IT Governance

Cyber Health Check

Sample report

Protect • Comply • Thrive

Cyber Health Check
Prepared for
Evelyn Murphy,
Chief Information Officer,
Baratheon PLC

Table of contents

1. Introduction

1.1 Background

Baratheon PLC (Baratheon) invited IT Governance to perform a high-level Cyber Health Check in order to provide an independent, external assessment of its exposure to cyber risk.

The health check took place at the head offices in London on 13 January and included an online staff questionnaire. This was supported by a remote systems assessment, which took place on 19 January.

This Cyber Health Check is, by nature, high level and depends on information provided by senior personnel; it is not, and should not be treated as, a detailed audit of cyber exposure against a specific cyber control set.

For information on the nature of a cyber threat that could be launched by a motivated intruder, please see Appendix C.

2. Executive summary

Following IT Governance's high-level review of Baratheon's cyber health, we consider that the company has all the building blocks in place for effective cyber security and – most importantly – management commitment to security.

We have made 23 recommendations to improve cyber security. We have grouped our recommendations, below, under three headings: 2.1 Basic cyber hygiene; 2.2 Cyber governance framework, and; 2.3 Policies, procedures and technical controls. Findings from the Cyber Health Check are detailed in Section 5.

2.1 Basic cyber hygiene

Recommendations are:

- Undertake regular independent penetration testing (recommendation 10);
- Enforce encryption policies for removable media (recommendation 21);
- Review event logs on a regular basis (recommendation 22).
- Consider the business need to extend secure email facilities (recommendation 13);
- Consider using an email filtering system with enhanced facilities (recommendation 14);
- Ensure high-privilege user accounts are assigned to unique individuals (i.e. not shared) (recommendation 19);
- Consider implementing a security information and event management (SIEM) system (recommendation 23).

2.2 Cyber governance framework

It is a basic cyber security principle that, without effective board-level cyber governance and risk management, organisations remain vulnerable to cyber attack.

Actions that should be taken are:

- Introduce metrics to provide stakeholders with assurance and visibility that cyber security controls are operating effectively (recommendation 1);
- Improve information security skills (recommendation 6);
- Enhance and evaluate staff training and awareness (recommendations 7, 8 and 9);
- Undertake a Cyber Essentials Plus assessment (recommendation 16).
- Develop an information asset register (recommendation 2);
- Establish a formal risk register and define risk appetite (recommendations 3 and 4).

2.3 Policies, procedures and technical controls

Cyber attackers look for and exploit known vulnerabilities.

Actions should include:

- Clearly communicating location of key policies to staff (recommendation 5);
- Ensure that any third-party patching requirements are adhered to (recommendation 11);
- Review the current web surfing policy (recommendation 12);
- Ensure all visitors are provided with visitor's passes on entry to the building (recommendation 17);

- Establish controls for zero-day malware attacks (recommendation 18);
- Investigate firewall intrusion detection facilities (recommendation 15);
- Introduce a formal bring your own device (BYOD) policy (recommendation 20).

3. Context

3.1. Baratheon PLC

Baratheon PLC (Baratheon) provides market research and analytics solutions to B2C retailers of all sizes. Its proprietary analytics technologies are available to clients as a managed online service or in slimmed-down versions as commercial off-the-shelf (COTS) software. The company also offers a number of street research and consultancy services.

The organisation is global in scope, with offices in London, where it has its headquarters, and further offices in New York, Paris and Melbourne.

There are approximately 400 members of staff at the London head offices, covering functions such as IT, Sales, Marketing, Account Management and Development.

3.2 IT Governance Limited

IT Governance Ltd was identified as a company that has the experience to provide professional service to organisations, and ongoing support and advice in relation to the adoption and implementation of management systems and processes to manage cyber risk and, as such, has been asked to perform the Cyber Health Check described within this report.

4. Methodology

4.1. Approach

The Cyber Health Check consists of a four-phase approach.

Phase 1: Identify cyber risk

- Identify key digital assets, including personally identifiable information (PII).
- Identify the major threats and cyber risks to those assets.
- Identify risk appetite on a scale between cautious and aggressive.
- Identify key legal, regulatory and contractual obligations, such as the GDPR and the PCI DSS.

Phase 2: Audit planned mitigation

- Assess effectiveness and completeness of the controls in place to deal with the identified risks, looking at people, process and technology.
- Review onsite wireless network security implementation.
- Conduct remote vulnerability scans of websites and internet connections.
- Deploy an online staff questionnaire to gauge employee understanding of their role in protecting the organisation.

