Business Risk

A taxonomy-based model of security-driven business risks

Area of corporate strength or wellbeing	Business harms The possible types of consequence and/or cost of a serious but realistic business risk materialising	Key business risks Adverse outcomes that could arise (as seen from a business perspective) that could cause serious business harm and that could have a security risk as a root cause or enabler	Key operational risks One-off or repeated operational breaches, compromises, disruptions or failures (whether by omission or commission) that could lead to the associated business risk and could have a security risk as a root cause or enabler	Key security risks One-off or repeated security risks (particular threats leading to particular security breaches) that could cause or enable the associated operational risk to materialise
Regulatory - Financial services industry	A combination of: * Penalties and/or fines * Public warnings and censure * Restrictions or conditions imposed on services offered within a territory * Potential removal of banking licence	A serious or material breach of rules that triggers a regulatory investigation	Loss of regulated service (e.g. payments)	A repeated security breach of any kind that has a significant affect on service availability
		A serious or material breach of rules that requires notification to a regulator	Loss of regulated service; Significant outage of a non-regulated but critical system	DDoS that has a significant and extended affect on service availability; Unintentional systems intrusion by a member of (own or service provider) staff that results in system unavailability; Systems intrusion by an external agent that results in system unavailability; Malicious damage to critical assets
			Data breach	Staff error in response to a phishing attack; Malware-enabled data theft Systems intrusion by organised crime resulting in data theft Unauthorised access to restricted data by a rogue (own or service provider) employee using their own or another logical account; Data theft by hackers
Regulatory - Civil and Markets	A combination of: * Penalties and/or fines * Public warnings and censure * Court proceedings against Directors or Executives deemed to have been negligent * Legal fees * Court-imposed damages	Serious financial reporting misstatement with a very large bottom line impact	Accidental or negligent errors in reporting data	Undetected errors in manually entering reporting data (e.g. into reporting spreadsheets)
			Deliberate falsification of reporting data (e.g. to conceal a true situation as part of a cover-up by a rogue trader who had run up huge losses);	Deliberate deletion / modification of reporting data by a rogue member of staff; Staff tampering with a key reporting system
		Improper release of sensitive information (e.g. price-sensitive information, staff personal or financial data; client personal or financial data in a non-transparent banking jurisdiction;)	Accidental or careless release of sensitive information to an external party;	Staff error in response to a phishing attack
			Deliberate passing of sensitive information to an external party;	Unauthorised access to, and disclosure of, restricted data by a rogue (own or service provider) employee using their own or another logical account
			Loss of (portable media holding) sensitive data	Accidental loss of portable data storage media (e.g., laptop, USB drive; CD)
		Failure to keep and retain adequate records	Procedural failure meaning required records are not retained	Q - are there any significant security threats that could give rise to this?
			Accidental or careless deletion of records (prior to their retention or from the retention archive)	Accidental or careless deletion of data by a member of (own or service provider) staff;
			Deliberate deletion or falsification of records (prior to their retention or from the retention archive)	Deliberate deletion / modification of record data by a rogue member of (own or service provider) staff; Tampering with retention and archival systems by a rogue member of (own or service provider) staff;
		Failure to comply with listing obligations	Failing to report on a material breach in the annual report	Accidental or careless deletion of data by a member of (own or service provider) staff;

