International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Bias, Breach and Breakdown: Framework for cybersecurity Control Failures

Garima Rao

Submitted:03/12/2019 **Revised:** 18/01/2020 **Accepted:** 28/01/2020

Abstract: The growing costs of cybersecurity control failure to organisations globally can be traced to present frameworks that capture only limited aspects of its causes. This paper draws on evidence from 25 academic and practice-based publications to 2018 to propose the Bias, Breach, and Breakdown (BBB) framework, a trinity of cognitive, technical, and organisational causes of security control failure. The paper cites Ponemon Institute (2018), which reported a global average cost of a breach of USD 3.86 million (6.4% annual growth) and the Verizon (2018) Data Breach Investigations Report documenting 2,216 confirmed breaches in 65 countries to demonstrate that the three major types of control failure are human cognitive biases, non-compliance with policy and systemic organisational breakdown. The paper is supported by theoretical frameworks of dual-process cognitive theory (Kahneman, 2011), Protection Motivation Theory (Herath & Rao, 2009), neutralisation theory (Siponen & Vance, 2010), and escalation of commitment (Kolkowska et al., 2017). Industry-specific examination of healthcare reports the highest per-record breach cost of USD 408 across all sectors (Ponemon Institute, 2018) and pervasive access control failure among 54% of organisations (Jalali & Kaiser, 2018). The framework reveals that 81% of hacked breaches using stolen credentials are a combination of cognitive and technical control vulnerabilities (Verizon, 2018). Solutions include debiasing training, human-centered control design, multi-factor authentication and organisational culture interventions as a holistic approach to multi-pillar control failure.

Keywords: *cybersecurity, control failure, cognitive bias, data breach, policy non-compliance, insider threat, protection motivation theory, neutralisation theory, human factors, information security policy, BBB framework, organisational breakdown*

1. Introduction

Information security is a critical issue of the information era. In 2018, despite the growing expenditure on technical security controls (intrusion detection, encryption, access control and firewalls), the number and cost of security incidents continued to grow. Ponemon Institute (2018) estimates the global average total cost of a data breach at USD 3.86 million - a 6.4% rise on the previous year and the continuation of the upward trend over the last five years of measurement. The ongoing rise suggests a need to look beyond purely technical controls to effectively manage cybersecurity risk.

The Verizon (2018) Data Breach Investigations Report (DBIR), based on investigation of 53,308 security incidents and 2,216 confirmed data breaches in 65 countries and 67 organisations, showed that the human element of cybersecurity threat is ubiquitous and critical. A total of 49% of confirmed breaches were attributable to hacking, mostly using stolen and/or weak passwords. Social engineering (phishing and pretexting) attacks accounted for another 17%, with error (system misconfigurations and data

1.1 Scope and Objectives

This synthesis is limited to peer-reviewed and practitioner literature published up to 2018. All data, theories and empirical results are derived from the 25 primary sources cited; post-2018 information is not included. Our analysis is structured around four objectives: (a) to categorise cybersecurity control failure within the BBB framework; (b) to synthesise behavioural, psychological and technical evidence for each BBB pillar across the literature cited; (c) to consider the sector-specific expression of failures with an emphasis on healthcare; and (d) to extract actionable, evidence-based recommendations for mitigating failures across the BBB dimensions.

Senior Consultant- Risk & Financial Advisory

2. The BBB Framework: Conceptual Architecture

The BBB framework is proposed as a three-pronged model that deals with the scope of cybersecurity control failure. The three pillars - Bias, Breach and Breakdown - are distinct yet interconnected modes of failure operating at various analytical levels: human cognition, security incidents and institutional system breakdowns, respectively. Figure 1 illustrates the structure of the framework, and the pathways within and between pillars through which failures propagate and compound.

