Introduction

I'm Leum* Dunn CISSP, CEH, CNDA, CISMP, MBCS

I'm a Cyber-Security Analyst**

I'm rubbish at creating slide decks

I will probably read off the slides tonight – I know that's against the rules, but I haven't memorised this yet – sorry!

**yes, it really is spelt like that, my dad was a mechanic, it's got something to do with Petroleum!*

***I break [computer] stuff for a living*

The top 100 things I'd do if I ever ~~became an EVIL OVERLORD~~ found myself in charge of Cyber-Security.

Stuff we'll be looking at today

More quality slides than you can shake a stick at!

Well, actually since this is the '100 Things' talk, it's a little over 100 slides… duh!

Best be quick eh?

Inspiration

This top 100 list was originally inspired by this
http://www.eviloverlord.com/lists/overlord.html

1. Asset register.

I can’t manage the kit if I don’t know where it is or what it does.

2. DNS

I can’t manage the kit if I can’t reliably connect to it/communicate with it.

3. Patch all the things.*

I can't rely on the kit if someone else is exploiting it for their own ends.

If 'the business' decides I'm not allowed to patch all the things straight away, I will remember that it's not realistic to ignore the gaps, so I'll introduce compensating controls until 'the business' gives me a window.

**and compensate where I can't.*

4. Antivirus software.

I’ll invest in a product (consider next-gen) and keep it up to date.

5. Training.

I will ensure my staff know how to use the tools I have made available to them.

6. Stop believing that ‘The Perimeter’ is a thing.

It is 2017! Users will tether their phones; make use of Cloud backed storage services and abuse BYOD policies!*

**bless their little cotton socks!*

7. Password management.

Users will be lazy and think that passwords like ‘January2017!’ and ‘February2017!’ are acceptable.

I will stamp out this behaviour and encourage the use of cross platform password management tools like KeePass XC.

Passwords should be strong and complex, but I will not enforce needless frequent changes.

8. Default passwords.

I will not leave default passwords in place.

9. Defence in depth.

Firewalls, antivirus, patching, regular data backups, intrusion detection, intrusion prevention, network access control and honey traps are all part of the modern environment. I will make use of them all (whilst keeping both rule number 5 in mind)!

10. Device naming conventions.

I will chose a standard and stick with it. Modern kit is often virtual, mobile and portable, so I'll avoid using geographic location as part of that standard. Giving assets names that reflect their function makes it easy for threat actors to home in on their targets, but naming servers after my favourite bands won't help my staff. Find a line somewhere in the middle.

11. Toys

I will stop buying whatever security ‘toy’ is in vogue right now. If I’m doing the basics right, then they offer little of additional value. If some big ‘event’ has highlighted the importance of cyber-security to the Company Board, such that all eyes are upon me, and I have some extra budget, I will buy my team cakes and put the rest of the money aside for a rainy day.


EVIL OVERLORD TIPS #12
One of my advisors will be an average five-year-old child. Any flaws in my plan that he is able to spot will be corrected before implementation.

13. Accounts.

I will ensure that user accounts and administration accounts are separate and distinct. I will regularly audit system access privileges and I will disable accounts when staff have left. I will not delete old accounts because it makes auditing historical security events difficult and it creates additional work when ex-staff are re-hired! Admin accounts will not be used for BAU/Back office tasks such as responding to email.

14. 2FA

I will encourage the use and support of two factor authentication.

15. Data register.

I can’t manage the data if I don’t know where it is, what it’s for or who owns it!

16. RAID and backups.

RAID is not the same as backups. I will remember this and insist that the operations team invest in actual, modern backup solutions (something that won't require tapes to be shipped in from an off-site location and then take all day to restore from). I will encourage the Operations team to test their backups regularly.


EVIL OVERLORD TIPS #17
When I employ people as advisors, I will occasionally listen to their advice.

18. Hardening.

I will standardise and harden my OS builds. I will make use of industry standard baselines such as those provided by the Centre for Internet Security. Where relevant, I will also harden applications, productivity tools and web servers.

