrusion detection model (Katsikas, 2017) will reflect actual snort development processes. As events are created, the model is adjusted to best benefit from the events, sometimes without human intervention! (Ganesan, et al., 2019). Snort IDS mode can send a termination signal (TCP Reset or ICMP Unreachable) to the infected ATM systems automatically, stopping the DOS streams (Carter & Stiffler, 2001).
  - Accordingly, the snort model will parse events on the fly and automatically detect the DOS attacks in the bank's systems as they occur! Additional plugins could also be emplaced to parse alerts in a readable format, correlating breach information to a particular point in time (Viavi, 2020), so long as the technological knowledge and manpower is there, however.
- ❖ Incoming SMTP/Emails
  - Will likely show evidence of phishing if they have not been deleted and even if they have, it could imply further tampering by unauthorised parties. A successful traceback might lead to a

prosecution of the one responsible and/or the blacklisting of the email address.

- Due to the scrutiny of email evidence in court (OUT-LAW GUIDE, 2005), any potential revelation of DOS malware phishing emails would need to demonstrate compliance with electronic implementation standards (BSI, 2014).
- One long-term preventative measure to scan and examine external emails would be to increase staff awareness training of suspicious emails (i.e. typo's, strange requests or source addresses, attachments, etc). Local Banking could also employ threat protection solutions on their firewall and email servers to scan incoming packages. This depends on their budget and willingness to accept third party technology inside the network, however.

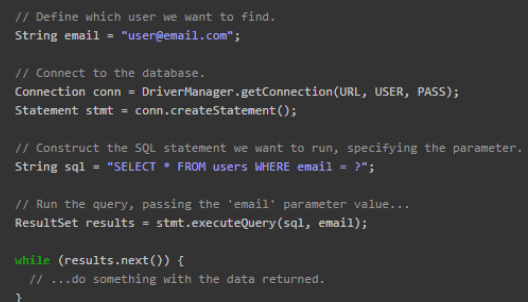
#### ❖ SQL Logs and Database contents

- Could verify that malware is attempting to access employee or bank data using SQL Injection (Prodromou, 2019). If Local Banking has a mobile app or website, database logs, married up to the source logs, may evidence indications of a vulnerability inside the forementioned source software.
- By ensuring all user inputs are sanitised and escaped, Local Banking can minimise the threat to their databases from this avenue (see Figure 6).
- Sanitisation of inputs should be a relatively simple change for developers to make, regarding cost and time concerns (Smith, 2019), but would be relatively useless if the DOS malware is only that.

#### ❖ Credential abuse

- Number of ways an attacker could have gained access to credentials (dumpster diving, social engineering, shoulder

For example, a secure way of running a SQL query in JDBC using a parameterized statement would be:



```
// Define which user we want to find.
String email = "user@email.com";

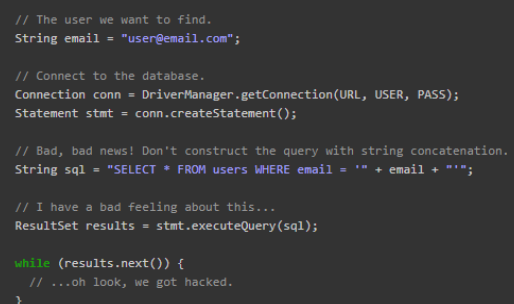
// Connect to the database.
Connection conn = DriverManager.getConnection(URL, USER, PASS);
Statement stmt = conn.createStatement();

// Construct the SQL statement we want to run, specifying the parameter.
String sql = "SELECT * FROM users WHERE email = ?";

// Run the query, passing the 'email' parameter value...
ResultSet results = stmt.executeQuery(sql, email);

while (results.next()) {
    // ...do something with the data returned.
}
```

Contrast this to explicit construction of the SQL string, which is **very, very dangerous**:



```
// The user we want to find.
String email = "user@email.com";

// Connect to the database.
Connection conn = DriverManager.getConnection(URL, USER, PASS);
Statement stmt = conn.createStatement();

// Bad, bad news! Don't construct the query with string concatenation.
String sql = "SELECT * FROM users WHERE email = '" + email + "'";

// I have a bad feeling about this...
ResultSet results = stmt.executeQuery(sql);

while (results.next()) {
    // ...oh look, we got hacked.
}
```

Figure 6: Example of sanitising user inputs inside SQL queries. Local Banking could employ this on any configurable fields and escape malware instantiated SQL queries (Hacksplaining, 2021).

surfing etc). Even if 2FA\* has been implemented, valuable evidence logs will show a successful credential validation and of which one has been used.

- Considering the size of the bank, valuable credentials are likely limited to few, high profile user accounts. This makes it easier to figure out which require revocation of privileges and which require further securing (e.g. changing passwords, enforcement of good password standards (Singer, 2019)).
- Where possible, Local Banking could reduce their reliance on credential authentication. Instead relying upon biometric or token-based (SSO\*) authentication (NCSC, 2018) and account lockout. Albeit an expensive solution and likely infeasible to implement soon (Jeffrey, 2012), reducing reliance would slow down the malware if it were designed to attack credentials.