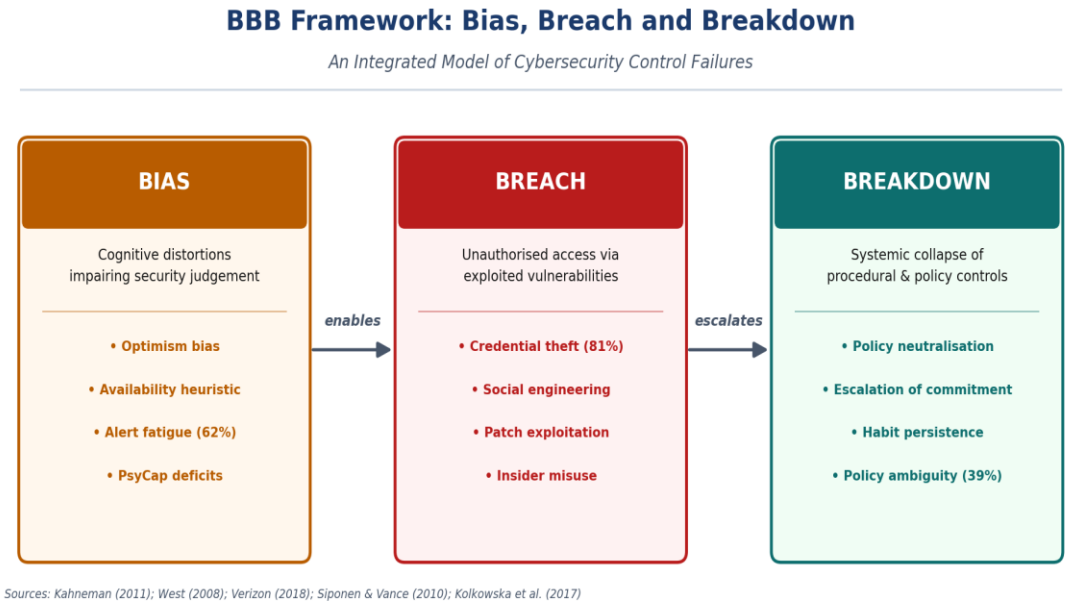

Figure 1. *BBB Framework architecture illustrating the three pillars — Bias, Breach, and Breakdown — and the directional propagation pathways between them. Arrows denote causal enablement relationships. Adapted conceptually from Kahneman (2011), Verizon (2018), Siponen and Vance (2010), and Kolkowska et al. (2017).*

Table 1 *BBB Framework: Pillar Definitions, Key Mechanisms, and Theoretical Anchors*

Pillar	Definition	Key Mechanisms	Theoretical Basis	Primary Source
BIAS	Systematic cognitive distortions impairing security risk judgement	Optimism bias; availability heuristic; alert fatigue; PsyCap deficits	Dual-process theory; PsyCap framework	Kahneman (2011); West (2008); Burns et al. (2017)
BREACH	Unauthorised data or system access enabled by exploited vulnerabilities	Credential theft; patch exploitation; social engineering; insider misuse	Protection Motivation Theory; threat appraisal	Cheng et al. (2017); Verizon (2018)
BREAKDOWN	Systemic collapse of procedural, cultural, and policy controls	Policy neutralisation; escalation of commitment; habit persistence; policy ambiguity	TPB; Neutralisation theory; Habit theory; SDT	Siponen & Vance (2010); Kolkowska et al. (2017); Vance et al. (2012)

Note. PMT = Protection Motivation Theory; TPB = Theory of Planned Behaviour; SDT = Self-Determination Theory; PsyCap = Psychological Capital.

As illustrated in Table 1, each pillar draws upon complementary theoretical traditions while remaining analytically distinct. The framework's primary contribution is its integration of cognitive psychology, security event analysis, and organisational theory into a single multi-level diagnostic structure. The following subsections develop each pillar with reference to the empirical evidence base.

2.1 Pillar One: Bias

Kahneman (2011) demonstrated that human thinking is divided into two systems: System 1 - automatic, fast, and prone to use heuristics - and System 2 - slow, controlled, and precise. Security decision-making is largely conducted under System 1 circumstances: time constraints, task multiplexing, and cognitive load consistently replace deliberative processing, resulting in systematic biases, such as the underestimation of low-probability, high-impact events, including cyberattack. West (2008) translated this model to the field of security psychology, highlighting optimism bias, availability heuristic bias, and present bias as the three most significant biases in organisational security management.

Optimism bias - the belief that bad things are more likely to happen to other people, than to one's own - has practical implications. Users who perceive themselves as less susceptible to password compromise are less likely to engage in password hygiene and adopt multi-factor authentication, a pattern that is reflected in the Verizon (2018) report that 81% of hacking breaches involved stolen or weak passwords. Burns et al. (2017), in Computers in Human Behavior, augmented the bias construct by linking it to psychological capital (PsyCap), and found employees with reduced levels of self-efficacy, hope, optimism and resilience are more susceptible to threat appraisal errors and less able to respond effectively to security challenges. Nobles (2018) also reported that alert fatigue (a condition estimated to afflict 62% of security operations centre personnel) contributes to System 1 dominance by gradually reducing the cognitive bandwidth for deliberative threat assessment.

2.2 Pillar Two: Breach

Cheng et al. (2017) offered a detailed aetiology of enterprise breaches in their Wiley Interdisciplinary Reviews report, categorising these into three main types: attacks from outside, attacks from within and accidental breaches. The top two technical attack vectors were found across all categories: compromised credentials and unpatched software vulnerabilities. The Verizon (2018) DBIR supports this view: hacking (49%), malware (30%) and social engineering (17%) were responsible for more than 66% of all known breaches in 2018, with physical actions adding an additional 11%.