19. Firmware.

I will ensure that device firmware is not omitted from my patching schedule.

20. VIPs

I will carefully explain to executives and members of The Board that they are the most likely targets for phishing and attack. I will exclude them from any BYOD policy and provide hardened, standardised, monitored equipment from which to work. I will educate them in email hygiene and deny them their requests for admin rights on their BAU user account.

21. Change management.

I will send all my staff on a foundation level training course that introduces the concepts behind change management.

22. Development culture.

Agile or Waterfall? It doesn't matter, it's not a security concern!

What does matter is that whatever methodology is chosen, all teams use the same tools to document their work (for example; tickets = Jira, wiki = Confluence, version control = Git). Regardless of how everyone works, all the information goes in the same place!

23. Encryption.

I will encrypt all the things. GDPR will basically insist on it and Brexit will not make us exempt from that requirement!

EVIL OVERLORD TIPS #24

I will maintain a realistic assessment of my strengths and weaknesses. Even though this takes some of the fun out of the job, at least I will never utter the line "No, this cannot be! I AM INVINCIBLE!!!" (After that, death is usually instantaneous.)

25. Software.

I will encourage the use of a standard set of mature and stable software tools.*

**Open Source software should be under active development and supportable!*

26. Removable media.

I will design and implement a policy for the use of removable media. That policy will address the need for encryption of removable media and describe the process for scanning externally sourced media with sheep dip machines prior to introduction to the network. Users should expect their behaviour to be monitored in this regard.


EVIL OVERLORD TIPS #27
I will never build only one of anything important. All important systems will have redundant control panels and power supplies. For the same reason I will always carry at least two fully loaded weapons at all times.

28. Risk appetite.

I will not eat anything bigger than my head!

29. Documentation.

Documentation will be kept up to date. Any adoption of Agile development methodologies will not be considered an excuse to drop this requirement. Commenting your code does not equate to documenting it*

If we fail audits, we lose customers.

**and if you don't even have a README ready to go, don't bother deploying your code!*

30. Vulnerability scans.

I will encourage my staff to conduct regular vulnerability scans of the estate and report back.

The staff who conduct these scans will not be the same staff who are responsible for patching the estate.

31. Administration.

No one person in my security team will have all the keys to the kingdom. Roles and responsibilities will be clearly defined and staff will be rotated through those roles every quarter.

EVIL OVERLORD TIP #32

I will not fly into a rage and kill a messenger who brings me bad news just to illustrate how evil I really am. Good messengers are hard to come by.

33. Least privilege.

User accounts will be tailored to the role being performed and only access that is required to perform those duties will be provided. Access in this context, doesn't just mean read/write access to directories and files, but to network resources and the internet.

There will be no '*guest*' account.

34. Email hygiene.

I will block macro enabled Office documents along with the usual list of file types (.com .exe etc). I will encourage the use of plain text email and set plain text to be the default option in mail clients.*

**yes, this will upset the marketing and branding departments who spent ages arguing over what font to use in the company email signature!*

35. Wi-Fi access.

I will insist that all wireless connectivity is via VPN and 2FA.

36. Monitoring staff.

I will monitor user activity where appropriate and legal to do so. Particularly in cases where sensitive or classified systems and data are concerned.

I will question activities that appear to be outside of normal, expected bounds (such as unusual working hours).

37. Policy documents.

Users are expected to be familiar with Policy documents, so these documents will be made easily accessible to staff and they will become integral to the culture and company ethic.

Policy documents are a **statement of intent**, they reflect who we are and how we do business. They will not be hidden from clients or otherwise obfuscated for fear of them being '*used against us*' if we fail to match up to our own expectations.

38. Awareness.

I will produce metrics that illustrate our effectiveness at blocking malware, foiling DOS attacks and generally catching baddies. These metrics will be shown to The Board and to staff alike in order to highlight the important work being done by the cyber security team.