Phase 3: Analyse cyber risk

- Identify the areas in which controls are weak and fail to meet the risk management and compliance objectives.
- Identify the most appropriate controls or control frameworks that will cost-effectively close the gaps to an acceptable level.

Phase 4: Prioritise improvements

- Develop a prioritised action list with a roadmap of recommendations.
- Identify what must/can be done immediately to address the most critical risks.

5. Findings

5.1. Governance and cyber security framework

5.1.1 Initial overview

Baratheon considers itself to be primarily at risk of cyber attack through the receipt of emails that contain malicious software or purport to be from a legitimate source. Baratheon has suffered from spoof emails encouraging staff to make payments that exceed their authority.

Management has raised additional concerns regarding the potential for a motivated intruder to remove data, and physical security issues. Aside from the motivated intruder, Baratheon considers itself to be subject to opportunist attack rather than from a targeted attack.

As Baratheon devices are frequently connected to client environments, those devices must be free of malware to avoid the risk of infecting client systems, and to avoid damage to Baratheon's reputation.

5.1.2. Cyber risk governance

Cyber risk governance is discussed and managed by the directors at board meetings on a regular basis. Evelyn Murphy (CIO) is responsible for and has ownership of matters related specifically to information security, in coordination with Ivan Kosminski (COO), who has ownership of quality- and security-related matters.

Recommendation 1: We consider the next step in the cyber governance process is to establish metrics to give the board assurance that key elements of cyber security are in place and operating, covering:

a) Basic technology cyber hygiene indicators on:

- the security of boundary firewalls and internet gateways;
- establishment of secure configurations;
- access control arrangements;
- patch management, which includes vulnerability scans of the internal network.

b) Adherence to a staff training and awareness programme, and the results of surveys and audits of staff understanding.

5.2. Cyber management

5.2.1. Asset register

Baratheon is in the process of amalgamating and formalising its existing asset registers into one manageable database, which will become the organisation's asset register.

Information does not form part of the existing asset registers. Baratheon's data is hosted on virtual servers with a document management system shared by all divisions, which is a key asset for the business. Baratheon will need to establish an information inventory and identify owners for that information as a basis for ensuring that any Baratheon data held by third parties is protected by appropriate security. We also note that there is no formal classification scheme in place for information assets.

Recommendation 2: Baratheon should develop an information asset register and review its proposed classification scheme.

5.2.2. Risk register

A number of outstanding actions from security reviews are being tracked by Baratheon, but there is no formal risk register. Baratheon also has no defined risk acceptance criteria.

Recommendation 3: A formal risk register should be established. The risk register serves as a central repository for the organisation's risk information and allows information resulting from the risk management process to be suitably sorted and standardised. Its key function is to provide management, the board and key stakeholders with significant information on the main risks faced by the organisation. The risk register also gives the organisation's risk management stakeholders a clear view of the current status of each risk at any point in time. The risk register should be owned by an executive member of the board.

Recommendation 4: A suitable risk appetite should be defined so that the amount and type of risk that Baratheon is willing to take in order to meet its strategic objectives and support sustainability is recorded, and this can then be used to perform an accurate risk assessment.

5.2.3. Legal, regulatory and contractual requirements

Baratheon demonstrated an in-depth knowledge of its current legal, regulatory and contractual requirements, such as those relating to the Data Protection Act, anti-bribery, freedom of information, computer misuse, licensing regulations, Marketing Research Society requirements, UK employment law and UK health and safety.

There have been no reported breaches of legal, regulatory and contractual requirements in the last 12 – 24 months.

5.2.4. Policies and ISMS

Baratheon has put in place a high-level information security policy, a range of acceptable use policies and an incident response reporting procedure. These have been made available to staff on the company intranet.

The staff survey (see Appendix A) posed questions on the awareness of policies.

89% of respondents are aware that Baratheon has policies but, worryingly, 11% of staff claim to be unaware of policies, and 59% do not know where to find policy information. Of most concern is that 36% of staff claim not to know of the incident reporting procedure, and 49% would not know how to report an information security incident or to whom.

As cyber incidents can be identified in real-time or after the event, speedy awareness of incidents is essential to be able to minimise the impact and to take remedial action.

