Risk Identification Report

Business: Pampers Pets

Summary

Two risk assessments were conducted for Pampers Pets. The first risk assessment looks at the business in its current state. The second risk assessment explores the potential business risk after digitalisation. For the hypothetical transformation, it's assumed the business gains the following technological systems: a business private network and improved website with personalised pages. Risk Assessments include STRIDE risk identification, DREAD threat analysis and a risk mitigation strategy is offered for too.

The chosen models are effective for identifying and presenting risk to stakeholders, whilst being reputable to local government (DSIT, 2016), and academics (Williams & Yuan, 2015); developed by Microsoft. Each identified risk is given a short identifier as a label for convenience, somewhat inspired by Kim et al, 2022, although no data flow diagram is given.

In this report, the DREAD analysis is altered to capture constraints affecting the identified risks, instead of the traditional allocations of scores. The reasoning behind capturing constraints instead of scores, is to make explicit the contextual structure that bounds the risks, operationalise the risk categories on materialistic quantities, and reveal the role of the state of the business on each risk's dynamics. Past efforts have been made on quantifying risks levels for a DREAD threat assessment, such as by Archana Singhal et al (2011) who resort to fuzzy logic, and that of Hussein et al (2011) who try to use formal methods. However, a focus on the constraints that affect individual risks is missing in discourse. The tendency for risk management to introduce errors by subjective inputs such as scores has been criticised heavily by academic such as Hubbard (2019). By using indefinite values in constraints, room is left for further research into how to find definite values.

Pre-digitalisation Risk Assessment

Fig 1. STRIDE Risk Identification for pre-digitalised business

Risk Category	Potential Risk
Spoofing	S31: Customers making fake orders online, S32: Tradesmen offering fake services to the business, S33: Businesses infringing trademark, S34: Evil Twin attack on Wi-Fi hotspot
Tampering	T31: Physical damage to assets, T32: Modification of merchandise such as pet food, T33: Modification of business information such as pricing, T34: Deletion of business information
Repudiation	R31: Anonymity of email addresses, R32: Irrecoverability of business information due to lack of digital backup, R33: Unlogged data actions
Information Disclosure	I31: Unauthorised access to local computers, I32: Unauthorised access to staff phones
Denial of Service	D31: Loss of Supply line, D32: Power outages, D33: Loss of internet service,

	D34: Interruptions to customer facing services, D35: Loss of regulatory approval
Escalation	E31: Misguided trust, E32: Unauthorised Information access, E33: Viral Incidents

Fig 2 DREAD Threat Analysis for pre-digitalised business

Threat	Damage	Reproducibility	Exploitability	Affected Users	Discoverability
S31	AC	AC	AC - &RS	0	c
S32	SC	SC	SC - &SD	0	s
S33	EP	EP	EP - &BD	g	l
S34	NV + IV	NV + IV	NV + IV - WD	c + s	h
T31	AV	AV	AV - &PF	0	p
T32	CV + LP	CV	CV - &CD	c	p
T33	AV	AV	AV - &ID	s	i
T34	AV	AV	AV - &ID	s	i
R31	AC + SC	AC + SC	AC + SC - &SD	0	c + s
R32	AV	AV	AV - &ID	s	i
R33	TV	TV	TV - &TD	0	h
I31	TV	TV	TV - &TD	s	h
I32	NV + IV	NV + IV	NV + IV - PD	c + s	h
D31	FP	FP	SC - &SD	0	ss
D32	OV	OV	SC - SD	0	t
D33	NV	NV	SC - SD	r	h
D34	OV	OV	PV - RS	c	c
D35	OV	OV	OV	0	k
E31	SC	SC	SC - &SD	0	s
E32	IV	IV	IV - TD	s	t
E33	AV	AV	AV - &VD	g	c

Key:

& := the quantity can accumulate as its discovered

AC := the maximum amount of money that the business would spend in response to a larger order than available in stock, anticipating a legit transaction.