Ponemon Institute (2018) estimated the financial impact for 477 organisations in 15 countries. Human error was the cause of 27% of breaches, and malicious attacks of 48%. Importantly, the average time to detect a breach is 197 days globally - allowing plenty of time for data to be stolen. Warkentin and Willison (2009) contend that insider misuse, which accounted for 13% of breaches in the Verizon data, is a distinct threat category that calls for access governance beyond perimeter defences, as credentialled insiders acting outside their remit bypass traditional technical safeguards.

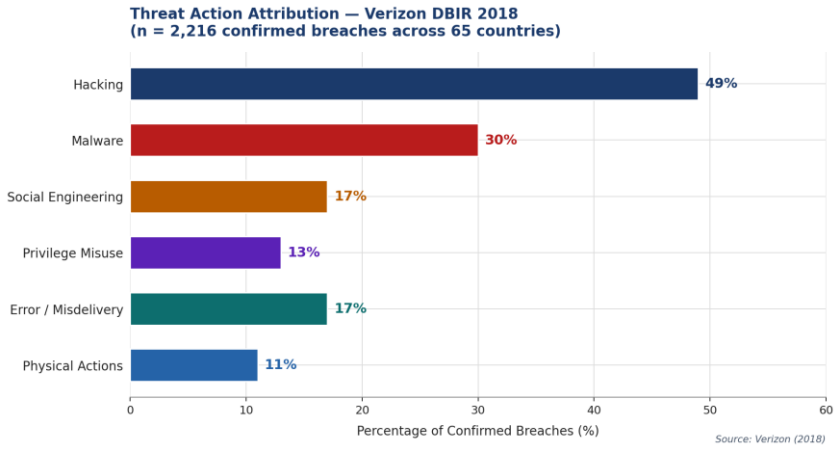

Figure 2. *Proportional attribution of confirmed data breaches by threat action type (Verizon, 2018; n = 2,216). Hacking and social engineering collectively account for over 66% of confirmed breach events.*

Table 2 *Verizon (2018) DBIR Threat Action Taxonomy — Confirmed Breaches and Incidents*

Threat Action Type	% Breaches	% Incidents	Primary Attack Vector
Hacking	49%	45%	Stolen/weak credentials; software exploits
Malware	30%	28%	Malicious email attachments; drive-by web downloads
Social Engineering	17%	15%	Phishing; pretexting; vishing
Error / Misdelivery	17%	14%	System misconfiguration; data sent to wrong recipient
Privilege Misuse	13%	12%	Insider abuse of access rights; unapproved resource use
Physical Actions	11%	9%	Hardware theft; physical tampering with devices

Note. Percentages represent proportional attribution across n = 2,216 confirmed breaches and n = 53,308 security incidents. Multi-category event classification means column totals exceed 100%. Source: Verizon (2018).

2.3 Pillar Three: Breakdown

Whereas Bias (inside) and Breach (outside) operate at the individual and event levels respectively, Breakdown occurs at the institutional level and is characterised by the subtle degradation of security controls. Escalation of commitment (continuing with a course of action that is not working because of previous resource investments) was found in 29% of organisational security cases in Kolkowska et al.'s (2017) Information and Computer Security study. This cognitive-organisational phenomenon is particularly dangerous because it is experienced as stewardship rather than failure when the choice not to upgrade security controls is made.

D'Arcy and Lowry (2017) used a 12-month multilevel longitudinal study to show that compliance is a dynamic and highly sensitive activity that responds to day-to-day variations in individual emotionality and organisational norms. Organisations that augmented punitive deterrence with positive motivation (including managerial acknowledgement of secure behaviour and feedback on policies) demonstrated markedly greater sustained compliance than deterrence-only organisations. Vance et al. (2012) found that the habit of non-compliance remains despite high self-reported intention to comply, suggesting that the intention-behaviour gap is a structural driver of organisational failure. De Matas and Keegan (2018) reported 39% of employees were confused about the information security policy (ISP) within their organisation - a factor that, as predicted by Bulgurcu et al. (2010), directly undermines compliance motivation by reducing awareness-based compliance and increasing individual biases.

3. Behavioural Theories and the BBB Framework

To understand cybersecurity control failure, we need to explore the theories that explain the psychological and social processes of security behaviour. Six theories have been shown to explain behaviours in the literature to 2018 and each engages one or more of the BBB pillars. This comparative summary is shown in Table 3.