Recommendation 5: As a matter of urgency, Baratheon should communicate the location of policies to staff and highlight the importance of the incident reporting procedure. Awareness of other policies should be subsequently communicated.

5.2.5. Roles and responsibilities

The CIO is accountable for the security of the IT systems and the data held therein. The IT Manager is responsible for IT support and security. There are no formal cyber security qualifications held by anyone within the organisation.

Our vulnerability assessments have highlighted critical vulnerabilities in the infrastructure, and we have suggested a number of areas where security could potentially be improved – such as data loss prevention (that is, identifying email containing sensitive data leaving the organisation) and implementation of a security information and event management system (SIEM).

Mitigating cyber risk requires personnel who are able to understand cyber attack vectors, assess the threat horizon, and identify and implement appropriate technical and procedural counter measures, and we note that Baratheon does not have staff with professional security qualifications, such as Certified Information Systems Security Professional (CISSP)[1], Certified Information Security Manager (CISM)[2] or Information System Audit and Control Association (ISACA) cyber security qualifications[3].

The acquisition of recognised qualifications by staff responsible for security would provide a stronger governance position, and assurance to the board that the IT function has the capability to identify and, as a result, mitigate the widest set of cyber threats.

Recommendation 6: Baratheon should review cyber security skills and competences, and ensure its IT staff have adequate cyber security skills to help meet current cyber risk challenges.

5.2.6. Staff training and awareness

Baratheon staff receive a brief IT training session run by the IT Manager as part of their induction, which provides limited coverage on information security.

There is no formal process in place for raising information security awareness, and it is likely that Baratheon may not be able to rely on staff capabilities to resist cyber attacks. The board has previously been informed of phishing attacks that are targeted at senior/director-level staff (whaling). Staff are the primary route for the introduction of malware into systems and data loss through poor information handling. Therefore, staff training is a key management control.

The staff survey indicates that all but two individuals would refuse to disclose authentication details to their bank. Given the publicity surrounding criminals attempting to gain access to bank details, it is surprising that two individuals are still susceptible to this social engineering attack. Baratheon staff are clearly very trusting, as 70% would hand over their login details to a senior member of staff over the phone, 34% would not check an email from a customer, 54% do not lock their screen when leaving their desk, over 94% hold doors open for others, and over 54% do not ever challenge strangers in the workplace. This user behaviour indicates that staff are susceptible to social engineering attacks and phishing attacks.

Management acknowledges that staff training could be improved through updating the material and provision of more regular training activity. Industry best practice is to conduct staff refresher training at least annually, and to include tests of comprehension of the training material.

Recommendation 7: Baratheon should establish an annual training programme for staff. Given the spread of locations and the limited resource to conduct training, we

[1] CISSP is offered by (ISC)[2].
[2] CISM is offered by ISACA.
[3] ISACA offers cyber security qualifications at Fundamentals, Practitioner and Specialist levels.

suggest investigating e-learning to ensure that current and consistent messages are delivered to staff. We also recommend that completion of annual staff training is a key metric.

Recommendation 8: In addition to training, a formal information security awareness programme with quarterly updates on key topics should be introduced.

Recommendation 9: Staff training is a key control to minimise the risk of cyber security incidents and, despite comprehension tests, the ability of staff to use that information to work securely is a further aspect to consider. Therefore, we recommend that Baratheon considers conducting social engineering and phishing exercises to determine staff awareness levels and understanding.

5.3. Cyber security controls

5.3.1. Secure configuration

There are baseline builds for laptops and desktops, using a mixture of Windows 7 and 10 operating systems, and some internal applications are built on Vista systems. All servers are Windows 2012.

Microsoft Active Directory is used to manage group policy and passwords. Active Directory is also used to configure servers, routers and firewalls. There is a default security policy for all machines. There are group policies and standard user policies such as for standard users and the Network Team.

File server permissions are controlled by Active Directory according to group.

Network access points are totally locked down.

Active Directory is used as a network and application device inventory, and new devices are added manually.

There are no exceptions in the standard build across the organisation, which includes Microsoft operating systems and the Office package.

iPhones are used throughout the organisation and these synchronise by ActiveSync to Microsoft Exchange.

All Windows machines are patched in line with the Windows patching policy on a monthly basis. Baratheon has a group set up that includes a laptop, desktop and server, which is patched before the latest patches are rolled out across the organisation.

Antivirus updates are rolled out using the central console, which is also used to govern group policy. Antivirus updates are set to update automatically throughout the estate.

