James Chad Ballay

**Make a list of specific authentication threats Alice might face.**

Alice may not practice good password practices.

* Simple passwords.
* Passwords stored in unsecure fashion.
* Passwords not rotated.
* Passwords shared with multiple other users

Alice may blend work and personal activities and therefore increase the threat surface.

* No separate social media accounts for business and therefore open her business to personal phishing attacks
* Personal usage of systems tends to be more casual with regard to security constraints.
* Not physically securing work laptop during transit from work to home.

Alice’s lack of a backup strategy not only is risky for business continuity but without a comprehensive way of securing these backups she exposes a threat service for attackers to have a backdoor installed.

Alice may not compartmentalize her data by having a separate but equally secure password on her spreadsheets beyond the password for system access.

**Make a list of specific authentication risks Alice might face.**

Physical damage to computer hardware and software. - Strong threat. Her laptop isn’t being locked up in her office at all times when it isn’t in use. Stealing this and attacking it at their leisure is a very likely risk.

Physical damage to recovery disks. - Weak threat. An attacker could modify her recovery disks and then damage her laptop to trigger her installing a backdoor. Unlikely but still a chance.

Subversion of computer hardware and software. - Strong threat. She has no periodic and secure offsite backup strategy she opens herself to a huge blast radius if her system is ever compromised.

Disclosure of spreadsheets. - Strong threat. Each of her spreadsheets should require passwords to access that are individually unique and secure. This way if someone compromises her system, her critical data may remain secure. Or if they compromise one of her spreadsheets they don’t compromise all of them.

Identity theft of online business and credentials. - Strong threat. Each of her critical accounts need to have secure passwords and they each in turn need to be unique. Two factor should be enabled where possible.

Identify theft of social media and credentials. - Strong threat. Most social media business accounts tend to use a personalization strategy for customer engagement. Alice very likely blends her personal social media accounts with her business accounts. This increase the surface area for phishing attacks. When people use systems they tend to follow the context that they are in. Security protocols don’t get as rigourously followed in personal settings and places. Etc, etc...

**Authentication Policy**

Alice shall default to creating passwords to being 16 characters or longer. Passphrases or sentences should be used to ease memorization.

Alice shall default to using complex passwords that have at least one character from each of the character classes: Uppercase, lowercase, number.

Alice shall, where able to, set passwords to have expiry periods to enforce password rotation. If systems do not provide a programmatic mechanism, she shall schedule a task to manually perform this action.

Alice shall enable biometric or token authentication where possible.

Alice shall implement an offsite backup strategy with a commercial third-party service.

Alice shall select the backup vendor based not only on cost but also for indemnification for data loss or data breach so as that they protect Alice’s data.

Alice shall store recovery software in a secure location so that attackers cannot modify materials for backdoor installation.

Alice shall purchase a second laptop and separately set it up to perform the same functionality as her primary laptop.

Alice shall document the configuration steps needed to set up the second laptop to provide business continuity.

Alice shall rotate between laptops periodically and leave the secondary laptop powered off in a secure location.

Alice shall segregate her work and personal access so that she no longer uses her work systems for anything but work.

Alice shall not share credentials with anyone else unless business process dictates this.

Alice shall secure her business data into compartmentalized password protected mechanisms. For instance, each of her spreadsheets should have a password enabled and each of these passwords should be unique.

Alice shall power down her laptop when not in use to prevent authentication attempts when she isn’t present to note errors, warnings, or other system metrics that would alert her to these attempts.

Alice shall keep her work laptop physically secure in her office to prevent theft or tampering.