#### ❖ Honeypots

- Another way to determine if the malware is more than a DOS delivery service, the honeypot will report evidence of data sniffing inside the bank's network. Considering the recommended placement location of honeypots, see (ZELLEKE, 2020), it would be placed at a terminal between the ATM network and the bank's central network as shown in Figure 7's purple arrow.
- Although an excellent data gathering method and a good indicator of an attack, honeypots are probably too costly and complex for an SME to setup at the current time (Evans, 2002). They will be unlikely to assist investigators with the current attack and might be implemented in the wrong locations to best benefit Local Banking.
- Namely, it would have been unlikely an ATM mimic honeypot was deployed by Local Banking, as opposed to a customer database honeypot, without the benefit of foresight and considering limited manpower and budget issues.

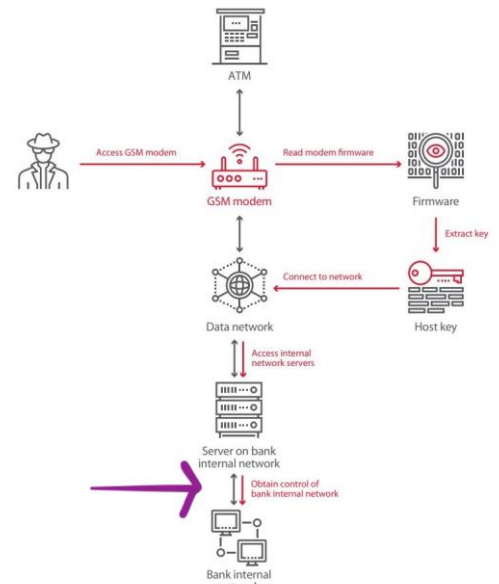


Figure 7: Recommend location on where to place a honeypot if the bank does not already have one (Positive Technologies, 2018)

Following the examination step, the value analysis of the evidence will commence to both parse and prepare it for presentation. The phase will constitute the basis for any investigation into an employee themselves, along with providing a “break” to reorganise and arrange investigation resources into an appropriate format (Sonmez & Varol, 2017). In the case of Local Banking, the investigation will require refactoring of the logs to extract only the relevant information, as well as validating the worth of data obtained from the ATM images. Since the investigation will be looking for incriminating information on the attacker (e.g. IP addresses, steganographic digital fingerprints (Memon, 2005)), searching through TCP network logs via tcpdump would be a good start (specifically searching for excessive SYN or socket requests) (Chirico, 2005). To establish if the breach is more ambitious, high honeypot, non-DOS stream activity on bait databases or credentials would be a good indication that perhaps there is something else hiding in Local Banking’s systems (Edith Cowan University, 2007). In addition to this, matching up email logs with the first network indications of the breach will assist the bank’s limited staff in tracking back the breach to its source. About staff, each member who could have caused the breach (intentionally or not) should have an internal case report recorded against them that marries up incriminating evidence with them (first response, 2020). The primary concern for the lead investigator would be striking the balance between too much and too little refactoring. An extended analysis phase would produce a longer, more expensive and overly complex investigation presentation. Considering the size of the bank and need to competitively serve customers, Local Banking would be unlikely to accept these costs (Hu, 2019). On the flip side, a rushed or rough refactor would mean evidence is still entangled with legitimate information. For Local Banking, one scenario could be that they misidentify the perpetrator (due to the poorly formatted evidence), resulting in discord amongst their limited employee count.

### Evidence Presentation

This phase concerns the consolidation of the analysed evidence into a summary format, subsequently showcasing the results to Local Banking’s board. Not only is the presentation going to be showing the head of Local Banking details of the upcoming investigation, but it will also supply a baseline to future investigators on the history of cyber breaches within the organisation (Grobler & Solms, 2009). Figure 4 depicts the principles the investigation stuck to and the evidence should



reflect that. Meaning, evidence should be presented as close as possible to its original form (when it is not, preservation phase processes would have flagged changes made) and displayed with the knowledge the evidence would be able to stand up in court (Sherman, 2006). Why is this important? Assuming Local Banking wishes to prosecute the antagonist to this attack, they will need clear, undisputable evidence that ties the antagonist to it (otherwise their case may be thrown out) (Irwin, 2019).

Documentation that details the evidence will need to include an element of explanation of DOS, malware and the wider reaching effects of cyber security breaches (e.g. reputation, severity propagability) for an uneducated audience. It will also need to convey mitigation and breach countermeasure recommendations to the board, regarding actions to undertake (forensicsciencesimplified, 2013). For example, presentation documents could imply high counts of SYN flooding originating from a compromised ATM server. The suggested course of action (according to the investigator) could be to increment the half-open backlog and/or utilise SYN cookies to offload handshake handling to the client side (Cloudflare, 2021). This could even be extrapolated to include the internal network, except the clients are now separate router nodes within the bank's network. In addition to this, such documentation could be maintained and expanded upon by the bank over time in the form of security policy training (Dhillon, 2015). In which case, the bank and its future employees can learn from the breach and know how to guard against such a threat in the future. It is said that employee training is crucial to prevent breaches before they occur (Truta, 2020), but this is even more so when evaluating the cost of a data breach vs the financial cost and time of employee training programs (Pendergast, 2015).

