Mistakes

1. No RFID protection
2. Untrained staff
3. No CCTV in public areas
4. No security guards present
5. Excessive privileges
6. Weak policy
7. Unprotected Devices[1]

[1] The perpetrator was caught using the device in Nairobi, Kenya, which tells me that he was able to easily gain entry to the machine and there must not have been a strong password in place.

Recommendations

a) Implement CCTV
b) RFID Protective Wallets
c) Untrained Staff
d) Out of hours access
e) Policy Improvements
f) Device security
g) Principle of least privilege

Implement CCTV should be implemented into all public areas around the building. CCTV will provide visual evidence following an attack which can be used as evidence to build a better case. It is highly likely that if CCTV was currently implemented in public areas the perpetrator would have been identified, however monitoring was not in place. This also includes CCTV on the 19th floor which can be controlled by BCTAA, as it is important that they acknowledge what happens out of hours to prevent an attack such as this from happening again. This may be a high cost depending on the amount of area that is covered but the benefit massively outweighs the cost implications.

Recorded CCTV should be stored for later review, however must comply with the general data protection regulations to ensure that data is not being misused. Data should not be held for excessive amounts of time, only for the amount of time required for its purpose and distribution of evidence should be properly verified. Any stored recordings should be locked away to prevent unauthorised access and distribution of data.

RFID Protective Wallets should be provided to all members of staff who own an ID card with any level of access. RFID protective wallets will prevent identity card theft as they block data transmissions to the card until it is removed from the casing. The usage of these cards should be enforced in company policy and should be addressed during staff training. The cost of these wallets is minimal compared to the benefits received. I believe that if these wallets were distributed to staff and in use on the night of the attack, the perpetrator(s) would not have been able to gain access to the 19th floor as they would not have been able to copy card credentials.

I believe that the main reason for the theft of the devices was due to the senior management's identification being stolen during the party. This would have been prevented if their card was stored in an RFID wallet. Security policy should ensure that this procedure is followed and should be taught to staff via training. See recommendation c) untrained staff for more information.

Untrained staff should be provided cyber security training that enforces the company security policy to ensure compliance. Staff should be trained to enforce the company security policy and how to properly mitigate potential tasks. Staff members should also be consistently updated about any changes or known risks. It was made clear given the evidence provided that the company security policy may be overlooked by members of staff. Training should be free of charge to all members of staff and BCTAA should maintain regular checks to ensure compliance and policy refinement.

Out of hours access should not be permitted. There is no reason for anyone to have access to the building during out of hour's times, unless they are a cleaner or member of security. Senior management currently has 24/7 access which is not necessary, this level of access will not be fully utilized and therefore only poses a vulnerability.

Access should be restricted based on date/time. There is no need to have access to the building after work hours and during holiday times which leaves these times and dates vulnerable to attack.

Refer to recommendation g) Principle of least privilege for more detail.

Policy Improvements should be implemented to address issues not accounted for in the current security policy. This may include accounting for all devices, locking the device when not in use (WIN+L) and ensuring that they are not left unattended which will prevent this attack from happening again in the future. Accounting for devices may be a matter of maintaining a shared spreadsheet and rental of devices should be logged on the system to the staff members ID and logged again when returned. Locking unused devices will ensure that the device cannot be accessed without the password, which doesn't prevent physical access but that should already be mitigated with the implementation of a TPM chip. Unattended devices should not be left on show, they should be placed in a physically locked carry case during travel when on person and kept in an equally secure location at other times. This is addressed further later in the document.

Device Security all devices should be physically secured to mitigate issues that arise following theft. This includes full disk encryption, TPM chips, proper configuration and strong passwords. The surface pro 3 comes with a built in TPM chip which should have been properly configured via BitLocker on windows 10 to ensure that the disk was fully encrypted and that physical access to data isn't possible without authorisation. Passwords should be strong and regularly changed, a range of 8-16 characters is standard and should contain a mixture of upper and lower case with symbols.

The **principle of least privilege** should be enforced across all staff identification so that they receive the correct amount of privilege to get their job done, but not too much that it poses a vulnerability and not too little that it impedes workflow. Staff members should not be permitted 24/7 access as this is excessive and poses a vulnerability to the security of the 19th floor out of hours.

Alternative recommendations

1. Enforce incorrect usage of RFID badges that cards should only be on person during work hours or if needed, otherwise it should be stored safely elsewhere. It should be seen as unacceptable to be taking an identification card to a social event as this poses a vulnerability to BCTAAs security.
2. Change ID format following attack. The current ID card number contains too much information and can be easily cracked once format is known as the floor number and

business number is always the same on all cards, which leaves 6 alternative numbers between 0-9 for the staff personal number.

Weaknesses and omissions

This addresses the current cyber security documentation held by BCTAA.

1. Currently staff members must inform their team leader who then informs senior management. This is unreliable and information should not be accounted for in this way. Information should come straight from the witness to prevent loss of information or incorrect details that may have been mistaken or lost during communication which is very likely. I am aware that a written account is also provided but there is still risk that the story may become skewed coming from a messenger.

Improvements to security policy

Theft of data

a) Ensure that all portable storage media is kept secure on personnel at all times and is stored in a locked location.
b) Lock all devices whilst idle and do not leave devices unattended. If you are leaving your desk the device should be locked. If you are leaving the office your device should be taken with you or properly secured and accounted for.
c) Password protection should be enforced across all devices. This includes mobile phones with at least a 6-8bit PIN number and string passwords should be 8-16 characters long minimum with a mixture of upper and lowercase letters with a mixture of symbols. Preferably containing up to three random words.
d) All devices must maintain full disk encryption via bit locker or third party software such as Vera crypt.
e) Staff domain accounts should be setup to prevent access to the local machine. All staff members should be provided a login ID to devices and custom passwords should be issued. Admin account should be hidden and inaccessible on all BCTAA devices.
f) Ensure that sensitive information is handled securely. When working on sensitive documentation, ensure that you are facing away from a wall or other obstruction. This will prevent shoulder surfing. If confidential information is being passed over the phone, ensure that you are in a private space. Confidential data transmissions should only be sent via company VPN.

Theft of IT equipment

g) Register and track all devices, all devices should be registered and accounted for via a company spreadsheet. Tracking should be enabled in order to locate missing devices.
h) Engrave all devices with a serial number, company name or logo. This will ensure that any stolen device can be identified and this will prevent the perpetrator from being able to sell the equipment to the public.
i) Ensure that portable devices or physical storage media containing sensitive information are securely stored in physically locked carry cases to mitigate the chances of pickpocketing and theft.

Infection of company IT systems with malware

a) Scheduled full scans should be made on all devices to mitigate attack vectors, an infected PC could be left unknown and be detrimental to the security of BCTAAs network.

b) Anti-virus software should be installed on all company and personal devices connected to the network and servers must be maintained with frequent security scans.

Unauthorised access to BCTAA systems

a) Domain accounts should be setup and maintained via a domain controller and logins should be logged on the network. Any unauthorised accessed accounts should be disabled.