		[illegible]	Q - What other operational breaches might give rise to a listing compliance failure?	Q - What (if any) security breaches might give rise to any of these?
		Improper, unethical or illegal business practices. For example: * Insider trading * Market abuse or manipulation * Trading against customers' interests	Breach of Chinese Walls or other segregation controls	Unauthorised access to sensitive / segregated business data by a member of (own or service provider) staff; Unauthorised access to segregated user accounts by a member of (own or service provider) staff
			Falsification of records (to conceal improper practices)	Deliberate deletion / modification of management data (e.g. monitoring and reporting data) by a rogue member of staff; Deliberate tampering with management systems (e.g. monitoring and reporting systems) by a rogue member of staff
Financial	A combination of: * Direct loss of funds * Penalties and/or fines * Restrictions on future offerings imposed by a regulator * Costs of investigation and remediation * Loss of customer confidence and future business	One-off or persistent theft or fraud by organised crime that had high aggregate value	Organised crime breaking into company payment systems	System intrusion by organised crime resulting in: * improper disclosure of client data; * improper use of an internal company system; * improper insertion / modification of payment transactions; * improper modification of management systems and/or management records (e.g. reporting records);
			Collusion between organised crime and a member of staff	Improper use by a rogue employee of their own or another logical account
			Organised crime breaking into the company's links to external payment networks	Infrastructure system intrusion by organised crime resulting in: * improper insertion / modification of payment transactions; * improper modification of management records (e.g. reporting records);
		A rogue trader running up huge losses over an extended period of time	Trading in excess of authority / limits	Unauthorised deletion / modification of business data (e.g. limits, records of trades);
			Breach of segregation controls	Unauthorised use of another person's logical account (in violation of segregation rules)
			Disguising actions by falsifying records	Unauthorised deletion / modification of business data (e.g. limits, records of trades); Unauthorised modification of management systems (e.g. monitoring and reporting systems)
		Large scale or persistent fraud by a member of staff against a high-value (retail or corporate) client	Tampering with, or creating false, client instructions	Unauthorised use of another person's logical account (the client's); Unauthorised modification of business data (e.g. falsifying client instructions);
			Tampering with, or creating false, transactions	Unauthorised modification of business data (e.g. transactions); Unauthorised use of a colleague's user account (to conceal the true source of the false transactions)
			Circumventing segregation controls on payment release	Unauthorised use of another person's logical account (in violation of segregation rules)
			Disguising actions by falsifying records	Unauthorised deletion / modification of business data (e.g. records of instructions and transactions); Unauthorised modification of management systems (e.g. monitoring and reporting systems)
		One-off or persistent embezzlement, theft or fraud of [illegible]	Tampering with, or creating false, invoices	Unauthorised modification of business data (e.g. creating false invoices)
			Tampering with, or creating false, transactions	Unauthorised modification of business data (e.g. transactions); Unauthorised use of a colleague's user account (to conceal the true source of the false transactions)

		bank money by a member of staff, amounting to a huge sum	Circumventing segregation controls on payment release	Unauthorised use of another person's logical account (in violation of segregation rules)
			Disguising actions by falsifying records	Unauthorised deletion / modification of business data (e.g. records of invoices and transactions); Unauthorised modification of management systems (e.g. monitoring and reporting systems)
Cultural	A combination of: * Reduced market share; * Reduced revenues; * Increased cost of operation * Reduced equity value	Failure to innovate	Inability to retain top quality staff (due to the existence of a weak controls culture)	A wide range of simple security breaches that occur repeatedly because the company has chronically poor controls, poor staff security education and training, and a weak security culture
		Low staff performance	Reduced staff trust and co-operation	Improper disclosure of sensitive data (e.g. staff personal data); Improper use of a personal logical account (e.g. prying into a colleagues personal data)
Reputational - Corporate	A combination of: * Reduced market share; * Reduced revenues; * Reduced equity value	Loss of trust in the company by stakeholders	Leaking of highly sensitive information (e.g. that a national agency had launched an investigation into suspected illegal / corrupt company practices);	Intentional disclosure of highly sensitive information by a disgruntled employee
		Reputation undermined by prominent and sustained negative publicity	Chronic / repeated operational failures such as those in the business risk below that have a significant affect on retail customers	Extensive intrusion into company systems; Repeated unauthorised access, copying and exfiltration of sensitive data;
		Reputation tarnished by negative publicity of limited duration. (Social media has increased the ease with which anyone can create negative publicity. There is nothing to suggest that people pay less attention to bad publicity as a result.)	Any loss of customer facing services	See examples under Operational - Service Availability above
			Data breach	See 'Data Breach' security risks higher up
			Poor responses to internal process failures	Chronic accidental or careless modification of customer data by staff
Reputational - Brand	A combination of: * Having to close down a line of business in a country or region * Having to settle damages in a class-action suit	Brand reputation undermined by providing what is perceived to be an unethical or corrupt service	A number (more than just one) of rogue individuals trading against clients' interests, committing market abuse, etc.	See Security Risks under 'Improper, unethical or illegal business practices' above
			An unauthorised disclosure that showed that unethical or corrupt behaviour had been going on for some time (with senior management knowledge);	Intentional disclosure of highly sensitive information by a disgruntled employee
		Brand reputation undermined by providing what is perceived to be a poor or uncompetitive service	Chronic internal process failures	Chronic accidental or careless modification of customer data by company staff