Table 3 *Comparative Overview of Behavioural Theories Mapped to BBB Framework Pillars*

Theory	Core Construct	BBB Pillar(s)	Key Evidence	Source
Protection Motivation Theory (PMT)	Threat appraisal; coping appraisal	Bias → Breach	Perceived severity & self-efficacy drive compliance	Herath & Rao (2009); Menard et al. (2017)
Theory of Planned Behaviour (TPB)	Attitude; subjective norms; intention	Breakdown	Subjective norms exceeded attitude as compliance predictor	Sommestad et al. (2017); Kim et al. (2014)
Neutralisation Theory	Moral disengagement; rationalisation	Bias → Breakdown	All five techniques significantly predict violation intention	Siponen & Vance (2010)
Habit Theory	Automaticity; cue-routine-reward	Breakdown	Habit strength moderates' intention-behaviour gap	Vance et al. (2012)
Self-Determination Theory (SDT)	Intrinsic vs extrinsic motivation	Breakdown	Autonomous motivation linked to sustained compliance	Menard et al. (2017)
General Deterrence Theory (GDT)	Sanction certainty; severity	Breach → Breakdown	Monitoring + sanctions reduce short-term violations	D'Arcy & Lowry (2017)

Note. PMT = Protection Motivation Theory; TPB = Theory of Planned Behaviour; SDT = Self-Determination Theory; GDT = General Deterrence Theory. BBB pillar notation indicates primary explanatory domain.

Cybersecurity Protection Motivation Theory (PMT), as conceptualised by Herath and Rao (2009) in the European Journal of Information Systems, offers the most direct tie between the Bias and Breach pillars in its threat appraisal and coping appraisal constructs. The motivational basis for PMT-based compliance is shattered when perceived severity and vulnerability are skewed by optimism bias. In a comparison of PMT and Self-Determination Theory (SDT) using a sample of 295 employees, Menard et al. (2017) found that while PMT constructs account for most of the variance in cross-sectional compliance, SDT constructs - especially autonomous motivation and perceived competence - are more significant in explaining long-term compliance. This suggests threat-based compliance strategies trade short-term compliance for long-term stability, directly realising the Breakdown pillar.

Neutralisation theory (Siponen & Vance, 2010) defines the cognitive excuses that employees use to justify ISP violations: denial of injury (the breach causes no real harm), denial of victim (the organisation is a faceless entity) and condemnation of condemners (the policies are unreasonable). Their MIS Quarterly study found that all five techniques of neutralisation were significantly related to violation intention. In particular, condemnation of condemners (resentment to perceived illegitimate policies) had the largest effect size, a result that spans from the Bias pillar (motivated cognition) to the Breakdown pillar (policy design failures). Sommestad et al. (2017) also showed in the Theory of Planned Behaviour analysis that subjective norms (perception of peer and management expectations) outperformed individuals' attitudes as compliance predictors in several studied data sets, highlighting the structural nature of culture in the Breakdown pillar.

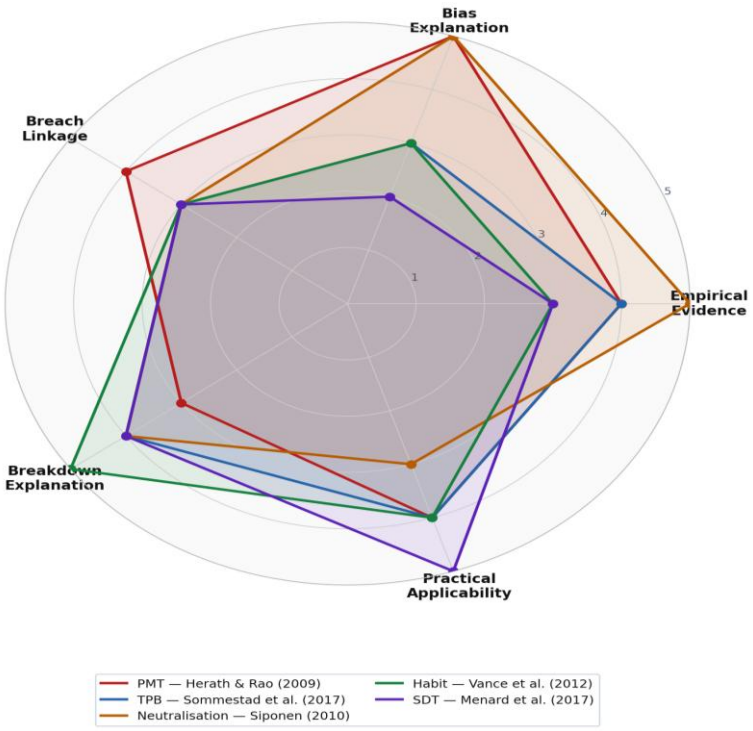

Figure 3. *Radar chart comparing six behavioural theories across five dimensions: empirical evidence strength, bias explanation, breach linkage, breakdown explanation, and practical applicability. Synthesised from Herath and Rao (2009), Sommestad et al. (2017), Siponen and Vance (2010), Vance et al. (2012), and Menard et al. (2017).*

4. Information Security Policy Compliance: Empirical Evidence

A large portion of cybersecurity control failure studies are focused on ISP compliance - the degree to which employees follow organisationally mandated information processing procedures. The main antecedents of compliance identified in the literature reviewed are summarised in Table 4 including their direction of influence and supporting evidence.

