ISSN: 2473-4901
v12 n6780

Teaching Cybersecurity Principles Through Case-Based Analysis of Cyber Risk

David J. Yates
dyates@bentley.edu

Arthur Ream III
areamiii@bentley.edu

Department of Computer Information Systems
Bentley University
Waltham, MA 02452, USA

Abstract

Using real-world breaches to teach cybersecurity is established practice. This paper contributes a reusable instructional artifact: a case-based framework for an upper-level undergraduate course that maps fifteen takeaways and exemplar incidents to assessable learning objectives. Three clusters—risk visibility and business alignment, incident response and cyber resilience, and modern and future-facing exposure—form a past–present–future reasoning arc. The framework connects durable concepts such as risk management, access control, incident response, and governance to incidents and changing cyber risk. We demonstrate its application through Equifax (2017), Target (2013), and Ring (2019). Instructors can substitute newer incidents while preserving the relationship among cluster, takeaway, case, and objective. Preliminary post-instruction evidence from nine students' Equifax and Target work shows that the objectives can be translated into assessable tasks. The evidence includes independently coded artifacts and consensus ratings but does not establish causal learning gains or transfer to unfamiliar cases.

Keywords: cybersecurity education, case-based teaching, risk management, incident response, cyber resilience, connected devices.

Teaching Cybersecurity Principles Through Case-Based Analysis of Cyber Risk

David J. Yates and Arthur Ream III

1. INTRODUCTION

Cybersecurity courses ask students to learn durable principles such as risk management, access control, incident response, resilience, and governance. These principles can remain abstract when encountered only as textbook concepts or framework categories. Real incidents involve incomplete information, legacy systems, vendor relationships, human procedures, delayed decisions, and business consequences that unfold over time. Students therefore need practice connecting cybersecurity vocabulary to concrete failures. They must ask what control was missing, why risk was visible or invisible, who owned it, how technical choices shaped impact, and what the organization should have learned.

This paper presents a case-based framework for an upper-level undergraduate cybersecurity course. It organizes fifteen real incidents into three teaching clusters (risk visibility and business alignment, incident response and cyber resilience, and modern and future-facing exposure) along a past, present, and future arc that moves from what organizations should have seen before failure, to how they respond when prevention fails, to how principles transfer as technology changes. The clusters are not a universal taxonomy but a scaffold for comparing incidents and transferring ideas across cases.

Teaching cybersecurity through real breaches is not new, and this paper does not claim it as a contribution. Less developed is a reusable structure connecting diverse incidents to specific, assessable learning objectives and supporting transfer across cases. The paper's primary contribution is this structure: an instructional artifact of three tables organizing fifteen case-linked takeaways, exemplar incidents, and learning objectives along a past, present, and future arc. Unlike a single teaching case, it provides breadth across governance, resilience, and emerging exposure while linking each case to an objective supporting discussion, team analysis, exams, or written assignments. It also supports case substitution as the threat landscape changes without changing the framework's underlying instructional purpose.

2. PEDAGOGICAL FRAMING: PAST, PRESENT, AND FUTURE THROUGH CASES

2.1 Why Cases Help Students Connect Principles to Incidents

Textbooks and frameworks give students vocabulary for principles such as risk management, access control, incident response, and governance. Students also need practice applying this vocabulary to incomplete, organizationally complex incidents, where failures usually involve interactions among visible weaknesses, business decisions, technical architecture, human processes, and delayed response.

Case-based teaching moves students from definition to application by asking why concepts such as segmentation, materiality, Zero Trust, or incident response matter in a specific organizational failure. Students must interpret facts, make judgments, compare alternatives, and justify recommendations rather than recall terminology (Prince, 2004; Herreid, 1994). It positions students as analysts who connect technical evidence to organizational consequences and defensible recommendations. Within cybersecurity education, prior work advocates top-down teaching through cases and breach analysis and develops course structures around them (Cai & Arney, 2017; Luburić et al., 2019).

2.2 The Past–Present–Future Arc

The framework uses a past–present–future arc as a teaching device, not a strict chronology. Older incidents do not represent only older problems, nor do newer incidents represent only emerging risks. Instead, the arc organizes three kinds of reasoning: what organizations should see before failure, how they should respond when failure occurs, and how principles transfer into changing technological

conditions. The arc connects recurring failures across time without assigning any case to one temporal category.