AV := the value of all assets

BD := the minimum amount of money it costs to deceive customers into accepting the legitimacy of a duplicate business

c := the number of customers

CD := the minimum amount of money it costs to modify some merchandise

CV := the value of current stock

EP := the maximum profit the business can make if it had expanded as much as possible

FP := the maximum profit the business can make once all stock is sold

g := the global population

h := the number of customers who are hackers

I := the amount of business information items

ID := the minimum amount of money it costs to modify some business information

IV := the value of the business information

K := the number of relevant regulatory bodies

l := the number of locations to do business within

LP := the maximum amount of profit the business can make with the current stock

OV := the value of the whole business including projections

NV := the maximum value of networked technology to the business.

P := the number of products

P := the amount it costs for staff

PD := the minimum amount of money it costs to gain access to staff phone

PF := the fee for damaging property

r := the number of customers who use remote services

RS := the maximum amount available to a customer for refunds

s := the number of services

ss := the number of supply services

SC := the maximum amount of money that the business would spend on a service in response to unexpected additional service costs .

SD := the minimum amount of money it costs to deceive the business owner into accepting changes in service.

T := the number of assets dependent upon electricity

TD := the minimum amount of money it costs to access the computers

TV := the value of the business information stored on the computers

VD: the minimum amount of money it costs to go viral

WD := the minimum amount of money it costs to perform an evil twin attack

Fig 3. Risk Mitigation Strategies for pre-digitalised business

Risk	Strategies
S31	Increase opportunities to move excess stock, such as bulk sales, Make risky orders require loyalty-based privilege, Make risky orders require identification
S32	Enforce stricter requirements before partnerships
S33	Open channels to hear customer suspicions, Take legal action on trademark breaches, Increase business reach to most profitable platforms and locations, Maintain positive business image
S34	Require connection to a business VPN to monitor data access
T31	Join an insurance scheme for cover of property damage
T32	Join an insurance scheme for cover of property damage
T33	Enforce strict access control on attack surface, Keep log system of actions and events on attack surface, Keep a data backup for data recovery in case of attack
T34	Enforce strict access control on attack surface, Keep log system of actions and events on attack surface, Keep a data backup for data recovery in case of attack
R31	Establish identification for communication that requires business action
R32	Keep a data backup for data recovery in case of attack
R33	Keep log system of actions and events on attack surface
I31	Enforce strict access control on computers, Enforce role-based privilege for data actions, Keep log system of actions and events on computer
I32	Enforce role-based privilege for data actions,
D31	Maintain relationships with alternative suppliers
D32	Maintain backup generators,

	Maintain relationships with technicians
D33	Maintain backup internet service
D34	Hire security guards
D35	Subscribe to regulatory services for regulation updates
E31	Enforce role-based privilege for data actions,
E32	Encrypt databases
E33	Keep log system of actions and events in business, Maintain positive business image

Risk Summary for pre-digitalised business

Figure 2 shows some of the largest damaging threats found to the pre digitalised business include S33, T31, T33, T34, R32, D31, D33, D34, D35 and E33. The development on an online presence can help mitigate S33 and E33. T33, T34 and R32 can be mitigated by a data backup system, such as a cloud backup system. T31, T32, D31, D32, D34 and D35 can be mitigated by increasing the business partner network.

During the DREAD analysis, the reproducibility of threats has been related to the potential damage of the threat, not the difficulty of it, as it's assumed there exists people in existence who are capable at exploiting all risks if the reward is large enough. Penetration testing could yield insight into the skill required to exploit a threat too, to factor in if wanted, but without damage, the threat is not reproducible.

Similarly, penetration testing would provide more exploitability insights to establish attacker costs and determine if a threat is worth exploiting. The outlier to this requirement is D35 which does not cost the 'perpetrator', so is always a threat.

Figure 2 also shows that threats that have large discovery include S31, T31, T32, T33, T34 R31, R32 and E33. Of those, S31 and R31 can be mitigated by stricter identification protocols, T33 and T34 can be mitigated by decreasing the attack surface and increasing the costs to perform the attacks.