## **Conclusion**

Cyber incidents are on the rise, as are the complexity and multipurpose objectives of the attackers that cause them. As such, the likelihood of multipurpose malicious software being present within Local Banking is not a hypothesis to be taken lightly. With such knowledge comes the dreaded reality of higher reputational and countermeasure costs to deal with the advanced threat. However, to not do so further damns Local Banking into a tricky position where little evidence has been gathered (if at all) that would be accepted in court to prosecute the one responsible. In essence, Local Banking will need to make judgement calls on what



measures to implement first (if at all) considering their limited budget. A full-scale cyber investigation will always be expensive, but the true test of whether it will be valuable will depend on where, when and how their resources are applied to combat current and future threats.

## **References & Appendices**

### **References**

ABI, 2021. *Cyber risk insurance*. [Online]

Available at: <https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/>

[Accessed 27 1 2021].

Access Partnership, 2020. [Online]

Available at: <https://www.accesspartnership.com/access-partnerships-guide-to-computer-emergency-response-teams-certs/>

[Accessed 3 2 2021].

Amrin, N., 2015. *The Impact of Cyber Security on SMEs*. [Online]

Available at: [http://essay.utwente.nl/65851/1/Amrin\\_MA\\_EEMCS.pdf](http://essay.utwente.nl/65851/1/Amrin_MA_EEMCS.pdf)

[Accessed 31 1 2021].

Antonopoulos, A. M., 2010. *Honeypots for hacker detection*. [Online]

Available at: [https://www.networkworld.com/article/2213251/honeypots-for-hacker-](https://www.networkworld.com/article/2213251/honeypots-for-hacker-detection.html#:~:text=A%20honeypot%20is%20a%20system,an%20alert%20can%20be%20generated.)

[detection.html#:~:text=A%20honeypot%20is%20a%20system,an%20alert%20can%20be%20generated.](https://www.networkworld.com/article/2213251/honeypots-for-hacker-detection.html#:~:text=A%20honeypot%20is%20a%20system,an%20alert%20can%20be%20generated.)

[Accessed 7 2 2021].

Association of Chief Police Officers, 2021. *Good Practice Guide for Computer-Based Electronic Evidence*. [Online]

Available at: [https://www.7safe.com/docs/default-source/default-document-library/acpo\\_guidelines\\_computer\\_evidence\\_v4\\_web.pdf](https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf)

[Accessed 1 2 2021].

Ayers, R., 2017. *Mobile Device Forensics - Tool Testing*. [Online]

Available at:

[https://www.nist.gov/system/files/documents/2017/05/08/mobiledeviceforensics\\_enfsc\\_2008.pdf](https://www.nist.gov/system/files/documents/2017/05/08/mobiledeviceforensics_enfsc_2008.pdf)

[Accessed 7 2 2021].

Benkhelifa, E., Thomas, B. E., Tawalbeh, L. & Jararweh, Y., 2016.

*Framework for Mobile Devices Analysis*. [Online]

Available at:

<https://www.sciencedirect.com/science/article/pii/S1877050916302794>  
[Accessed 7 2 2021].

BSI, 2014. *BS 10008*. [Online]

Available at: <https://www.bsigroup.com/en-GB/bs-10008-electronic-information-management/>  
[Accessed 4 2 2021].

Carter, E. & Stiffler, R., 2001. *Intrusion Detection: Cisco IDS Overview*. [Online]

Available at: <https://www.ciscopress.com/articles/article.asp?p=24696#:~:text=The%20TCP%20reset%20response%20essentially,Basic%20Cisco%20Secure%20IDS%20Configuration.>  
[Accessed 7 2 2021].

Chirico, M., 2005. *DoS Attacks (SYN Flooding, Socket Exhaustion): tcpdump, iptables, and Rawsocket Tutorial*. [Online]

Available at: [http://souptonuts.sourceforge.net/tcpdump\\_tutorial.html](http://souptonuts.sourceforge.net/tcpdump_tutorial.html)  
[Accessed 5 2 2021].

Cloud Security Alliance, 2013. *ISO 27037*. [Online]

Available at: <https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf>  
[Accessed 1 2 2021].

Cloudflare, 2021. *SYN Flood Attack*. [Online]

Available at: <https://www.cloudflare.com/en-gb/learning/ddos/syn-flood-ddos-attack/>  
[Accessed 5 2 2021].

Cloudflare, 2021. *What is the Internet Control Message Protocol (ICMP)?*. [Online]

Available at: <https://www.cloudflare.com/en-gb/learning/ddos/glossary/internet-control-message-protocol-icmp/>  
[Accessed 7 2 2021].

Cluckey, S., 2013. *DDOS on an ATM network? Impossible. Right?*. [Online]

Available at: <https://www.atmmarketplace.com/articles/ddos-on-an-atm-network-impossible-right/>  
[Accessed 22 1 2021].

Corporate Finance Institute, 2021. *Asset Management*. [Online]

Available at:

<https://corporatefinanceinstitute.com/resources/knowledge/finance/asset-management/>

[Accessed 26 1 2021].

Cott, J. V., n.d. [Online]

Available at: <https://www.lepide.com/how-to/track-file-deletions-and-permission-changes-on-file-servers.html>

[Accessed 25 1 2021].

Day, J., 2020. [Online]

Available at:

<https://www.simplybusiness.co.uk/knowledge/articles/2020/05/what-is-an-sme/>

[Accessed 22 1 2021].