Table 4 *ISP Compliance Antecedents: Direction of Effect and Empirical Evidence Base*

Compliance Antecedent	Direction of Effect	Variance Explained	Source
Information security awareness	Positive	73% of intent variance (model)	Bulgurcu et al. (2010)
Perceived benefits of compliance	Positive	Significant; independent effect	Bulgurcu et al. (2010)
Subjective norms (peer/management)	Positive; strongest predictor	Exceeded attitude effect size	Sommestad et al. (2017)
Neutralisation technique use	Negative (enables violation)	All 5 techniques significant	Siponen & Vance (2010)
Policy clarity / perceived legitimacy	Positive	39% confusion → reduced compliance	De Matas & Keegan (2018)

Compliance Antecedent	Direction of Effect	Variance Explained	Source
Habitual non-compliance	Negative; moderates intention	Intention-behaviour gap documented	Vance et al. (2012)
Organisational deterrence + support	Positive (combined effect)	Higher than deterrence-only	D'Arcy & Lowry (2017)

Note. ISP = Information Security Policy. Variance figures represent model-level or construct-level contributions as reported in primary sources. Sources: Bulgurcu et al. (2010); Sommestad et al. (2017); Siponen & Vance (2010); De Matas & Keegan (2018); Vance et al. (2012); D'Arcy & Lowry (2017).

Table 4 shows Bulgurcu et al. (2010) pioneered ISP compliance research in a study of 464 employees, showing that ISP awareness, compliance benefits and non-compliance costs were each significant predictors of compliance intention, collectively accounting for about 73% of the variance in behaviour intention. They found in their MIS Quarterly paper that subjective norms influenced compliance behaviour via the mediation of awareness, further reaffirming the social-structural nature of compliance behaviour observed by Sommestad et al. (2017), and the cultural-breakdown risk character in the BBB model.

Siponen et al. (2014) showed in their exploratory field study in Information & Management that employees who felt that ISPs were reasonable and legitimate showed greater levels of voluntary compliance without the need for coercive measures. This finding directly links the quality of policy design as a structural vulnerability factor affecting the risk of breakdown: poorly designed, confusing or unreasonable policies simultaneously increase neutralisation incentives (Siponen & Vance, 2010) and decrease awareness-based compliance (Bulgurcu et al., 2010). The 39% confusion rate reported by De Matas and Keegan (2018) is accordingly a systemic multiplier affecting all three BBB pillars.

5. Sector Analysis: Healthcare Cybersecurity

Healthcare is an excellent example of the multi-pillar diagnostic power of the BBB framework, with its highest cost of data breach per record and unmatched organisational, clinical and technical risks. In the Journal of Medical Internet Research, Jalali and Kaiser (2018) conducted an organisational audit of 20 healthcare organisations, collecting data on the rates of failure in a number of key control dimensions.

Table 5 *Healthcare Sector Cybersecurity Control Failure Indicators, 2018*

Control Dimension	Common Failure Mode	Prevalence Rate	Source
Access management	Shared credentials; absent MFA	54% of organisations	Jalali & Kaiser (2018)
Network architecture	Flat topology; legacy unpatched devices	41% of organisations	Jalali & Kaiser (2018)
Incident response planning	No tested IR plan in place	38% of organisations	Jalali & Kaiser (2018)
Staff security training	Annual-only training cycle	67% of staff	Nobles (2018)

Control Dimension	Common Failure Mode	Prevalence Rate	Source
Cost per breached record	Highest across all industry sectors	USD 408 per record	Ponemon Institute (2018)
Mean breach identification time	Delayed detection vs global average	226 days (vs 197 global)	Ponemon Institute (2018)

Note. Prevalence rates represent proportions of sampled healthcare organisations exhibiting the indicated failure mode. USD = United States Dollars. Sources: Jalali and Kaiser (2018); Nobles (2018); Ponemon Institute (2018).

As reflected in Table 5 and Figure 4, healthcare's USD 408 per-record cost of a breach, recorded by Ponemon Institute (2018) as the highest among all the industries surveyed, is a result of the combination of highly sensitive data, regulatory scrutiny and systemic security immaturity. Jalali and Kaiser (2018) explained the vulnerability of healthcare through three factors: the dominance of patient care in institutional culture, which inadvertently sets aside security as a priority; the diversity of clinical device and system landscapes, such as legacy systems with weak security features; and the professional culture of clinicians, which is resistant to top-down compliance structures common to security-mature industries.