The organisation's website is patched at the same frequency and time as other machines on the estate.

Notifications for updates to firmware for the firewalls are sent to the Network Security Team before being tested and applied.

Recommendation 10: Penetration testing should be carried out on an annual basis to assist in preventing cyber attacks.

Recommendation 11: Baratheon should understand any third-party patching requirements and ensure that they are adhered to.

5.3.2. Perimeter controls

There is a multi-layered network defence perimeter in place, which consists of a DMZ for the web servers and network firewalls. A small team of network engineers manage the network. There is some segregation with the web servers in the DMZ and there are test servers but there is no test network.

Automated scanning is set up on wireless access points.

Currently, there are no restrictions on web surfing, but Baratheon is in the process of installing a proxy server with a view to providing this capability.

There is a wide range of web browsers installed in line with the needs of the business, but these cannot be controlled in any way using group policy and, again, restrictions are limited.

Restrictions on the size of email attachments that can be sent are in place: 20 MB externally and 5 MB internally.

Transport Layer Security (TLS) is used as email encryption on some clients' accounts but this is not used across the board.

Baratheon's UK operations are based on a single site near Regent's Park in London, with the company occupying several floors of a serviced office block. Physical access to the building is well handled with an automated reception log in system. All visitors are accompanied into the office areas, but visitors do not receive badges so staff may not recognise whether someone is supposed to be in the office space or not.

Recommendation 12: Web surfing policy should be reviewed and designed to fit both the needs of the business and risks to the organisation's cyber security.

Recommendation 13: Baratheon should review availability of encrypted email facilities; if the risk-reward ratio is appropriate, make the facility more widely available.

Recommendation 14: Baratheon should consider using a fully-fledged mail filtering solution to gain better control of the spam and make use of other features such as data loss prevention (which can identify and trap confidential data being emailed out of the organisation).

Recommendation 15: Investigate intrusion detection systems options on the firewall, which will provide monitoring of malicious activity.

Recommendation 16: Baratheon should undertake a Cyber Essentials assessment.[4]

Recommendation 17: All visitors should be provided with visitor's passes on entry to the building.

5.3.3. Malware

Antivirus software protects the Windows firewalls and also scans the Microsoft Exchange Server. The antivirus is deployed across 100% of the estate. The antivirus is set to auto-update and pushes out the signature updates as and when they are received. Internal and on-access scanning are enabled and carried out automatically.

[4] Cyber Essentials scheme https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

If laptops are not connected to the network, the antivirus is set up to automatically download signature updates when an Internet connection becomes available.

Suspicious email attachments are quarantined or removed by the antivirus and alerts are sent to the user and the IT Team if any suspicious attachments are detected.

The antivirus is not configured to block emails with links.

Blacklists block spam at the firewall before it arrives at the Exchange server.

There are no specific controls in place for zero-day malware attacks.

Recommendation 18: Zero-day malware attacks should be added to the risk register. Once this has been established, a full risk assessment should be carried out to ascertain the risk of this type of malware attack to the organisation.

5.3.4. User access and user privileges

Microsoft Active Directory is used to control user access and privileges.

Access to systems and applications is provided according to a role-based system.

Default passwords for systems and applications ae changed via Active Directory.

Password complexity is set to eight upper- and lower-case characters with one number. Passwords expire after 30 days.

New users are created when a New User form is completed and provided to the IT Team. New users are forced to create a new password on first login. New users are trained by the IT Team on the password policy on induction.

All PCs and laptops are encrypted. Encryption on desktops is synchronised with the Active Directory or network password. Laptops have two passwords: the encryption password and a network password.

A Leaver's form is provided to IT when a user leaves the organisation. The user is either suspended or disabled in Active Directory and this removes access across the estate.

The IT Team has two accounts: a standard network account with low-level privileges, and a privileged account with higher-level administrator privileges the authentication details for which are shared between a handful of team members.

The Wi-Fi is connected to the firewall, hidden logically and filtered by MAC address. Wi-Fi is segregated and has its own port on the firewall so additional rules can be set up.

Recommendation 19: Ensure that all admins use a separate account as named individuals, and extend this approach to all systems where possible.

5.3.5. Mobile devices, mobile working and removable media

Baratheon makes use of a number of mobile devices, which are used by a largely mobile workforce. Various data can be accessed using the devices, including email, documents and photos, and they can backup data to Cloud-based accounts.