Good performance will be rewarded. There may be cake.*

**actual cake, not cake in a 'Portal' sense.*

39. Legacy kit.

Will be expunged with extreme prejudice!

40. Joiners, movers, & leavers

I will ensure that the HR department is fully aware of the IT Security aspects that need to be considered as part of their JML process. User accounts need to be disabled, file shares may need new owners, email mailboxes need to be closed and auto replies configuring if appropriate.*

**Pro-tip – don't let the staffer you just sacked set their own OOO message!*

41. Invest.

I will encourage ‘the business’ to invest in Cyber Security. That is to say I will explain that this includes not only servers, appliances and software, but also training, sharing best practise and corporate culture.

Investment isn’t just about finances.

42. Renew.

Vendor support contracts, product licences, hardware and similar will all need to be reviewed and renewed.

I won’t allow the business to operate on out of date software or equipment because ‘out of date’ is just a short step away from ‘legacy’, but carries the additional risk of not being considered obsolete.

Out of date means unpatched, unmaintained and out of support.

43. Preventative maintenance.

I will schedule regular maintenance of all equipment relating to the cyber-security of the business. I will order consumables along with new hardware purchases (such as server heatsink fans and other small things that often fail and are hard to source later on). Make and model details of key infrastructure devices will be kept in my asset register so that I don't have to visit the server room, just to find out what type of RAM the file server needs (etc).

44. Standardisation.

I will encourage the business to standardise equipment, processes and policies.*

**because...duh!*

Evil Overlord Rules #045

I will make sure I have a clear understanding of who is responsible for what in my organization. For example, if my general screws up I will not draw my weapon, point it at him, say "And here is the price for failure," then suddenly turn and kill some random underling.

46. SMB

I will disable SMB v1 and strongly discourage the use of v2. V3 is acceptable with SMB signing enabled, but even then I will encourage the adoption of sFTP and other platform agnostic file transfer methods with a more secure track record!

47. SSL

I will disable SSL support and move over to TLS 1.2 (or IPSEC) wherever appropriate.

48. File hashing.

I will encourage the use of file hashing to maintain the integrity of data.

I will not use MD5, SHA1 or other compromised hashing algorithms.

49. Respect boundaries

Privacy is a difficult concept to apply in the modern working environment, especially where classified data is concerned.

That said, **I will trust users by default**, respect their personal space and only monitor behaviour and activity where there is a specific business need. After all, ‘the business’ has already vetted and employed our users.

They deserve the benefit of the doubt.

50. Javascript.

I will block Javascript in the browser wherever possible. Where impossible, I will enable ‘click to run’ in web browsers.

Similarly I will block Flash, Shockwave, Real Player, Quicktime and other Web 1.0 plugins.

51. Centralised management.

I will take advantage of the various tools, dashboards, and consoles that I have access to in order to centrally manage and administer to the estate.

52. Trust, but verify.

I understand that ‘the business’ needs to initiate transactions, to communicate, to express, to discuss and to socialise. I know that all these interactions require trust in order to be valuable, but **I will encourage our users to verify information**. To check the veracity of emails and communiqués and to be alert for fraud, phishing and scams. Research new clients, check credentials, ask for references.

53. Stay current.

I will stay abreast of the current developments in technology and monitor Security Journals for details of emerging threats.

I will encourage my team to do the same and I will make time in the day for them to do so.

54. Clear desk policy.

Keep those Post-It Notes off of your monitors! Reminders for appointments, meetings, social events all leak information. I will instruct the cleaning staff to securely destroy any paperwork they find at the end of the night.

Similarly, staff will be reminded not to leave information in plain view from outside the building (passers-by love to nosy in windows and noticeboards are treasure-troves of information)!

55. Pay the cleaning staff a fair wage and learn their names!*

**Wheaton's Law applies!*

56. No names.

Don’t give out (other people’s) names, job titles or responsibilities over the phone or in an email.