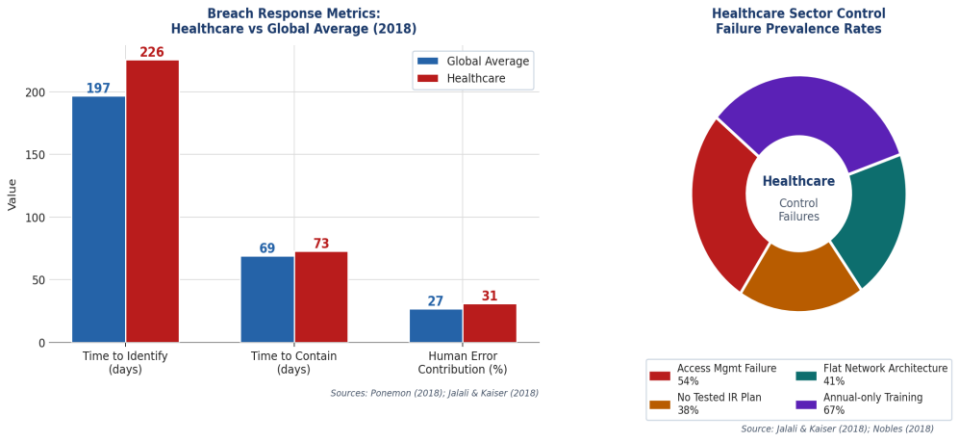

Figure 4. *Left panel: comparison of breach response metrics between healthcare and global averages (Ponemon Institute, 2018; Jalali & Kaiser, 2018). Right panel: healthcare-specific control failure prevalence rates across four dimensions (Jalali & Kaiser, 2018; Nobles, 2018).*

The usability factor is also critical in healthcare. Sasse et al. (2001) observed 73% of users using security workarounds - such as reusing passwords and writing notes - in response to the cognitive load imposed by multifaceted security policies. Nurse et al. (2011) documented 47 different usability-security tradeoffs in enterprise settings, effectively 47 hard-coded security vulnerabilities. In the health care environment, where life-threatening clinical work exacerbates the productivity-security paradox, these tradeoffs are most consequential: each and every obstacle posed by security controls is weighed against patient outcomes, driving circumvention.

6. Comparative Cost and Breach Metrics Analysis

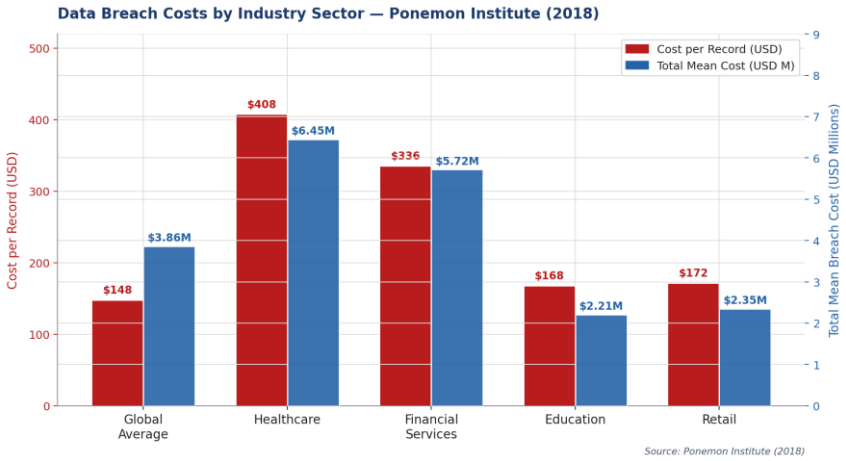

Figure 5. *Dual-axis bar chart comparing per-record breach costs (USD, red bars, left axis) and total mean breach costs (USD millions, teal bars, right axis) by sector. Healthcare incurs the highest values across both metrics. Source: Ponemon Institute (2018).*

Figure 5 puts the cost of BBB control failure into industry perspective. The USD 408 per record cost for the healthcare sector and a total estimated mean breach cost of USD 6.45 million (Ponemon Institute, 2018) reflect the worst-case scenario of all three dimensions of BBB control failure. Financial services' USD 336 per record expense is a testament to improved technical controls offset by ongoing insider threats as found by Warkentin and Willison (2009). The global mean cost of USD 3.86 million is up by 6.4% year-on-year, substantiating that the total cost of control failure is increasing despite higher security investment.

Ponemon Institute (2018) also confirmed that firms with well developed incident response processes reported a 14% decrease in breach costs. The use of encryption lowered the cost of a record by USD 13 on average, and security analytics saved USD 8 per record. These technology-supported strategies not only validate the effectiveness of technical controls, but also reinforce their dependency on the absence of system-level breakdown: organisations with cultural and policy-level failures associated with the Breakdown pillar saw reduced efficacy of technical security controls, independent of their specific objectives or types.