There is no formal bring your own device (BYOD) policy. Furthermore, a lack of mobile device management means that technical controls are also not in place to help govern the use of mobile devices.

As yet, there are no physical restrictions preventing access to network devices by removable media. We recommend that builds are hardened using tools such as Security Compliance Manager.

A recent incident involving customer data being left on a desk in an unencrypted USB device was identified. The USB stick was left by an employee who had copied some data and then left it on the desk. Eventually it was picked up and checked, and found to have sensitive information on it. This highlights the need to enforce encryption policies and gain better control over removable devices and information. If the device had been left somewhere public, then the damage could have been significant.

Recommendation 20: Baratheon should formalise the BYOD policy to give staff clear guidance on the issue. Users should acknowledge the policy on a regular basis. We also recommend implementing mobile device management to gain better control over mobile devices.

Recommendation 21: Baratheon should introduce and enforce encryption policies for removable media.

5.3.6. Security monitoring

There is a monitoring strategy in place and improvements are being made as and when possible in line with the needs of the business.

Monitoring is not carried out in real time but alerts are set up to notify the IT Team if any exceptions occur. Monitoring is set up across the estate on servers, workstations, laptops, firewalls, etc.

Improvements could be made to storage of the firewall logs, as currently they are kept on the firewalls themselves and capacity is limited so logs are overwritten. If the logs were offloaded to an internal server, then they could then be archived for access at a later date.

Microsoft Exchange logs are monitored and stored.

Recommendation 22: We recommend Baratheon reviews the available event logs in the infrastructure on an ongoing basis, and ensures that at least three months' logs are available to support incident analysis.

Recommendation 23: Baratheon should consider implementing a security information and event management system (SIEM) that centrally logs key events and security type events from servers, network devices and other consoles. This will allow simple evaluation of risks and identification of breaches.

5.4. Business continuity and incident management

Baratheon has a disaster recovery plan, but no formal business continuity management system in place. Although its disaster recovery plan does not directly link to IT incidents, all incident calls are reported to IT. Cyber incidents will be handled by the IT department in the first instance, and then raised with the CIO and, if appropriate, the Board.

As Baratheon has a small, dedicated IT team and the CIO is very close to operational activity, we are satisfied that incidents will be escalated appropriately. However, as noted in the staff survey, there is a real concern of an incident being reported in a timely manner.

6. Conclusion

Management awareness of cyber risk is high but Baratheon needs to take a number of steps to improve its cyber health.

There are a number of security policies that need to be created and/or reviewed as part of establishing sound information security practices. At the time of audit, this was a work in progress.

Staff training and awareness was also a pressing concern, and we have made recommendations to provide a more robust training and awareness programme for staff.

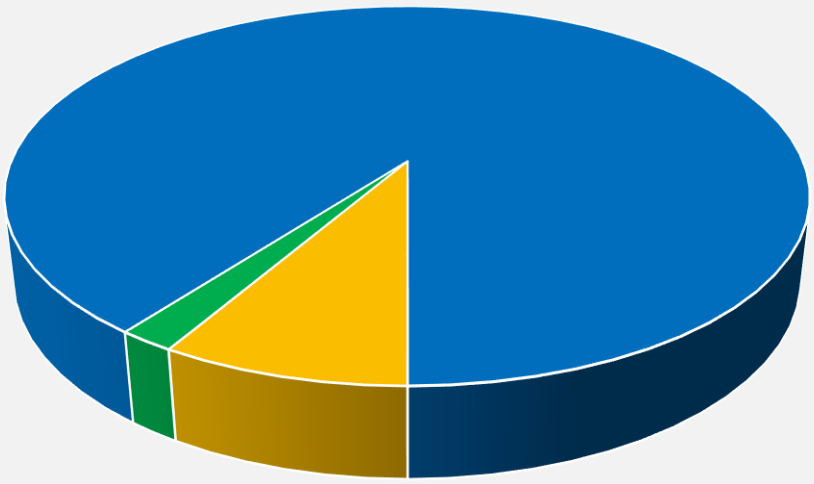
Appendix A: Staff cyber security compliance survey

Out of approximately 400 staff, 100 responded to the invitation to complete an online questionnaire.