DF Labs, 2019. *The Importance of Evidence Preservation in Incident Response*. [Online]

Available at: <https://www.dflabs.com/resources/blog/the-importance-of-evidence-preservation-in-incident-response/>

[Accessed 31 1 2021].

Dhillon, G., 2015. *WHAT TO DO BEFORE AND AFTER A CYBERSECURITY BREACH?*. [Online]

Available at:

<https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf>

[Accessed 5 2 2021].

Edith Cowan University, 2007. *Proceedings of The 5th Australian Digital Forensics Conference*. [Online]

Available at: <https://storage.googleapis.com/pub-tools-public-publication-data/pdf/33460.pdf>

[Accessed 5 2 2021].

Efe, A. & Akyol, A. D., 2019. *Review of Mobile Malware Forensic*. [Online]

Available at:

[https://www.researchgate.net/publication/336774577\\_Review\\_of\\_Mobile\\_Malware\\_Forensic](https://www.researchgate.net/publication/336774577_Review_of_Mobile_Malware_Forensic)

[Accessed 7 2 2021].

Ellis, D., 2021. *6 Phases in the Incident Response Plan*. [Online]  
Available at: <https://www.securitymetrics.com/blog/6-phases-incident-response-plan>  
[Accessed 26 1 2021].

European Union Agency for Cybersecurity, 2021. *Training material for SMEs*. [Online]  
Available at: <https://www.enisa.europa.eu/publications/archive/training-material-SMEs>  
[Accessed 27 1 2021].

Evans, A., 2002. *Honeypots - Weighing up the Costs and Benefits*. [Online]  
Available at: <https://www.giac.org/paper/gsec/2300/honeypots-weighing-costs-benefits/103964>  
[Accessed 7 2 2021].

Exabeam, 2017. *What is SIEM?*. [Online]  
Available at: <https://www.exabeam.com/siem-guide/what-is-siem/>  
[Accessed 2 2 2021].

first response, 2020. *Cyber Crime & Forensic Fraud Investigations: Case Study 2*. [Online]  
Available at: <https://first-response.co.uk/fraud-forensic-investigations/>  
[Accessed 5 2 2021].

forensicsciencesimplified, 2013. *A Simplified Guide To Digital Evidence*. [Online]  
Available at: <http://www.forensicsciencesimplified.org/digital/how.html>  
[Accessed 5 2 2021].

FortiGuard Labs, 2019. *NTP.Monlist.Command.DoS*. [Online]  
Available at: <https://www.fortiguard.com/encyclopedia/ips/38074>  
[Accessed 7 2 2021].

Ganesan, A. et al., 2019. *Extending Signature-based Intrusion Detection Systems With*. [Online]  
Available at: <https://arxiv.org/pdf/1903.12101.pdf>  
[Accessed 3 2 2021].

Ghafur, S. et al., 2019. *A retrospective impact analysis of the WannaCry cyberattack on the NHS*. [Online]  
Available at: <https://www.nature.com/articles/s41746-019-0161-6>  
[Accessed 3 2 2021].

Ginovsky, J., 2014. *ATM, DDoS attacks increasing*. [Online]  
Available at: <https://m.bankingexchange.com/channels/item/4571-atm-ddos-attacks-increasing>  
[Accessed 22 1 2021].

Gogoi, M. & Mishra, S., 2018. *DETECTING DDoS ATTACK USING Snort*. [Online]  
Available at:  
[https://www.researchgate.net/publication/338660054\\_DETECTING\\_DDoS\\_ATTACK\\_USING\\_Snort](https://www.researchgate.net/publication/338660054_DETECTING_DDoS_ATTACK_USING_Snort)  
[Accessed 25 1 2021].

Grobler, M. & Solms, S. v., 2009. *FUSING BUSINESS, SCIENCE AND LAW: PRESENTING DIGITAL EVIDENCE IN COURT*. [Online]  
Available at: <https://journals.co.za/doi/pdf/10.10520/EJC51043>  
[Accessed 5 2 2021].

Hacksplaining, 2021. *Protecting against SQL injection*. [Online]  
Available at: <https://www.hacksplaining.com/prevention/sql-injection>  
[Accessed 7 2 2021].

Hamilton, R., 2018. *DDoS Attack Glossary: Top 12 Attack Vectors*. [Online]  
Available at: <https://www.cpomagazine.com/cyber-security/ddos-attack-glossary-top-12-attack-vectors/>  
[Accessed 26 1 2021].

Harris, S., 2006. *NIPS and HIPS*. [Online]  
Available at: <https://www.itprotoday.com/security/nips-and-hips>  
[Accessed 7 2 2021].

Hu, E., 2019. *Why small business need DDoS protection more than ever*. [Online]  
Available at: <https://www.mlytics.com/blog/why-small-business-need-ddos-protection-more-than-ever/>  
[Accessed 5 2 2021].

Hunter, N., 2020. *Role-Based Access Control for a Complex Enterprise*. [Online]  
Available at: <https://thycotic.com/company/blog/2020/09/01/role-based-access-control-for-a-complex-enterprise/>  
[Accessed 31 1 2021].

IDRISSI, B. E., 2019. *Long-Term Digital Preservation: A Preliminary Study on Software and Format Obsolescence*. [Online]  
Available at: <https://dl.acm.org/doi/epdf/10.1145/3333165.3333178>  
[Accessed 22 2 2021].

