HAZARD LOG/RISK MATRIX VALUES, CONTROL/MITIGATION MEASURES AND EFFECTIVENESS.						
Subject Area Under Consideration: **Compliance with GDPR – Working Draft**			**Location:** Somewhere within the EU		**Date: 25 May 2018** **Author: A N Other**	
(a) **Log Ref:**	**(b)** **Hazard Description**	**(c)** **Likelyhood/ Frequency**	**(d)** **Consequence/ Severity**	**(e)** **Risk (c x d)**	**(f)** **Control/Mitigation Measures Applied**	**(g)** **Comments**
1	**Unauthorised intrusion capturing personal data entered on domain host server from browser whilst ordering online**	**5**	**2**	**10**	**Connections between client web browser and server secured by TLS connection to provide privacy and data integrity. Valid SSL certificate ensures that all information sent to the site is encrypted, secure and private and tamper proof.**	**Likelyhood of intrusion succeeding to capture meaningful data reduce from level 5 to 2.** **Risk now 2 x 2 = 4 Acceptable**
2	**Attacks aimed at stealing card holder data.**	**5**	**5**	**25**	**Card transactions processed by third party payment service provider(s) that maintain PCI Data Security Standard Level 1 compliance. No cardholder data is stored locally. MOTO telephone order card details shredded immediately after order processed. Telephone orders not recorded.**	**Likelyhood of cyber card holder data attack succeeding reduced from Level 5 to 1.** **Risk now 1 x 5 = 5 Acceptable**

HAZARD LOG/RISK MATRIX VALUES, CONTROL/MITIGATION MEASURES AND EFFECTIVENESS.						
Subject Area Under Consideration: **Compliance with GDPR – Working Draft**			**Location:** **Somewhere within the EU**		**Date: 25 May 2018** **Author: A N Other**	
3	**Loss or theft of hardware or data at local level**	**5**	**3**	**15**	**Hardware kept in a secure location. Sensitive data files stored on encrypted storage media protected by strong password. Authorised user access to system strong password protection.**	**Likelyhood of loss or theft of hardware or data at local level reduced from Level 5 to 3.** **Risk now 3 x 3 = 9 Tolerable**
4	**External intrusion and virus threats at local level**	**5**	**3**	**15**	**Maintaining an effective firewall and anti-virus protection on router and network hardware including regular scans and updates to detect and prohibit external threats and unsafe and malicious software download attempts.**	**Likelyhood of external intrusion and virus threat stealing or corrupting data at local level reduced from Level 5 to 3.** **Risk now 3 x 3 = 9 Tolerable**
5	**Abuse of data made available to an IT third party for software development or troubleshooting.**	**5**	**5**	**25**	**Data supplied for such purpose has name, address, phone and email addresses removed locally before submission.**	**Likelyhood of abuse of data made available to an IT third party impacting personal data removed.**

HAZARD LOG/RISK MATRIX VALUES, CONTROL/MITIGATION MEASURES AND EFFECTIVENESS.						
Subject Area Under Consideration: **Compliance with GDPR – Working Draft**			**Location:** **Somewhere within the EU**		**Date: 25 May 2018** **Author: A N Other**	
6	**Loss or theft of hard copy data stored at local level**	**5**	**2**	**10**	**Records of orders received required to comply with HMRC legal and regularity obligations are stored on encrypted storage media for a minimum period of 6 years. Paper records of telephone orders (not card details) and customer correspondence are retained for up to 6 months and then incinerated.**	**Likelyhood of loss or theft of hard copy data stored at local level reduced from Level 5 to 3.** **Risk now 3 x 2 = 6 Tolerable**

Mike Hughes – Sellerdeck Community Forum Thread 57450 Posts #17 through #20 with edits in red text.

I've spent a little time considering the various opportunities for customers data to be accessed and what kind of measures might be appropriate to mitigate them. I'm sure the list isn't complete so please feel free to add, comment, disagree as you like. It would be good if we could come up with a list of risks and measures that covers most of the bases.

1. Early access / Interception. (data open to access coming in / going out of the secure system)

Prevention:

- Encrypt the webpages with SSL.
- Encrypt customer orders while on the Server
- Encrypt the customer emails, uploads, etc - Coming in Sellerdeck 2018

2. Loss or theft of hardware (Computer / Laptop / Backup drives)

Prevention:

- Encrypt the data on the storage media
- Secure access to the computers (strong passwords, HW Keys?)

3. Malicious Access (hackers, viruses, etc)

Prevention:

- Protect the network - HW Firewall on router, secure WiFi, etc
- Protect the computer. Effective Firewall, Anti Virus, etc with regular updates and scans.
- Encrypt sensitive data in the database *** 'someword' (and/or just data that can identify the individual)

4. Unauthorised Access

Prevention:

- Password protect the computer.
- HW keys?