Route all calls and unaddressed enquiries through trained, security conscious front line staff.


EVIL OVERLORD TIP #57
BEFORE EMPLOYING ANY CAPTURED ARTEFACTS OR MACHINERY, I WILL CAREFULLY READ THE OWNER'S MANUAL.
imgflip.com

58. Social media policy.

I will be clear and explain what is and is not acceptable behaviour on Social Media. I will explain the risks of data leakage through Social Media. I will use the 'Robin Sage'* case study as an example of how and why this is important. I will include Fitness apps in my definition of Social Media.

* *Make a note, look this up, seriously!*


PROGRAM: SAMARITAN
STATUS: UNKNOWN
COMPETING SYSTEMS : MONITORING ...
OPERATIONAL CONFLICT POTENTIAL
3.47%
PROGRAM: PRISM
ACTIVE, DECOY
Evil Overlord Rules #059
I will never build a sentient computer smarter than I am.
imgflip.com


Evil Overlord Rules #060
My five-year-old child advisor will also be
asked to decipher any code I am thinking of using.
If he breaks the code in under 30 seconds, it
will not be used. Note: this also applies to passwords.
imgflip.com

61. Social engineering.

I will educate staff to understand what this is and how their desire to be helpful in a number of situations might be taken advantage of.

I will not blame staff for making mistakes and falling victim to this tactic, we're all human after all.

62. Automated alerts.

I will encourage my staff to investigate all such alerts and work hard to get the signal/noise ratio right. Investigating alerts will be the responsibility of everyone in the team and conducted according to a rota.

No one system will fall to just one individual to investigate.

63. Segregation.

I will provide multiple methods of allowing people to segregate work and private life. For example, personal email and social media in browser A, company intranet and business web applications in browser B. Use of separate virtual machines if appropriate.

64. Policy enforcement.

Encourage HR* to openly enforce policy. There is no need to name and shame, but policies will be seen as barriers if not enforced and supported by HR.

* *Do not confuse IT teams with the 'Police'. Most of the time, Policy breaches are HR / Line Management issues.*

65. Don’t hide I.T.

I won’t allow the business to hide computers under desks, behind screens or otherwise keep them out of sight. Instead, machines will be kept in plain sight and checked regularly for unauthorised peripheral devices (such as hardware key-loggers, rogue wireless access points, personal phones and tablets that fall outside the scope of any BYOD policy).

66. Device disposal.

Broken, unserviceable, redundant equipment will be disposed of securely, not thrown out with the general waste.

This includes the use of Degaussing machines, secure wipe software tools, and mechanical shredders, **dependant on the sensitivity/classification of any data** previously stored on the device.


Evil Overlord Rules #067
No matter how many shorts we have in the system, my guards will be instructed to treat every surveillance camera malfunction as a full-scale emergency.
imgflip.com

68. Network bridging.

Will not be permitted. I will utilise security tools to block this where users cannot be trusted to follow the rule.

69. Biometrics.

I will only permit the use of biometric access controls as part of a multi-factor solution.

No system will be accessible with just a fingerprint alone.

70. Remote access.

I will not allow machines to have the Wake on Lan setting enabled. I will not permit the use of remote access tools which use short or plain text passwords. Only staff with a genuine business need will be permitted to remotely access their computer. It will not be possible to disconnect another user's live session without their permission.

71. Buy more cake!*

Appreciated and rewarded staff are happy staff. Happy staff are trustworthy staff, and Industrial espionage is a real thing.**

**even when times are hard!*

***the cake doesn't have to be actual cake!*

72. Automate the boring stuff.

I will leave work for my team to do. My staff will not become lazy or complacent. I will watch for signs of ‘unconscious competence’ and remember Rule 31.

73. Smartphones.

I will remember that **most of these rules apply to smart devices too**. They have operating systems that need patching, storage that needs encrypting and user accounts that need protecting. In many cases, they have just as much access to sensitive data as workstations. Obsolete/Outdated phones will not be permitted as BYOD kit and they will be disposed of securely.