Imperva, 2021. *DDoS Attacks*. [Online]  
Available at: <https://www.imperva.com/learn/ddos/ddos-attacks/>  
[Accessed 32 2 2021].

Internet Society, 2017. *State of IPv6 Deployment 2017: 4.1 Get Started*. [Online]  
Available at: <https://www.internetsociety.org/resources/doc/2017/state-of-ipv6-deployment-2017/>  
[Accessed 72 2 2021].

Intersoft Consulting, 2018. *Art. 13 GDPR - Information to be provided where personal data are collected from the data subject*. [Online]  
Available at: <https://gdpr-info.eu/art-13-gdpr/>  
[Accessed 31 1 2021].

IPRR, 2009. *What is an Investigation Methodology?*. [Online]  
Available at: <http://www.iprr.org/evals/evalsintro.html>  
[Accessed 30 1 2021].

Iqbal, H. & Naaz, S., 2019. *Wireshark as a Tool for Detection of Various LAN Attacks*. [Online]  
Available at:  
[https://www.researchgate.net/publication/335810050\\_Wireshark\\_as\\_a\\_Tool\\_for\\_Detection\\_of\\_Various\\_LAN\\_Attacks](https://www.researchgate.net/publication/335810050_Wireshark_as_a_Tool_for_Detection_of_Various_LAN_Attacks)  
[Accessed 32 2 2021].

Irwin, L., 2019. *Morrisons heads to the Supreme Court over data breach*. [Online]  
Available at: <https://www.itgovernance.co.uk/blog/morrisons-heads-to-the-supreme-court-over-data-breach>  
[Accessed 52 2 2021].

itgovernance, 2018. *GDPR penalties and fines*. [Online]  
Available at: <https://www.itgovernance.co.uk/dpa-and-gdpr-penalties>  
[Accessed 27 1 2021].

James, L., 2015. *Computer Forensics: Preserving Evidence of Cyber Crime*. [Online]  
Available at:



<https://deloitte.wsj.com/riskandcompliance/2015/01/12/computer-forensics-preserving-evidence-of-cyber-crime/>  
[Accessed 30 1 2021].

Jeffrey, C., 2012. *Customized Biometric Solutions for SME's*. [Online]  
Available at: <https://www.m2sys.com/blog/guest-blog-posts/customized-biometric-solutions-for-smes/>  
[Accessed 7 2 2021].

Jones, M., 2020. *Why Cybersecurity Training is Crucial for SMEs*. [Online]  
Available at: <https://fleximize.com/articles/014117/cybersecurity-training-smes>  
[Accessed 31 1 2021].

Kaspersky, 2018. *What is IP spoofing?*. [Online]  
Available at: <https://www.kaspersky.com/resource-center/threats/ip-spoofing>  
[Accessed 7 2 2021].

Kaspersky, 2020. *What's the Difference between a Virus and a Worm?*. [Online]  
Available at: <https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms>  
[Accessed 7 2 2021].

Katsikas, S. K., 2017. *Intrusion Detection Systems*. [Online]  
Available at: <https://docplayer.net/16476894-Intrusion-detection-systems.html>  
[Accessed 3 2 2021].

King, J. & Williams, L., 2014. *Log your CRUD: design principles for software logging mechanisms*. [Online]  
Available at: <https://dl.acm.org/doi/abs/10.1145/2600176.2600183>  
[Accessed 25 1 2021].

Kok, J., 2019. *Banks need to increase ATM security*. [Online]  
Available at: <https://www.fintechnews.org/the-rise-of-atm-attacks/>  
[Accessed 22 1 2021].

Koychev, V., 2015. *Build IPS Virtual Appliance Based on Vmware ESXi, Snort and Debian Linux Step-by-step Tutorial*. [Online]  
Available at: [https://snort-org-site.s3.amazonaws.com/production/document\\_files/files/000/000/069/ori](https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/069/ori)

[ginal/Snort-IPS-Tutorial.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20210206%2Fus-east-1%2Fs3%2Faws4\\_request&X-Amz-Date=20210206T16420](https://ginal/Snort-IPS-Tutorial.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20210206%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20210206T16420)  
[Accessed 6 2 2021].

KPMG, 2018. *BUILDING A CYBER RESILIENT BUSINESS*. [Online]  
Available at:  
<https://assets.kpmg/content/dam/kpmg/uk/pdf/2018/04/building-cyber-resilience-in-asset-management.pdf>  
[Accessed 31 1 2021].

Kumire, J., 2020. *How are banks dealing with a rise in cyber attacks?*. [Online]  
Available at: <https://11fs.com/article/how-are-banks-dealing-with-a-rise-in-cyber-attacks>  
[Accessed 22 1 2021].

Leccisotti, F. Z., 2015. *GUIDELINES FOR IT SECURITY IN SMEs*. [Online]  
Available at: <https://www.combattingcybercrime.org/files/virtual-library/phenomena-challenges-cybercrime/guidelines-for-it-security-in-smes.pdf>  
[Accessed 31 1 2021].

