Contents

1 Printing over Avian Carriers [25 marks] 1
- 1.1 Impacts on the business . . . 1
- 1.2 Operationalisation . . . 2
- 1.3 Usability . . . 2
- 1.4 Security . . . 3
  - 1.4.1 Benefits . . . 3
  - 1.4.2 Drawbacks . . . 3
- 1.5 Alternate solutions . . . 4
- 1.6 Conclusion . . . 4

2 DREAD Analysis [25 marks] 4
- 2.1 There is one main firewall that monitors and controls all traffic that enters and leaves the network (i.e. it sits between the Class 4s and the Internet.) [8 marks] . . . 5
- 2.2 You have a firewall behind each Class 4 switch that operate independently of each other. [8 marks] . . . 6
- 2.3 You have a firewall integrated into each ZK483 that is administered by a specialist attached to each business unit. [8 marks] . . . 7
- 2.4 Give a brief reasoning as to which scenario out of the three is the best to be in. [1 mark] . . . 7

3 References 8

1 Printing over Avian Carriers [25 marks]

Although using 'printing pigeons' inspired by the 'experimental, not recommended standard' (Waitzman, 1990) IP over Avian Carrier initially appears to offer a secure and quick solution to the recent printer and network compromise, in practice it raises many concerns in terms of operationalisation, usability and security, while also not being a very scalable solution.

1.1 Impacts on the business

Using people ('printing pigeons') to transport data/prints to and from printer corners will have major impacts on business operations. For starters, having to have extra employees will cost more in the long run than just upgrading and securing the network. Print corners will start to become bottlenecks of each floor, and I can imagine that most of them will have

queues assuming that the 'printing pigeon' is also the one that takes the completed prints back to the employee who requested it.

As the company grows, more 'printing pigeons' will be required to ensure that there are as little delays as possible, however the number of printers will not increase, so delays will still be present.

Although 'printing pigeons' will be properly employed employees who have undergone the same checks as everyone else, there is nothing stopping them snooping on the documents being printed, be it straight from the USB or after printing. In the case of sensitive documents, you would assume that the person wanting said documents would directly go to the printer themselves, to lower the risk of someone seeing documents they shouldn't; or worse, pocketing a USB with the documents on.

1.2 Operationalisation

When USBs are not in use (i.e. at the start/end of a workday), they would need to be kept in secure storage so that documents do not get leaked. This would require a new policy to be put in place, and one trusted person to be in charge of unlocking the storage place and handing out the correct USBs. There is also nowhere to say that the files are deleted after printing, so secure storage is a must in-case of sensitive files being printed.

Although networking has been removed from the printers, this does not eliminate the need for maintenance on the printers — infact it can make it more difficult. A lot of issues can usually be fixed remotely, but not if there is no networking to the printer. This would require a technician to always be on the move between floors to fix printers, reducing the amount of work that they can get done. As well as this, not being networked means that there are no print logs automatically tracked, this will have to be done manually. Print logs can be useful if someone has printed something that they shouldn't have, or to check if something actually got printed.

1.3 Usability

As mentioned earlier (Impacts on the business), using 'printing pigeons' will significantly slow down the workflow of all employees, due to the fact the pigeons will be waiting around for prints to finish — this will be especially noticeable when someone requests a very big print job, potentially stopping all other activities in the print corner.

If someone were to need a document ASAP (e.g. for an impromptu meeting), there is no guarantee whether or not they will receive their prints on time, it will all depend on how many other people need printing at that time.

Of course, the pigeons could skip the queue if they explained the situation, however this would not work in a scenario where everyone needs emergency printing.

Using 'printing pigeons' will also heavily impact the bring-your-own-device (BYOD) users. If the printers were still networked, they would simply be able to press print on any device on the WiFi, and it would be printed. However, now that they are not networked, there is not guarantee that they can print at work; say all of the USB drives are USB-A and the BYOD user's device only has USB-C, does the company need to buy loads of adapters, or should the user provide their own?

1.4 Security

Removing networking from the printers will have both many benefits and drawbacks.

1.4.1 Benefits

Fully removing networking from the printers will eliminate the issue of a malicious actor 'getting access' (it is unclear if they actually got access to all of the ports on the printout) to all of the ports they said in the printed memo. Although printing is now trickier, as it required a physical human, it could vastly reduce printing out things that are not needed, as people do not want to wait for their prints.

1.4.2 Drawbacks

The drawbacks vastly outweigh the benefits.

With the BYOD policy, if someone wanted to print something, there is no one vetting what gets put on the USB. Say the user (unknowingly) had malware on their device, this can be transferred to the USB, which would then quickly spread across the company. However, this is not the only way that malware could be spread; what about if the user is a threat actor? They could intentionally put malware on the USB to gain unathorised access - the Melissa virus is an example from 1999 which 'When a user opened an infected document, the virus would execute its code, which included replicating itself by sending infected emails to the first 50 contacts in the victim's Outlook address book' (SentinelOne, 2025)

Once again, a lot of this falls down to protocols and policies. From what I can see, there are not official policies in place. If a 'printing pigeon' lost a USB with sensitive documents on, there is no way to withdraw those documents.