The past dimension asks what an organization should have known, owned, escalated, or treated earlier, including failures in visibility, governance, inventories, accountability, and business alignment. The present examines response when prevention fails: access design, detection, containment, recovery, communication, and post-incident learning. The future considers how familiar principles transfer as boundaries shift into cloud services, data-rich platforms, connected devices, identity systems, software supply chains, and human support workflows. Across all three, the goal is preparation for unfamiliar incidents, not prediction.

2.3 From Case Narratives to Transferable Analysis

The goal is not memorizing breach histories. Incidents are useful when students practice analytical transfer through case-based inquiry (Herreid, 1994). Recalling that Equifax involved an unpatched Apache Struts vulnerability, Target involved third-party vendor credentials, or Ring involved connected cameras demonstrates knowledge of case facts. Explaining how those facts reveal broader patterns of risk visibility, access design, accountability, incident impact, privacy, and governance begins to demonstrate cybersecurity judgment.

Cybersecurity education must prepare students for incidents that have not occurred. A future breach may involve a different technology, industry, attacker, or regulatory setting, but students can still ask durable questions about visible risk, ownership, blast radius, data exposure, procedural weaknesses, and lessons learned. Comparison matters because transfer requires recognizing a principle even when an unfamiliar incident presents different surface details.

A standalone case deepens understanding of one incident. The framework asks students to identify its transferable principle, apply it to another incident, and articulate the assessable objective the comparison serves. This provides repeated practice moving among specific incidents, general principles, and new cases.

Cases therefore function as instructional lenses rather than isolated stories. Each is tied to a takeaway and learning objective, and Section 3 organizes fifteen cases into three cluster tables that support discussion, assessment, and substitution.

2.4 Related Work: Case-Based Cybersecurity Teaching

Real-breach cases are established in information systems and cybersecurity education. Plachkinova and Maurer (2018) present a teaching case that leads students through Target's vendor-management processes, third-party vulnerability, response, and lessons learned. Harrell (2017) analyzes the breach through a work-system, macro-ergonomic lens integrating technical, organizational, and human factors. Recent work has developed and evaluated a case-based learning instrument for information-security management and reviewed case-based learning for cybersecurity leaders (Ahmad et al., 2021; Anderson et al., 2024). Together with broader arguments for case-driven instruction (Cai & Arney, 2017) and structured case-study frameworks for security teaching (Luburić et al., 2019), this literature establishes case-based cybersecurity instruction while leaving course-level mapping of multiple incidents to transferable, assessable objectives and case substitution less developed.

Our contribution is not the use of breach cases or a new single case, but an organizing artifact above individual cases. Existing teaching cases develop one incident in depth, while CSEC 2017 and the NICE Workforce Framework define knowledge areas and work roles at the program level (Joint Task Force on Cybersecurity Education, 2017; Petersen et al., 2020). This middle level gives instructors more structure than an isolated case without prescribing a curriculum. Between them lies the gap addressed here: a concise, course-level structure linking diverse incidents to assessable learning objectives, clustering them along a past–present–future arc, and supporting case substitution.

3. THE CASE-BASED TEACHING ARTIFACT: THREE CLUSTER TABLES

This section presents the paper's central artifact: three cluster tables linking cybersecurity takeaways to exemplar incidents and student learning objectives. Section 4 develops Equifax, Target, and Ring as applications.

3.1 Design Logic: Curated Framework, Not Exhaustive Taxonomy

The framework is intentionally selective. Its incidents help students move from a specific case to a broader principle and then to unfamiliar incidents.

The framework was constructed as an instructor-designed artifact in four stages. First, durable course principles were organized around three recurring reasoning tasks: recognizing, owning, and communicating risk before failure; responding and sustaining operations when prevention fails; and transferring established principles to changing technologies and dependencies. These tasks produced the Risk Visibility and Business Alignment, Incident Response and Cyber Resilience, and Modern and Future-Facing Exposure clusters. The past–present–future arc is a pedagogical sequence, not a claim that cybersecurity problems fall into three exhaustive categories.