Marshall, A. M., 2015. *ISO/IEC 27042 : Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence*. [Online]  
Available at:  
[https://www.researchgate.net/publication/279206147\\_ISOIEC\\_27042\\_Information\\_technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence](https://www.researchgate.net/publication/279206147_ISOIEC_27042_Information_technology_-_Security_techniques_-_Guidelines_for_the_analysis_and_interpretation_of_digital_evidence)  
[Accessed 3 2 2021].

media, 2016. *What is an audit trail?*. [Online]  
Available at: <https://blog.signaturit.com/en/what-exactly-is-an-audit-trail-and-what-electronic-evidences-does-it-contain#:~:text=An%20audit%20trail%20is%20a,in%20any%20court%20of%20law.>  
[Accessed 1 2 2021].

Memon, N., 2005. *Information Hiding, Digital Watermarking and Steganography*. [Online]

Available at:

[https://eeweb.engineering.nyu.edu/~yao/EE4414/memon\\_F05\\_v2.pdf](https://eeweb.engineering.nyu.edu/~yao/EE4414/memon_F05_v2.pdf)  
[Accessed 5 2 2021].

Mukasey, M. B., Sedgwick, J. L. & Hagy, D. W., 2008. *Test Results for Mobile Device Acquisition Tool*. [Online]

Available at: <https://www.ojp.gov/pdffiles1/nij/224149.pdf>  
[Accessed 7 2 2021].

Murphy, D., 2021. *Track File Deletions and Permission Changes on Windows File Servers*. [Online]

Available at: <https://www.lepide.com/how-to/track-file-deletions-and-permission-changes-on-file-servers.html>  
[Accessed 25 1 2021].

National Crime Agency, 2021. *DDoS attacks are illegal*. [Online]

Available at: <https://www.nationalcrimeagency.gov.uk/?view=article&id=243:ddos-attacks-are-illegal&catid=2>  
[Accessed 2 2 2021].

NCSC, 2018. *Password policy: updating your approach*. [Online]

Available at: <https://www.ncsc.gov.uk/collection/passwords/updating-your-approach>  
[Accessed 7 2 2021].

NCSC, 2018. *Use single sign-on systems*. [Online]

Available at: <https://www.ncsc.gov.uk/collection/passwords/updating-your-approach#tip1-password-collection>  
[Accessed 7 2 2021].

Net Vault, 2020. *Data Backup and Disaster Recovery for Banks*. [Online]

Available at: <https://www.net2vault.com/industry-insights/data-backup-disaster-recovery.asp>  
[Accessed 31 1 2021].

Nominet UK, 2020. *Cyber security for SMEs*. [Online]

Available at: <https://www.theukdomain.uk/get-online/cyber-security-for-smes/>  
[Accessed 31 1 2021].

OneLogin, 2021. *What is Multi-Factor Authentication (MFA) and How Does it Work?*. [Online]

Available at: <https://www.onelogin.com/learn/what-is-mfa>  
[Accessed 6 2 2021].

Osbourne, C., 2021. *UK Research and Innovation suffers ransomware attack*. [Online]

Available at: <https://www.zdnet.com/article/uk-research-and-innovation-suffers-ransomware-attack/>  
[Accessed 2 2 2021].

OUT-LAW GUIDE, 2005. *Email as court evidence*. [Online]

Available at: <https://www.pinsentmasons.com/out-law/guides/email-as-court-evidence#:~:text=E%2Dmail%20is%20a%20form,will%20be%20subject%20to%20scrutiny.>  
[Accessed 4 2 2021].

Paloalto Networks, n.d. [Online]

Available at: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-ddos-attack>  
[Accessed 25 1 2021].

Paloato Networks, n.d. [Online]

Available at: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos>  
[Accessed 25 1 2021].

Paquet, C., 2009. *Network Security Using Cisco IOS IPS*. [Online]

Available at:  
<https://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=3>  
[Accessed 7 2 2021].

Park, C. H., Lee, J. & Kang, C., 2012. *Digital Forensic Investigation of Cloud Storage Services*. [Online]

Available at:  
[https://www.researchgate.net/publication/257687927\\_Digital\\_Forensic\\_Investigation\\_of\\_Cloud\\_Storage\\_Services](https://www.researchgate.net/publication/257687927_Digital_Forensic_Investigation_of_Cloud_Storage_Services)  
[Accessed 1 2 2021].

Pendergast, T., 2015. *Study: Employee Training Reduces the Cost of a Data Breach*. [Online]

Available at: <https://www.mediapro.com/blog/training-reduces-data-breach-cost/>  
[Accessed 5 2 2021].

Positive Technologies, 2018. *ATM logic attacks: scenarios, 2018.*

[Online]

Available at: <https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/>

[Accessed 5 2 2021].

Prodromou, A., 2019. *Using Logs to Investigate – SQL Injection Attack Example.* [Online]

Available at: <https://www.acunetix.com/blog/articles/using-logs-to-investigate-a-web-application-attack/>

[Accessed 4 2 2021].

Rapid7, 2017. *Preparation Phase of Incident Response Life Cycle of NIST SP 800-61.* [Online]

Available at: <https://blog.rapid7.com/2017/02/16/preparation-phase-of-incident-response-life-cycle-of-nist-sp-800-61/>

[Accessed 26 1 2021].

Reith, M., Carr, C. & Gunsch, G., 2002. *An Examination of Digital Forensic Models.* [Online]

Available at:

<https://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf>

[Accessed 25 1 2021].