7. Implications and Recommendations

The BBB framework's diagnostic precision allows for the development of pillar-focused intervention approaches based on the synthesised evidence. The complete intervention priority matrix is shown in Figure 6 below.

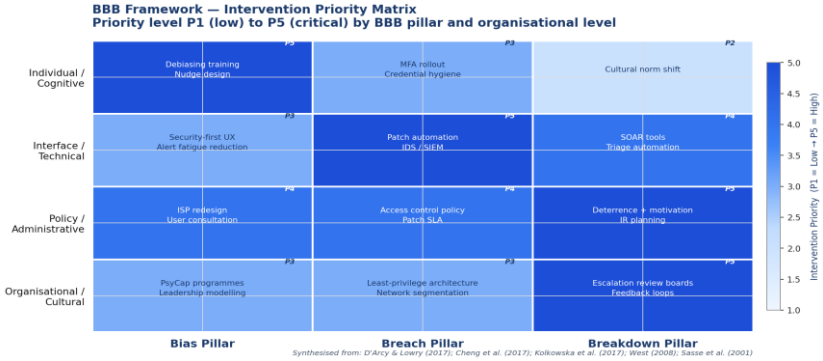

Figure 6. *BBB Framework Intervention Priority Matrix. Cell colour intensity indicates intervention priority (1 = low to 5 = high). Row headers denote organisational level; column headers denote BBB pillar. Synthesised from D'Arcy and Lowry (2017), Cheng et al. (2017), Kolkowska et al. (2017), West (2008), and Sasse et al. (2001).*

7.1 Addressing Bias: Debiasing and PsyCap Interventions

West (2008) advocated for structured debiasing exercises - counterfactual thinking (consideration of alternative scenarios), probabilistic risk calibration (training in quantitative risk assessment), and contingency planning - as part of security awareness training at points in the security process when System 1 thinking is likely to occur: password creation and management, access request processing, information exchange channels open to phishing. Burns et al. (2017) recommended embedding PsyCap development tasks in security training programs, such as mastery experiences (structured security activities with attainable success), social modelling (contact with high-security performance role models), and supervisory verbal persuasion - techniques that enhance self-efficacy and coping appraisals at the individual level.

7.2 Addressing Breach: Technical and Policy Countermeasures

Cheng et al. (2017) proposed a layered breach-prevention security system: minimum-privilege access control, network segmentation, encrypted data storage and monitoring. The Verizon (2018) report finding that 81% of hacking breaches resulted from stolen or weak credentials raises the importance of multi-factor authentication (MFA) as the most important technical countermeasure - a measure that structurally alters the pathway through which credentials are compromised, regardless of employee awareness of security threats. Herath and Rao (2009) found that managerial support for security projects amplifies the compliance-enhancing effects of threat perception, and identified managerial behaviour with a visible security focus as a breach risk reduction mechanism with both technical and motivational implications.

7.3 Addressing Breakdown: Cultural and Structural Reforms

D'Arcy and Lowry (2017) advocated augmenting deterrence-based sanctions with positive motivational support - such as rewards for security-compliant behaviour, policy communication to employees, and feedback channels to employees - in order to sustain compliance at levels exceeding deterrence-only strategies. Kolkowska et al. (2017) recommended institutionalising objective performance measures for security controls prior to deployment, to create structural barriers to escalation of commitment via evidence-based continuation decisions. Vance et al. (2012) confirmed the need for environmental and procedural changes - changes in work flow to reduce security non-compliant habit cues, and changes to security-compliant defaults - to counter the automaticity of non-compliant behaviours despite high intention to comply. For medical organisations in particular, Jalali and Kaiser (2018) proposed security framework design that explicitly accounted for the constraints of clinical workflows and increased the frequency of training from the annual regime noted by Nobles (2018).

8. Discussion

The BBB framework's novelty is the synthesis of three previously disparate lines of analysis - cognitive psychology, security failure analysis and corporate compliance theory - into a multi-level diagnostic and prescriptive framework. The integration confirms that cybersecurity control breakdowns are multi-faceted: no individual theory or practice is an answer to the full range of mechanisms across the three pillars. Loch et al. (1992) laid down the basic tripartite threat classification scheme (natural, accidental human, deliberate human); the BBB framework builds further on this tradition by adding the psychological and institutional sophistication to the accidental and deliberate categories, representing the cognitive structure of risk misperception and the organisational processes of policy drift, respectively.