Second, each cluster was decomposed into five actionable takeaways, providing balanced coverage and a manageable instructional sequence rather than implying that cybersecurity contains exactly fifteen principles. Each retained takeaway represented a distinct primary instructional purpose expressible through an assessable learning objective. Related concepts could reinforce one another, but takeaways requiring essentially the same student judgment or performance were not retained.

Third, one exemplar incident was selected for each takeaway using four criteria: authoritative documentation suitable for classroom use; clear illustration of the target principle; collective variation across sectors, technologies, and time; and substitutability without changing the takeaway or objective. Fourth, the matrix was reviewed within clusters for coverage and across clusters for unnecessary duplication and opportunities for comparison and transfer. Each of its fifteen rows links one primary takeaway, exemplar case, and assessable objective.

The framework complements curricular and workforce resources. CSEC 2017 and NICE define knowledge areas and work roles but do not prescribe how to translate principles into case-anchored objectives that instructors can assign, assess, and substitute (Joint Task Force on Cybersecurity Education, 2017; Petersen et al., 2020).

3.2 Cluster 1: Risk Visibility and Business Alignment

The first cluster addresses conditions that make cybersecurity failures possible before an incident becomes visible as a breach. Organizations must see and prioritize cyber-relevant risk and connect it to business decisions and consequences. Cyber situational awareness requires a usable understanding of assets, exposures, vulnerabilities, threats, and consequences (Franke & Brynielsson, 2014). Business alignment requires connecting cybersecurity priorities to organizational objectives, decision processes, and business impact rather than treating them as purely technical concerns (Philippou et al., 2020). The cluster therefore connects technical visibility with organizational responsibility and prioritization.

Table 1 moves from visible risk to inherited business risk, accountability, inventories, and business impact. Its cases span a software-vulnerability exposure, acquisition-driven inherited risk, accountability and escalation failure, remote-access and inventory gap, and healthcare business-impact case. Together, they show how different risks accumulate before a breach without duplicating one type of failure.

Takeaway	Exemplar case	Learning objective
Visible risks must be identified and prioritized.	Microsoft Exchange Server (2021); (CISA, 2021)	Students will be able to explain how visible weaknesses, including exposed systems, delayed patching, weak monitoring, and limited remediation capacity, should be prioritized before they become enterprise-level failures.
Cybersecurity risk travels with business decisions.	Marriott / Starwood (2018); (FTC, 2024)	Students will be able to analyze how mergers, acquisitions, legacy systems, and integration decisions can transfer or amplify cybersecurity risk.
Accountability must be assigned before risk becomes crisis.	Equifax (2017); (U.S. House Committee on Oversight and Government Reform, 2018)	Students will be able to evaluate how risk ownership, escalation authority, and treatment priorities shape whether known risks are managed before they become material failures.
Inventories must include remote-access paths and dormant accounts.	Colonial Pipeline (2021); (Blount, 2021)	Students will be able to explain why cybersecurity asset inventories must include remote-access paths and inactive or legacy accounts, and how an unmonitored remote-access route (such as the compromised legacy VPN account) can create an entry point for attackers.
Cyber risk must be translated into business impact.	Change Healthcare (2024); (American Hospital Association, 2024)	Students will be able to translate cybersecurity risk into business impact, including operational disruption, revenue and cash-flow loss, and continuity risk across dependent organizations.

Table 1. Risk Visibility and Business Alignment

3.3 Cluster 2: Incident Response and Cyber Resilience Lifecycle

The second cluster concerns capabilities organizations need when prevention fails. It combines incident response—prepared roles, coordinated processes, timely decisions, and translation of technical signals into organizational action (Ahmad et al., 2012)—with cyber resilience: continuity, damage limitation, trusted recovery, and improvement after disruption (Linkov & Kott, 2019). This emphasis is consistent with case-based teaching centered on organizational response and lessons learned rather than prevention alone (Plachkinova & Maurer, 2018; Harrell, 2017).

Table 2 presents five lifecycle-oriented objectives moving from access architecture and segmentation to detection, containment, recovery, and lessons learned. These objectives frame response as a lifecycle extending from preparedness through recovery and institutional learning after an incident.