Rouse, M., 2020. *risk analysis.* [Online]

Available at: <https://searchsecurity.techtarget.com/definition/risk-analysis>

[Accessed 26 1 2021].

Saleem, S., Popov, O. & Bagilli, I., 2014. *Extended abstract digital forensics model with preservation and protection as umbrella principles.*

[Online]

Available at: <https://core.ac.uk/download/pdf/82554968.pdf>

[Accessed 2021 1 25].

Schwartz, M. J., 2017. *ATM Hackers Double Down on Remote Malware Attacks.* [Online]

Available at: <https://www.bankinfosecurity.com/atm-hackers-double-down-on-remote-malware-attacks-a-10338>

[Accessed 22 1 2021].

Scott, T., 2014. 2:55 to 3:03. [Sound Recording]

(<https://youtu.be/BcDZS7iYNsA>).

SecAware, 2015. *ISO/IEC 27041:2015 — Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method*. [Online]

Available at: <https://www.iso27001security.com/html/27041.html>

[Accessed 3 2 2021].

SecAware, 2015. *ISO/IEC 27043:2015 — Information technology — Security techniques — Incident investigation principles and processes*. [Online]

Available at: <https://www.iso27001security.com/html/27043.html>

[Accessed 3 2 2021].

SecAware, 2021. *ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*. [Online]

Available at: <https://www.iso27001security.com/html/27037.html>

[Accessed 2 2 2021].

Secureworks, 2011. *If Hackers Sidestep Your Front Door, Who's Watching Your Back?*. [Online]

Available at: <https://www.secureworks.com/blog/why-hips>

[Accessed 7 2 2021].

Sharifi, A. Z., Zaheer, H., Azizi, M. F. & Faizi, J., 2019. *Detection and Prevention of Distributed Denial of Service attacks in SMEs: The Case of CloudPlus*. [Online]

Available at: <https://ieeexplore.ieee.org/document/8995022>

[Accessed 27 1 2021].

Sherman, S., 2006. *A digital forensic practitioner 's guide to giving evidence in a court of law*. [Online]

Available at: <https://cryptome.org/2014/03/forensic-evidence-in-court.pdf>

[Accessed 5 2 2021].

Shrivastava, G., Kavita, S. & Dwived, A., 2012. *FORENSIC COMPUTING MODELS: TECHNICAL OVERVIEW*. [Online]

Available at:

[https://www.researchgate.net/publication/242524844\\_FORENSIC\\_COMPUTING\\_MODELS\\_TECHNICAL\\_OVERVIEW](https://www.researchgate.net/publication/242524844_FORENSIC_COMPUTING_MODELS_TECHNICAL_OVERVIEW)

[Accessed 25 1 2021].

Silver, L., 2019. *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*. [Online]

Available at:



<https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/>  
[Accessed 7 2 2021].

Singer, D., 2019. *Top Ten 2019 Password Security Standards*. [Online]  
Available at: <https://www.liquidweb.com/kb/top-10-2019-password-security-standards/>  
[Accessed 7 2 2021].

Slattery, T., 2011. *A SELF-INFLICTED DENIAL-OF-SERVICE ATTACK*. [Online]  
Available at: <https://netcraftsmen.com/a-self-inflicted-denial-of-service-attack/>  
[Accessed 31 1 2021].

Smith, K., 2019. *Sanitize Your Inputs?*. [Online]  
Available at: <https://kevinsmith.io/sanitize-your-inputs>  
[Accessed 7 2 2021].

Soni, V., 2018. *Multifunctional malware becoming extensive in 2018, finds Kaspersky Lab report*. [Online]  
Available at: <https://www.dailyhostnews.com/multifunctional-malware-becoming-extensive>  
[Accessed 25 1 2021].

Sonmez, Y. U. & Varol, A., 2017. *Review of evidence analysis and reporting phases in digital forensics process*. [Online]  
Available at:  
[https://www.researchgate.net/publication/320829880\\_Review\\_of\\_evidence\\_analysis\\_and\\_reporting\\_phases\\_in\\_digital\\_forensics\\_process](https://www.researchgate.net/publication/320829880_Review_of_evidence_analysis_and_reporting_phases_in_digital_forensics_process)  
[Accessed 5 2 2021].

Tahiri, S., 2016. *Abstract Digital Forensics Model (ADFM)*. [Online]  
Available at: <https://resources.infosecinstitute.com/topic/digital-forensics-models/>  
[Accessed 25 1 2021].

Tarzey, B., 2012. *Buyer's Guide: Tips for small companies on IPv6 migration*. [Online]  
Available at: <https://www.computerweekly.com/feature/Tips-for-smaller-companies-on-IPv6-migration>  
[Accessed 7 2 2021].

The Hartman Team, 2020. *The 6 Phases of an Incident Response Plan*. [Online]

Available at: <https://hartmanadvisors.com/the-6-phases-of-an-incident-response-plan/#:~:text=The%20identification%20phase%20of%20an,is%20important%20to%20gather%20details.>  
[Accessed 7 2 2021].

Truta, F., 2020. *Employee Training is Key in Preventing Breaches, But is it Enough?*. [Online]

Available at: <https://www.securitymagazine.com/articles/92021-employee-training-is-key-in-preventing-breaches-but-is-it-enough>  
[Accessed 5 2 2021].