Evil Overlord #074

When I create a multimedia presentation of my plan designed so that my five-year-old advisor can easily understand the details, I will not label the disk "Project Overlord" and leave it lying on top of my desk.

75. Geo-location.

Unless required by a specific business workflow, metadata such as geo-location will be stripped from pictures and files for the protection of our staff and the business.

76. Accept the inevitable.

I cannot stop the cyber-attacks. But I can limit their damage and scope.

77. Playbook.

I will be prepared for the inevitable cyber-attack. I will have a playbook that details who needs to be informed, when they need to be informed and by what method.

This playbook is not a ‘plan of reaction’ but a tool to help ensure a swift, panic free initiation of countermeasures and compliance requirements.

78. Data classification.

I will encourage the adoption of a data classification procedure.

This will help me to understand what is important to ‘the business’.

I will expend most effort on protecting the important things.

79. Collaboration.

I will share what I can with Cyber-Security professionals who work for other companies. Together we can monitor threats and share best practise for mitigating risk. I am not an island.

80. Hiring staff.

I will hire people first, skills second. Cyber Security is a vast field and very few people have both the experience and qualifications I desire. I will look for enthusiasm and drive, for a love of the subject and a personality that fits our corporate culture. Then I will give them the opportunity to learn and develop the skills they lack.

81. Hire a lawyer.

I will hire (or at least consult with) a lawyer to navigate the small print, check EULAs, assist with ISO, PCI and GDPR compliance and generally keep us on the straight and narrow.

82. Hire a data scientist.

I will hire (or at least consult with) a data scientist who can analyse the alerts, events, logs and trends for us.

Creating useful metrics from noise is a valuable skill.

83. Assume we've been popped!

I will assume that there is a threat actor on my network already.

My policies, processes and procedures will take this into account.

I will limit this person's ability to traverse the network or gain additional access through the implementation of these rules!

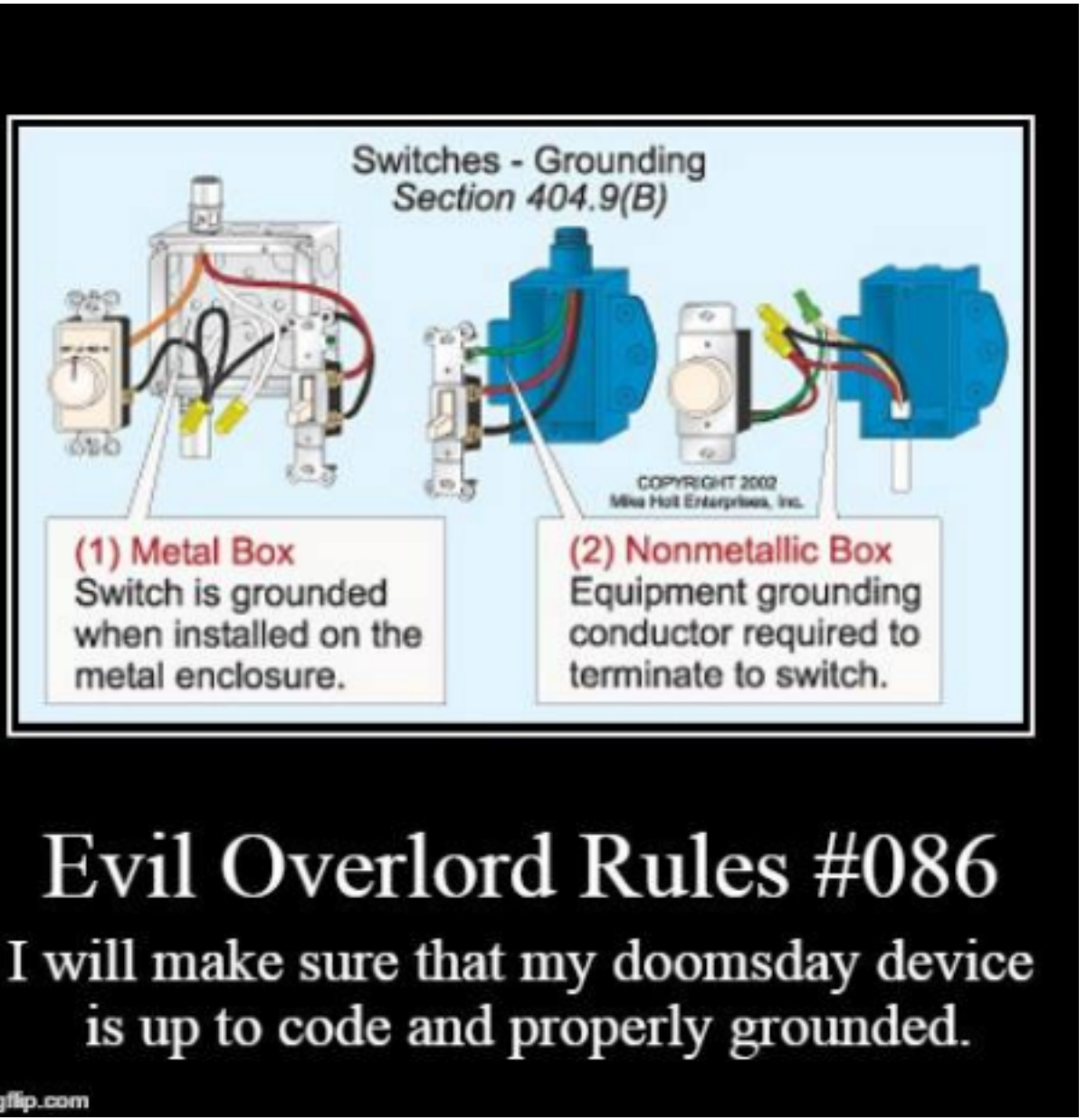
84. Never pay the ransom.