Takeaway	Exemplar case	Learning objective
Third-party access and segmentation shape incident impact.	Target (2013); (U.S. Senate Committee on Commerce, Science, and Transportation, 2014)	Students will be able to explain how third-party credentials, weak network segmentation, and Identify/Protect/Detect failures can expand blast radius and delay detection (NIST, 2024).
Early detection greatly reduces damage.	Anthem (2015); (U.S. Department of Health and Human Services, Office for Civil Rights, 2018)	Students will be able to analyze how delayed detection of unauthorized access enabled large-scale exposure of sensitive health data, and how monitoring and timely investigation reduce the duration and reach of a breach.
Isolation must be swift.	NotPetya (2017); (Microsoft, 2018)	Students will be able to explain how rapid containment of affected systems, credentials, and network segments can limit lateral movement and reduce business-wide disruption.
Recovery and remediation require skill and speed.	City of Atlanta ransomware attack (2018); (U.S. Attorney's Office, Northern District of Georgia, 2018)	Using the City of Atlanta attack as the incident context, students will be able to explain why recovering from a disruptive ransomware attack requires planned triage, validated restoration, system rebuilding, and continuity management, and why recovery speed and skill determine operational impact (Nelson et al., 2025).
Every breach should be analyzed for lessons learned.	OPM data breach (2015); (U.S. Government Accountability Office, 2017)	Students will be able to identify root causes, control failures, decision failures, and corrective actions that should follow from post-incident analysis.

Table 2. Incident Response and Cyber Resilience Lifecycle

3.4 Cluster 3: Modern and Future-Facing Cyber Exposure

The third cluster addresses exposure created by dependence on cloud services, connected devices, data-rich platforms, software supply chains, identity systems, and human support processes. Its technology dimension draws on the security, privacy, and trust challenges of interconnected environments such as the Internet of Things (Sicari et al., 2015). Its human and organizational dimension recognizes that failures often emerge from interactions among people, procedures, and system design rather than user weakness alone (Sasse et al., 2001). This cluster is a teaching device for transfer, not a formal taxonomy or prediction of a fixed future: It groups cases in which familiar principles must be reapplied as system boundaries shift.

Table 3 presents five objectives addressing trust assumptions, data retention, layered controls, connected technologies, and human or procedural attack paths.

Takeaway	Exemplar case	Learning objective
Zero Trust principles are essential.	SolarWinds (2020); (CISA, 2020)	Students will be able to explain why software updates and vendor-supplied code, as in the SolarWinds supply-chain compromise, cannot be treated as inherently trusted, and how Zero Trust principles apply continuous verification to internal and vendor activity (Rose et al., 2020).
Data retention increases breach impact.	23andMe (2023); (Office of the Privacy Commissioner of Canada & U.K. Information Commissioner's Office, 2025)	Students will be able to analyze how sensitive data collection, retention, sharing features, and data-linkage decisions can expand the harm caused by compromised accounts.
Defense in depth requires multiple layers.	Capital One (2019); (Capital One, 2021)	Students will be able to explain how a single misconfiguration, as in the Capital One cloud breach, can defeat an otherwise protected environment and why layered controls such as secure configuration, least privilege, and monitoring reduce dependence on any one safeguard (NIST, 2024).
Connected technologies move the attack surface into daily life.	Ring (2019 / 2023 FTC action); (FTC, 2023)	Students will be able to analyze how connected devices, cloud services, account controls, vendor access, and private-space data collection create new targets, dependencies, and governance obligations.
Human and procedural weaknesses can defeat technical controls.	MGM Resorts / Scattered Spider (2023); (CISA, 2025)	Students will be able to evaluate how help-desk procedures, identity checks, MFA resets, escalation rules, and security culture function as cybersecurity controls.

Table 3. Modern and Future-Facing Cyber Exposure

3.5 Using the Tables: Breadth, Transferability, and Case Substitution

The tables provide breadth without treating the cases as a fixed canon. Their objectives are related rather than mutually exclusive because incidents rarely fit isolated categories: Risk visibility affects detection, segmentation affects containment, data retention affects impact, and identity workflows affect technical and procedural controls. Even with these connections, each row emphasizes a distinct instructional point.