Even simply password protecting documents would be a part solution (there are tools out there to break protected documents' passwords).

As with everything in IT, humans are the weakest link.

1.5 Alternate solutions

There are various alternate solutions that are vastly better than employing extra people and disconnecting the printers from the network.

To re-network the printers and remove the 'printing pigeons', follow-me printing could be implemented. It is a system where prints are only released when the user that requested the prints physically swipes an ID card on the printer. Typically, unclaimed prints are purged anywhere from 1 to 24 hours after being sent.

One way that the threat actor could've accessed all of the ports that they did was via the public-facing webservers. If they are both on the same network as the central server and printers, the ports of the internal devices may not have been locked down correctly. Splitting any public-facing devices onto a separate VLAN would be a way to mitigate this issue. If they need to access anything from the central server, holes could be punched in the firewall to allow that access, but it would be very scope-specific and wouldn't allow full access.

1.6 Conclusion

In conclusion, I would suggest that 'printing pigeons' are not implemented due to all of the concerns above, and that a better system (be it follow-me printing or VLAN isolation) be implemented instead.

2 DREAD Analysis [25 marks]

Damage – **R**eproducibility – **E**xploitability – **A**ffected users – **D**iscoverability

2.1 There is one main firewall that monitors and controls all traffic that enters and leaves the network (i.e. it sits between the Class 4s and the Internet.) [8 marks]

Component	Score /10	Justification
D	9	Once past the main firewall, an attacker can move easily between devices and floors
R	8	A vulnerability on one CF883 can most likely be repeated on all CF883s
E	7	Highly exploitable as it can be accessed from outside the LAN
A	9	Everyone on the network, including the Guest WiFi if it is not on a separate VLAN
D	6	When the CVE becomes public (around 3 months' time), attackers will have more knowledge of this. Can replace all switches until patch is released (∼8 months)

Average DREAD score: **7.8/10**
Overall rating: **HIGH**

With this setup, if an attacker can gain access to the network, then they can easily spread across floors and throughout the whole organisation. While waiting for the patch to release, it might be worth changing out the affected CF883s for something else. This will cost quite a bit, and it really depends on how much the company value their network.

2.2 You have a firewall behind each Class 4 switch that operate independently of each other. [8 marks]

Component	Score /10	Justification
D	7	As each CF883 would have its own firewall, and it is one CF883 per floor, the attacker would only be able to gain access floor-by-floor
R	7	As it is split by floor, the same exploit could be used for each CF883, however multiple firewalls should slow down the attacker
E	7	Trickier to go floor-to-floor as there are multiple firewalls inside the LAN
A	6	Upon the attack commencing, only one floor's worth of users would be affected, however the attacker could move between floors, affecting more users
D	6	As before, when the CVE becomes public (around 3 months' time), attackers will have more knowledge of this

Average DREAD score: **6.6/10**
Overall rating: **MEDIUM**

This solution is better than the previous, as it limits the attack vector to only one floor at a time, however it doesn't stop the fact that if one CF883 gets compromised, the same attack could be used on the others. This is a highly plausible solution for the company, however it will cost a lot more than the previous solution as it has 5x more firewalls needed.

2.3 You have a firewall integrated into each ZK483 that is administered by a specialist attached to each business unit. [8 marks]

Component	Score /10	Justification
D	5	Having a firewall per business unit (assuming departmental level) reduces how much of the business the attacker can gain access to
R	5	The attack can be confined to a single business unit due to each one having a firewall
E	7	This does not remove the problem of the CF883s having an exploit
A	3	Only one business unit will be affected at a time. If the attacker moves through the network, they will be slowed down by the amount of firewalls implemented
D	5	The vulnerability affects only the CF883s, so having multiple ZK483s with firewalls means that attackers reading the CVE won't be as much of a risk as previous solutions

Average DREAD score: **5/10**
Overall rating: **MEDIUM**

Out of all three solutions, this one seems the most feasible and plausible. The guest WiFi is also now isolated from the rest of the network with its own firewall, so it will be trickier for an attacker to use that as an entrance point. However, it will cost even more than solution 2, as compared to having five firewalls, there are now 12; and it is now administered by a specialist, that is another person that needs to be paid per business unit.

2.4 Give a brief reasoning as to which scenario out of the three is the best to be in. [1 mark]

I would recommend going for option 2: each Class 4 has its own firewall. It is a good compromise between security benefits and cost. Unlike option 3, it doesn't need a specialist to maintain it, and unlike option 1, it makes it significantly harder for the attacker to move around the network once inside.

3 References

References

SentinelOne (2025). *What is a Macro Virus? Risks, Prevention, and Detection*. Web Page. https://www.sentinelone.com/. Available at: `https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-a-macro-virus/` [Accessed 02/02/2026].

Waitzman, D. (1990). *IP Datagrams on Avian Carriers*. Web Page. https://www.rfc-editor.org/. Available at: `https://www.rfc-editor.org/rfc/rfc1149.txt` [Accessed 20/01/2026].