If my company falls victim to a ransomware (or hostageware) attack, I will not pay the ransom.

My rules have prepared me for this possibility, I know how to limit the damage and recover.

85. Webcam covers.

All of our workstations will be installed with a cover for the webcam.


Switches - Grounding
Section 404.9(B)
COPYRIGHT 2002
(1) Metal Box
Switch is grounded when installed on the metal enclosure.
(2) Nonmetallic Box
Equipment grounding conductor required to terminate to switch.
Evil Overlord Rules #086
I will make sure that my doomsday device is up to code and properly grounded.
imgflip.com

87. Need to know.

In furtherance of rules 20, 33 and 78, only people who have a legitimate business need to know ‘the thing’, will be able to access ‘the thing’.

Consider the benefits of both the Bell-LaPadula and Biba models and apply them as appropriate.

88. Certificates.

Self-signed and expired certificates should be avoided.

Use of such erodes faith in a model of trust that is important to the cyber-security of ‘the business’.

89. Browsers.

I will configure add-ons such as ad-blockers and privacy minders centrally. They will be updated and audited.

Users may not install add-ons such as ‘PushBullet’ that can compromise 2FA or bridge other purposeful segregations between work and home.

90. Autolocking.

In furtherance to rule 18, devices will be configured to lock after a period of inactivity. Additionally, portable devices with access to sensitive materials will be configured to autolock if the user is not nearby (for example; via Bluetooth vicinity lock).

I will learn from the mistakes of the Dread Pirate Roberts!

91. Digital assistants.

Bixby, Cortana, Echo, Google Assistant, Siri and others will all be disabled and banned from sensitive areas on our premises. Our BYOD policy will take account of the increasing popularity of these aids and make it clear where their use is inappropriate.

Similarly special provisions may be required for smart watches and fitness bands dependant on the data they collate and their methods of communication with the internet.

92. Bluetooth.

I will discuss the risks associated with Bluetooth (BT) and its ability to create Personal Area Networks (PAN) with ‘the business’.