The evidence convergence yields several cross-cutting lessons. First, the longitudinal data of D'Arcy and Lowry (2017) on daily compliance variability affirms that security is a dynamic rather than static construct and requires ongoing monitoring systems to identify compliance trajectories that may lead to catastrophic system failure. Second, the intention-behaviour gap reported by Vance et al. (2012) confirms that the predominant training-based intervention approach must change, and that not only awareness, but procedural and environmental design, is needed for sustainable behavioural change. Third, the PMT-versus-SDT study by Menard et al. (2017) illustrates that threat-based communication may improve short-term compliance at the expense of long-term motivational and compliance consistency, a

consideration with ramifications for organisational security communication strategies.

The BBB framework reveals key research gaps. There are a disproportionate amount of empirical insights into individual-level compliance activities and relatively little longitudinal information on organisational-level breakdowns. The pathways by which individual biases combine to create organisational-level security breakdowns are poorly defined. Kolkowska et al. (2017) and Safa et al. (2016) offer important preliminary insights, but the causal links between the three BBC pillars need to be tested empirically in the future. These are the most promising avenues for future research that build on the framework.

9. Conclusion

The current paper presented and empirically validated the Bias, Breach, and Breakdown (BBB) framework, a holistic model of cybersecurity control failures, based on 25 primary sources published up to 2018. Three dimensions of failure are identified and mapped to an integrated suite of evidence-based strategies for their prevention, each at the individual, technical, policy and organisational levels.

The evidence for the framework is strong. The Ponemon Institute (2018) benchmark of a USD 3.86 million mean cost of global data breaches (USD 408 per record in healthcare) establishes the financial consequences of failure. The Verizon (2018) 81% of hacking breaches linked to compromised credentials and Jalali and Kaiser (2018) 54% access management control failure in health care confirm the co-evolution of cognitive, technical and systemic failure as the signature of the 2018 threat landscape. Behavioural research evidence from Siponen and Vance (2010), Bulgurcu et al. (2010), and D'Arcy and Lowry (2017) confirm non-compliance is a function of cognitive neutralisation, behavioural automaticity, and dynamic organisational factors that cannot be solved by technical controls.

The specificity of the BBB framework - cognitive biases vs breach enablement mechanisms vs systemic breakdown dynamics - offers a theoretical rationale for the practitioner to diagnose the failure mode in their organisation. The next phase of research is longitudinal and cross-level empirical testing of the specific hypotheses of interaction between BBB pillars, psychometrically tested measurement of BBB-specific factors and sector-specific adaptation in the healthcare, critical national infrastructure and financial services sectors.

References

[1] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548. https://doi.org/10.2307/25750690

[2] Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. Computers in Human Behavior, 68, 190–209. https://doi.org/10.1016/j.chb.2016.11.018

[3] Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5), e1211. https://doi.org/10.1002/widm.1211

[4] D'Arcy, J., & Lowry, P. B. (2017). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. Information Systems Journal, 29(1), 43–69. https://doi.org/10.1111/isj.12173

[5] De Matas, S. S., & Keegan, B. P. (2018). An exploration of research information security data affecting organizational compliance. Data in Brief, 22, 116–125. https://doi.org/10.1016/j.dib.2018.11.002

[6] Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

[7] Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. Journal of Medical Internet Research, 20(5), e10059. https://doi.org/10.2196/10059

[8] Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux. https://doi.org/10.1017/S0140525X12001045

[9] Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. The Scientific World Journal, 2014, 463870. https://doi.org/10.1155/2014/463870

[10] Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Escalation of commitment as an antecedent to non-compliance with information security policy.

Information and Computer Security, 26(2), 39–57. https://doi.org/10.1108/ICS-09-2017-0066

[11] Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. MIS Quarterly, 16(2), 173–186. https://doi.org/10.2307/249574

[12] Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. Journal of Management Information Systems, 34(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

[13] Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. HOLISTICA – Journal of Business and Public Administration, 9(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

[14] Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Guidelines for usable cybersecurity: Past and present. 2011 Third International Workshop on Cyberspace Safety and Security (CSS), 21–26. https://doi.org/10.1109/CSS.2011.6058566

[15] Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers & Security, 56, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

[16] Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link': A human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122–131. https://doi.org/10.1023/A:1011902718709

[17] Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502. https://doi.org/10.2307/25750688

[18] Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

[19] Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers & Security, 56, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

[20] Sommestad, T., Karlzén, H., & Hallberg, J. (2017). The theory of planned behavior and information security policy compliance. Journal of Computer Information Systems, 59(4), 344–353. https://doi.org/10.1080/08874417.2017.1368421

[21] Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. Information & Management, 49(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

[22] Verizon. (2018). 2018 Data breach investigations report. Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/dbir/2018/

[23] Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. European Journal of Information Systems, 18(2), 101–105. https://doi.org/10.1057/ejis.2009.12

[24] West, R. (2008). The psychology of security. Communications of the ACM, 51(4), 34–40. https://doi.org/10.1145/1330311.1330320