UK Domain, 2020. *Cyber security for SMEs*. [Online]

Available at: <https://www.theukdomain.uk/get-online/cyber-security-for-smes/>  
[Accessed 31 1 2021].

UK Government, 2021. *Reducing the Cyber Risk in 10 Critical Areas*. [Online]

Available at:  
[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/395716/10\\_steps\\_ten\\_critical\\_areas.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf)  
[Accessed 27 1 2021].

Veber, J. & Smutny, Z., 2015. *Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic*. [Online]

Available at:  
[https://www.researchgate.net/publication/283226153\\_Standard\\_ISO\\_270372012\\_and\\_Collection\\_of\\_Digital\\_Evidence\\_Experience\\_in\\_the\\_Czech\\_Republic](https://www.researchgate.net/publication/283226153_Standard_ISO_270372012_and_Collection_of_Digital_Evidence_Experience_in_the_Czech_Republic)  
[Accessed 1 2 2021].

Viavi, 2020. *Examining your network traffic with forensic analysis*. [Online]

Available at:  
[https://observersupport.viavisolutions.com/html\\_doc/current/index.html#page/observer/examining\\_your\\_network\\_traffic\\_with\\_forensic\\_analysis.html](https://observersupport.viavisolutions.com/html_doc/current/index.html#page/observer/examining_your_network_traffic_with_forensic_analysis.html)  
[Accessed 3 2 2021].

Watchguard, 2008. *Top 10 Threats to SME Data Security*. [Online]  
Available at: [https://www.watchguard.com/docs/whitepaper/wg\\_top10-summary\\_wp.pdf](https://www.watchguard.com/docs/whitepaper/wg_top10-summary_wp.pdf)  
[Accessed 31 1 2021].

Witts, J., 2021. *The Top 5 Biggest Cyber Security Threats That Small Businesses Face And How To Stop Them*. [Online]  
Available at: <https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/>  
[Accessed 31 1 2021].

Workfront, 2018. *The 5 Ws (and 1 H) that should be asked of every project!*. [Online]  
Available at: <https://www.workfront.com/blog/project-management-101-the-5-ws-and-1-h-that-should-be-asked-of-every-project>  
[Accessed 25 1 2021].

Writers, P., 2016. *Mobile Forensics and Its Challenges*. [Online]  
Available at: <https://hub.packtpub.com/mobile-forensics-and-its-challenges/>  
[Accessed 7 2 2021].

Yusoff, Y., Ismail, R. & Hassan, Z., 2011. [Online]  
Available at:  
[https://d1wqtxts1xzle7.cloudfront.net/49906131/0611csit02.pdf?1477562347=&response-content-disposition=inline%3B+filename%3DCOMMON\\_PHASES\\_OF\\_COMPUTER\\_FORENSICS\\_INVE.pdf&Expires=1611591653&Signature=cOqenkhpidSJXfBmdEsO7WHYW~qgS~nadoQYqE~zsXHbHFOx5oUt51ozh](https://d1wqtxts1xzle7.cloudfront.net/49906131/0611csit02.pdf?1477562347=&response-content-disposition=inline%3B+filename%3DCOMMON_PHASES_OF_COMPUTER_FORENSICS_INVE.pdf&Expires=1611591653&Signature=cOqenkhpidSJXfBmdEsO7WHYW~qgS~nadoQYqE~zsXHbHFOx5oUt51ozh)  
[Accessed 25 1 2021].

ZELLEKE, L., 2020. *How to establish a honeypot on your network*. [Online]  
Available at: [https://www.comparitech.com/net-admin/how-to-establish-a-honeypot-on-your-network/#Placement\\_of\\_the\\_honeypot](https://www.comparitech.com/net-admin/how-to-establish-a-honeypot-on-your-network/#Placement_of_the_honeypot)  
[Accessed 5 2 2021].

## [Appendix 1 – Acronyms/Abbreviations \(in order of appearance\)](#)

- Local Banking Ltd = place holder name for the bank chain in assignment description.
- AFDM - Abstract Digital Forensics Model = (Saleem, et al., 2014)

- DOS = Denial of Service = “A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.” (Paloalto Networks, n.d.).
- SME – Small-medium enterprise = “generally a small or medium-sized enterprise with fewer than 250 employees” (Day, 2020).
- ICMP – Internet control message protocol = “a network layer protocol used by network devices to diagnose network communication issues” (Cloudflare, 2021).
- DDOS - Distributed denial of service = “A Distributed Denial of Service (DDoS) attack is a variant of a DoS attack that employs very large numbers of attacking computers to overwhelm the target with bogus traffic.” (Paloalto Networks, n.d.).
- SSO – Single Sign On = “allows staff to use just one set of credentials to automatically gain access to multiple applications and services” (NCSC, 2018).
- LTDP - Long-Term Digital Preservation = “aims to ensure the accessibility, authenticity, intelligibility, and integrity of digital objects for long periods that may be unlimited.” (Idrissi, 2019).
- CERT – Computer Emergency Response Team = “groups of technical cybersecurity professionals who aid large organizations, such as enterprises, governments, or entire nations in preventing, detecting, responding to and recovering from cybersecurity incidents.” (Access Partnership, 2020).
- 2FA – Two Factor Authentication = “an authentication method that requires the user to provide two or more verification factors to gain access to a resource” (OneLogin, 2021).