I will ask for it to be disabled wherever possible due to the likelihood of complicating my Data Loss Prevention efforts.* If using Bluetooth to abide by Rule 90, I will chose the make and model of BT dongle carefully.

**whilst secretly knowing that the Board Members all love their wireless headsets too much to want to do it*

93. Risk Register.

Cyber-Security is not Information-Security, but I will adopt and adapt the practises of the latter where it makes sense to do so. Keeping a Risk Register will help me understand our weaknesses (Rule 24) and prove useful in discussing areas for investment with The Board.

94. Virtualise all the things!*

Security vendors like to sell appliances, but they limit options and introduce single points of failure. Virtual Machines have mobility in the event of hardware failure and are tin agnostic. I acknowledge that this is not always possible (for example; FIPS 140-2 Level 3 compliance which requires hardware tamper protection).

95. Connectivity.

Cyber-Security likes to think in terms of the CIA triangle, but it's also important to be able to break connections, to remove access to data or the network, at either a machine or user level (dependant on the threat). I will have protocols in place for when and how to sever access.

96. Email security.

Email is far from secure in its default configuration and it is difficult to improve things. Rule 34 addresses user behaviour, but adoption of technologies such as DMARC, DKIM and SPF can also help. Additionally it is important to enable the ability for users to digitally sign and encrypt email.

97. Pragmatism.

I will remember that Cyber-Security exists to enable the business. It is a discipline that should always focus on allowing transactions to occur (albeit safely). My team will work to avoid accusations of paranoia.

98. Policing.

The Cyber-Security team is not the ‘internet police’. We do not exist to monitor staff behaviour, personal use of the internet or otherwise provide evidence of staff making poor use of their time.

That’s for relevant line management and HR to deal with!

Evil Overlord Rules #099

Any data file of crucial importance will
be padded to a larger size than can be held
on any current portable data storage medium.


THIS VOUCHER ENTITLES THE BEARER TO 2 FREE INTERNETS.
FREE INTERNET
REDEEMABLE AT ALL PLACES WHERE GOOD INTERNETS ARE SOLD*.
*LOCAL RESTRICTIONS AND REGULATIONS APPLY.
Evil Overlord Rules #100
Finally, to keep my subjects permanently locked in a mindless trance, I will provide each of them with free unlimited Internet access.
imgflip.com

The top 10.

These ten rules enable the others. I think that getting these in place means you've 'got the basics right'.

Rule 45 - Clearly define the roles and responsibilities of your staff.

Rule 2 - Make sure that DNS is working correctly. If you don't have an asset register in place yet, you need DNS to conduct your host discovery efforts!

Rule 1 - Asset register. Thanks to rule 45, you know that you are responsible for cyber-security, so now you need to know what kit is out there.

Rule 3 – You've got a list of kit, now you need to start protecting it. OS, application and firmware patching comes next. Don't forget about mobile and peripheral devices (you'd be surprised how vulnerable multifunction printers can be)!

Rule 18 - Harden and standardise OS builds. If the build is standardised then patching and support is easier. If the build is patched and hardened then the chances of malware affecting the business is dramatically reduced.

Rule 4 - Antivirus. Arguably this is one of the less effective defences when compared to properly patching and hardening a build, but it's a requirement of most client lead audits and it provides a level of reassurance. Consider using traditional signature based AV alongside a more modern 'next-gen' product from a second vendor to cover all bases.

Rule 33 – Adopt and apply the Principle of Least Privilege to user accounts. This is typically done in conjunction with Role Based Access Controls.

Rule 13 – Audit your user accounts to ensure that provisioned access is still required.

Rule 25 – Standardise on a set of mature software tools. This limits risk from unsupported, beta, freemium and ad-supported software and eases the support and patching burden.

Rule 37 – Policy documents. As I suggest in the rules document, I believe that Policy documents should be a statement of intent, reflecting who the company is how they do business. Make sure everyone is familiar with policy and process to really protect against cyber-attacks.