One of the things that I am thinking about is Hardware keys and whether I can arrange it so that an encrypted partition can only be access when a USB key is in the computer. I think Goldkey do one but I suspect the cost might be a bit excessive for this kind of application. Whether it's needed for most SMBs I don't know.

Quote:

> Risk assessment in my experience should be Hazard identification, followed by [L]ikelyhood/frequency of occurrence, [C]onsequence/severity (sensitivity of data), [R]isk [L] x [C] rating then mitigation to reduce risk rating to a level that is acceptable/tolerable, presented in the form of a log (tabular listing). My recollection is that a [R] = [L] x [C] rating of 5 and below was acceptable and between 5 up to and including 10 tolerable with control measures implemented.
>
> I have seen this approach applied many times in industry for H & S assessments using a simple qualitative 5 x 5 matrix with [L] scored down from 5 (highly likely) 1 (extremely unlikely) and [C] scored up from 1 (very low severity) to 5 (catastrophic - extremely severe).

If we can agree a suitable list of hazards then it shouldn't be too hard to come up with a reasonable assessment of the Likelihood of occurrence for various approaches to mitigation.

I'm going to make a first attempt at quantifying the Consequence / Sensitivity of data side of things.

I see the scale of consequence / sensitivity (on a scale of 1 to 5 where 5 is the most serious) as being somewhere along the lines of :

5: Incredibly sensitive data such as medical records, sexual persuasion, bank records, passport details, credit card details, email servers, credit history, etc. This is stuff that you rightly expect to be protected to the highest level and never exposed publicly.

4. Less sensitive data but still private data that can have serious consequences. Things like political leanings, passwords, purchases from adult websites, photo storage servers, etc.

3. Name and address including phone number and email contacts etc. Things some of which you expect to be kept private but that might be available from public records, phone directories, etc and that could become sensitive when obtained by third parties and used for nuisance cold calling and random email marketing purposes.

2. Name and address details excluding phone number and email contact details that aren't that sensitive but readily available from public records i.e. Electoral Role.

1. Randomised / encrypted data with nothing that can be used to identify an individual or reveal any private data about them.

To my way of thinking, most of us as retailers will be at a consequence level of 3. Those of us that sell sensitive items such as adult goods or use passwords to access purchase history, etc might be at a higher level of 4.

If Sellerdeck encrypted the names, addresses, passwords and contact details in the database then the consequence level would probably drop to a 2.

What do you think? Does this work as a starting point for assessing the consequences / sensitivity of a data breach?

>>

Level 1 - State of the Art

Top level protection across the board with state of the art measures to provide physical barriers, network protection, computer protection, data protection, effective procedural measures and counter measure systems to identify and protect data through intrusion detection, honey traps, etc.

In terms of implementation efforts, this is the kind of stuff banks, government agencies, etc should be doing.

Level 2 - Professional Implementation

Similar in scope to the above but may not be using the best, latest and most effective measures. Still professionally implemented by people who know what they're doing.

This is the stuff you'd expect most large companies should be doing to protect data that is maybe

not the most sensitive.

Level 3 - Practical Implementation

Systems implemented to a practical level by people who aren't experts in their fields. Still using a good level of security for data loss mitigation where appropriate. So using decent firewall, good anti-virus software with regular updates, strong passwords for computer / wifi / encryption, hard disc encryption, storage in secure location etc.

This is probably the level we should all be aspiring to.

Level 4 - Practical with some clear weaknesses.

Similar to Level 3 but maybe with some weakness that make the system less secure. Maybe use weak passwords, free anti-virus, only update software occasionally, don't use encryption on the hard disc, maybe carry a laptop around with them containing the data, etc.

Level 5 - Poor.

Any system that doesn't achieve the higher standards.

>>

So where does that leave us?

If we assume that we should be protecting Level 3 Consequence data to at least a Level 3 mitigation level then we end up saying that in general the acceptable Risk level is somewhere around 9 or less (Being the Consequence x Protection Level)

This seems fair enough and I'm sure for each Hazard we can assess the Likelihood of occurrence and therefor work out what level of mitigation is acceptable.

There are a couple of immediate thoughts that come to me from looking at this.

1. Being able to reduce the Consequence risk by encryption of the sensitive data in Sellerdeck would immediately make our task much easier to achieve and much more secure overall. I realise this in itself is really a mitigation factor but it's certainly something I'd like to see (for the sensitive data only much as it has been done for card details in the past. And ideally for selectable fields).

2. If the assumption is correct that storing passwords raises the Consequence level because of their sensitivity (as these are often used by the individual across several sites) then that does suggest there's an impact on the level of mitigation we need to be using. Does anyone know if the user passwords to access order progress, etc are encrypted in the sellerdeck database as that would potentially be of benefit in achieving the desired data protection as well. Alternatively, it might be better to not offer that facility because of the security implications and the extra cost of protecting them to an appropriate level.