Question	Yes	No	Not sure
To your knowledge, does Baratheon have IT policies?	89%	1%	10%
To your knowledge, does Baratheon have network, email and acceptable use policies?	89%	2%	9%
To your knowledge, does Baratheon have an incident reporting procedure?	64%	3%	33%
To your knowledge, does Baratheon have DPA and privacy policies?	34%	2%	64%
To your knowledge, does Baratheon have social media policies?	71%	2%	27%
Do you know how to access company information and policies?	41%	40%	19%
Do you visit social media sites at work?	87%	9%	4%
If you received an email from your bank asking for authentication information, would you supply it?	2%	98%	0%
If the CEO phoned you to ask for your username and password to assist in dealing with a malware intrusion, would you supply it?	70%	23%	7%
If you received a customer email with a link or attachment, would you open it before first checking that it was genuine?	34%	61%	5%
Do you know how to identify if someone is attempting a social media hack?	18%	77%	5%
Do you ever check that the person responding to you on social media sites is who you think they are?	43%	56%	1%
Do you ever fill in quizzes and questionnaires on social media sites?	79%	19%	2%
If you suspected that you had witnessed an information security breach, do you know how to report it and who to?	51%	46%	3%
Do you ever write down your network (or any other) password?	47%	51%	2%
Do you know how to check if your anti-malware software is still running?	44%	52%	4%
Do you use portable devices such as smartphones, USB memory sticks, laptops or tablet computers at work?	98%	1%	1%
Do you use encrypted USB sticks?	11%	87%	2%
When leaving your desk, do you lock your screen?	54%	42%	4%
Do you handle sensitive information on your computer?	67%	32%	1%
Do you work while commuting on public transport?	86%	12%	2%
Would you use a screen protector to prevent others reading your screen?	22%	67%	11%
When entering the workplace do you hold the door open for others?	94%	5%	1%
When you don't recognise someone at work do you ever ask who they are and who they work for?	39%	54%	7%
Do you ever connect your personal mobile device to the company network?	84%	13%	3%
Do you ever use your home computer to access work data?	89%	11%	0%

Appendix B: Vulnerability scan

Infrastructure	
Rating	**#**
Critical	0
High	0
Medium	13
Low	3
Info	111



Summary of vulnerabilities by target						
Target	**Total**	**Critical**	**High**	**Medium**	**Low**	**Info**
xx.xxx.xx.xx	**29**	0	0	3	0	26
xx.xxx.xx.xx	**21**	0	0	3	2	16
xx.xxx.xx.xx	**26**	0	0	0	0	26
xx.xxx.xx.xx	**15**	0	0	3	0	12
xx.xxx.xx.xx	**36**	0	0	4	1	31

(Webserver)			
Ref #	**Severity**	**# of issues**	**Title**
EXT-001	**Medium**	5	SSL RC4 cipher suites supported (Bar Mitzvah)
	Medium	4	SSL versions 2 and 3 protocol detection
	Medium	4	SSLv3 Padding Oracle On Downgraded Legacy Encryption (POODLE) vulnerability
	Low	2	Webserver HTTP header internal IP disclosure
	Low	1	FTP supports cleartext authentication

Appendix C: Anatomy of an advanced persistent threat (APT) attack

1. Initial compromise – spear phishing or social engineering attack to introduce software that compromises an initial system. Required vulnerabilities: poorly trained staff, inadequate incident response systems, inadequately secured workstations and laptops.
2. Establish a foothold – communicate with command and control system from inside out. Required vulnerabilities: inadequate network monitoring, inadequate monitoring of outward bound traffic.
3. Escalation of privileges – increase privileges by compromising existing credentials. Required vulnerabilities: inadequate authentication security, inadequate privilege restrictions.
4. Lateral movement through the network – search out data and information to steal or otherwise compromise. Required vulnerabilities: inadequately patched servers, inadequate data security, inadequate network monitoring.
5. Maintain presence – place malware in multiple locations to prevent effective clean-up. Required vulnerabilities: inadequate internal technical security, inadequate patching, inadequate network monitoring.
6. Exfiltrate valuable data – packaged in .zip or .rar files. Required vulnerabilities: inadequate outward-bound monitoring, inadequate monitoring and investigation of internal data flows.
7. Maintain secrecy – clean up, delete files and anything that identifies presence.

All the vulnerabilities that are typically exploited by APT attackers are present in the organisation's cyber infrastructure, and it is likely that APTs are already live on the network. Earlier malware infestations may have been manifestations of just such an attack.

APT attackers are happy to have some malware identified and removed; this usually lulls their victims into a false sense of security.