A standalone case can support contextual analysis but does not itself provide a repeatable path to other incidents. The framework supplies this path. Students identify a takeaway anchored in one incident, compare its operation in another case within or across clusters, and apply the associated objective to an unfamiliar incident with different facts, technology, or organizational circumstances. This moves students from facts to principle, comparison, and transfer rather than treating each breach as self-contained.

Instructors can work in reverse: Begin with an objective, select its framework row, assign the exemplar or a substitute meeting the Section 3.1 criteria, and assess the same reasoning through discussion, team analysis, an examination question, or written work. Separating the stable takeaway and objective from the replaceable case permits updated incidents without changing the curricular purpose. Students are assessed on explaining and applying a transferable principle, not merely recalling a familiar breach. This structure makes assessment expectations explicit while allowing the incident context to change as threats and technologies evolve.

4. APPLYING THE FRAMEWORK: EQUIFAX, TARGET, AND RING

Section 3 presents the framework in breadth; this section applies one case from each cluster in depth.

4.1 Equifax (2017): Risk Visibility, Accountability, and Materiality

Equifax illustrates the first cluster because the breach was not simply a technical patching failure. The cause was Equifax's failure to patch a known Apache Struts vulnerability in an internet-facing dispute portal, but its teaching value lies in how this vulnerability existed alongside weak risk ownership, inadequate escalation, incomplete asset visibility, and insufficient protection of highly sensitive consumer data. The case moves students from "a missed patch caused the breach" to an integrated question: Why did a known weakness affecting high-value data fail to receive urgent organizational attention?

Equifax is especially useful for distinguishing ordinary technical risk from material business risk. A vulnerability affecting personally identifiable information held by a credit bureau should be treated differently from the same weakness in an isolated, low-value system. The exposed information was not easily changed, making the consequences more durable than many payment-card breaches. The same technical weakness becomes more urgent when it affects high-value, high-consequence data.

The case also clarifies why accountability matters before a crisis. When patching responsibility, system ownership, escalation, and treatment priorities are unclear, known vulnerabilities can remain unresolved even when a fix is available. Equifax connects risk registers, risk ownership, and escalation authority to organizational consequences, consistent with guidance on integrating cybersecurity risk into enterprise risk management (Quinn et al., 2025). It directly supports the framework's objective that students evaluate how ownership, escalation authority, and treatment priorities determine whether known risks are managed before becoming material failures (U.S. House Committee on Oversight and Government Reform, 2018).

4.2 Target (2013): Third-Party Access, Segmentation, and Incident Impact

Target illustrates the second cluster because pre-incident access decisions shape incident response and resilience. The breach is remembered for compromised third-party HVAC vendor credentials, but its instructional value is broader: Once attackers held valid credentials, weak segmentation allowed movement beyond the vendor-access environment toward payment systems. Access pathways created before an attack can determine its scale, speed, and consequences after attackers gain a foothold.

For students, Target connects concepts taught separately: third-party access (identity, least privilege, vendor oversight, and access review), segmentation (containment, lateral movement, and blast radius), and detection (monitoring, alert triage, escalation, and the difference between possessing security tools and acting on their warnings). Target therefore shows how third-party credentials, weak segmentation, and NIST CSF 2.0 Identify/Protect/Detect failures can expand incident impact and delay detection (NIST, 2024).

Within the framework, students recommend stronger vendor access management, segmentation, monitoring, and escalation, then explain how each would reduce blast radius and detection time. Incident response begins before the first alert: Resilience depends on architecture, access rules, and detection processes operating when compromise occurs (Ross et al., 2021). The U.S. Senate report's "missed opportunities" framing directs attention to the gap between warning signs and effective action (U.S. Senate Committee on Commerce, Science, and Transportation, 2014).

Because Target is an established teaching case (Plachkinova & Maurer, 2018; Harrell, 2017), we use it narrowly as the worked exemplar for one cluster, mapping third-party access and segmentation to an assessable learning objective and analytical moves students can apply across cases.