S33 and E33 can potentially affect the most users, as they can affect potential users too.

Post-digitalisation Risk Assessment

Fig 4. STRIDE Risk Identification for post-digitalised business

Risk Category	Potential Risk
Spoofing	S31, S32, S33, S34, S41: Spoofing specific users
Tampering	T31, T32, T33, T34, T41: Altering specific user information
Repudiation	R31, R32, R33,
Information Disclosure	I31, I32, I41: Unauthorised access to user information
Denial of Service	D31, D32, D33, D34, D35 D41: DDoS on private network
Escalation	E31, E32, E33

Fig 5. DREAD Threat Analysis for post-digitalised business

Threat	Damage	Reproducibility	Exploitability	Affected Users	Discoverability
S41	UV	UV	UV - UD	1	c
T41	UV	UV	UV - UD	1	c
I41	UV	UV	UV - UD	1	c
D41	NV	NV	NV - DD	c + s	n

Key:

UD := The minimum cost to spoof a user

n := the then number of network servers

UV := The value of an individual user

Fig 6. Risk Mitigation Strategies for post-digitalised business

Risk	Strategies
S41	Enforce two factor authentication
T41	Enforce strict access control
I41	Provide capability to keep personal data private
D41	Load balancing capabilities

Risk Summary for post-digitalised business

The risks of the post-digitalised business are almost identical categorically to the pre-digitalised business, as the business model doesn't change drastically. What does change is the values described in the DREAD analysis. How these values grow with digitalisation determines whether digitalisation is risky or not. An asymptotic analysis could be conducted, but it's fairly safe to assume value scale linearly with the number of assets that the business has, as it's the number of assets that ultimately dictates the maximum amount of damage that can be done. There are two exceptional conditions to this assumption:

1) Theres a potential risk to customers separate to business costs, and that increases with digitisation as customers are obliged to share more information to the business.
2) As a business becomes distributed, risks become more localised.

For these reasons, it's essential to meet customer-centred regulations. Risk mitigation funds should also be strategically distributed, to maximise efficiency and resilience of the business.

Should the business digitalise further?

The conclusion of this risk assessment is that digitalisation will not increase risk to the business, it's business growth that can increase risk. While the business attack surface increases with digitalisation, a distributed architecture builds resilience into the business against threats that

already exist, including those that worsen with business growth. As long as customer-centred regulations are followed, i.e. that the business is responsible, then the conclusion is that the business should digitalise.

References

Archana Singhal, S. & Banati, H. (2011) Fuzzy Logic Approach for Threat Prioritization in Agile Security Framework using DREAD Model. IJCSI International Journal of Computer Science 8(4): 182-190. DOI: https://doi.org/10.48550/arXiv.1312.6836

Department for Science, Innovation, & Technology. (2016) Conducting a STRIDE-based threat analysis. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1155778/Conducting_a_STRIDE-based_threat_analysis.pdf

Hubbard, D. (2019) *The Failure of Risk Management: Why It's Broken and How to Fix it*. 2nd Ed. Wiley

Hussain, S., Erwin, H. & Dunne, P. (2011) 'Threat modelling using formal methods: A new approach to develop secure web applications. 2011 7th International Conference on Emerging Technologies. Islamabad, Pakistan, 2011. IEEE. DOI: https://doi.org/10.1109/ICET.2011.6048492

Kim, K., Kim, K. & Kim, H. (2022) STRIDE-based threat modelling and DREAD evaluation for the distributed control system in the oil refinery. ETRI Journal. 44(6): 991-1003. DOI: https://doi.org/10.4218/etrij.2021-0181

Williams, I. & Yuan, X. (2015) 'Evaluating the effectiveness of Microsoft threat modelling tool'. *Infosec '15: Proceedings of the 2015 Information Security Curriculum Development Conference*. Kennesaw Georgia, 2015. New York: Association for Computing Machinery. 1-6. DOI: https://doi.org/10.1145/2885990.2885999