4.3 Ring (2019): Connected Devices, Vendor Access, and Private-Space Data

Ring illustrates the third cluster by moving cybersecurity analysis into domestic environments. The case concerns not only connected cameras or weak account security, but also the ecosystem linking

consumer devices, cloud services, mobile applications, vendor operations, employee access, and private-space data. Ring shows how risk changes when digital systems enter homes, doorways, and neighborhoods where users expect privacy: The attack surface extends beyond enterprise servers into daily life.

The case frames vendor access as a governance problem. Connected-device companies may need employees, contractors, or service providers to support products and manage platform operations. These pathways create risk unless access is limited, monitored, logged, and justified. The Federal Trade Commission alleged that Ring failed to control employee and contractor access to customer videos and provide adequate safeguards against account takeovers (FTC, 2023). Thus, privacy and cybersecurity controls must govern both external attackers and internal access pathways.

Ring's data are intimate. Home-security video may reveal household routines, visitors, children, neighbors, and movement patterns. Because harm is linked to the private-space context in which data are created, Ring introduces privacy as contextual integrity (Nissenbaum, 2004). It supports the objective that students analyze how connected devices, cloud services, account controls, vendor access, and private-space data create new targets, dependencies, and governance obligations (FTC, 2023).

Together, the cases demonstrate transfer across the three clusters. Equifax shows technical risk becoming material organizational failure when ownership and escalation are weak; Target shows incident impact shaped by pre-incident access and segmentation decisions; and Ring extends the same analytical habits into connected-device ecosystems where security, privacy, vendor access, and private-space data converge. All three rehearse movement from incident facts to a transferable principle and then to a new case, reinforcing the teaching claim that cybersecurity failures emerge from interactions among people, processes, technology, governance, and business decisions.

5. CLASSROOM USE, EVIDENCE, LIMITATIONS, AND CONCLUSION

5.1 Classroom Implementation

The framework functions as a synthesis activity in an upper-level undergraduate course after students encounter risk management, access control, incident response, and resilience (Meeuwisse, 2017). It connects textbook principles to incidents without requiring every incident to become a full case study.

One approach introduces the framework near the course's end as a review activity: Students compare the clusters, examine differences in technical cause and organizational consequence, and relate learning objectives within a cluster. A second approach uses Equifax, Target, and Ring for deeper analysis: Equifax for risk ownership and materiality, Target for third-party access and blast radius, and Ring for connected-device exposure and private-space data governance. In either format, students move from case facts to a learning objective and transferable principle. Instructors may also begin with an intended objective, select its framework row, and choose either the exemplar or an appropriate substitute.

The framework also supports assessment. Exams, exercises, or team presentations can ask students to apply one row to a new incident, emphasizing analysis across people, process, technology, governance, and business consequences rather than recall. For example, after analyzing Target, students could explain how access architecture and segmentation affected lateral movement, detection, and containment in an unfamiliar third-party compromise. The incident changes, but the Table 2 objective and expected performance remain stable.

5.2 Evidence from Student Work

The Equifax and Target student work provides preliminary evidence that the framework can be operationalized in assignments and exams. Before coding, submissions were de-identified and course grades finalized; only aggregate results are reported. The artifacts show post-instruction application, not causal evidence of learning gains, but demonstrate that the case-based objectives can become assessable tasks examined through post hoc coding rubrics.

The Equifax in-class exercise (Appendix A) asks students to apply stacked risk, materiality, probability, impact, proximity, risk registers, ownership, lifecycle stages, treatment options, and risk assessment (Meeuwisse, 2017); it aligns with the Equifax row in Table 1. The Target final-exam question (Appendix B) addresses third-party HVAC vendor credentials, segmentation, Identify/Protect/Detect failures, recommendations, blast radius, and detection time (NIST, 2024); it aligns with the Target row in Table 2. This pairing demonstrates how the same framework structure can support both a collaborative exercise and an individual examination question while preserving alignment between the case, objective, and expected reasoning.

The analysis covered 18 artifacts from nine students who completed both assignments. The Appendix C post hoc rubrics were applied respectively to the Equifax and Target submissions. The rubrics were not the original grading instruments; they were applied after instruction to describe how completely each response integrated the concepts represented by its corresponding framework row. Both authors independently coded every submission as Strong, Developing, or Limited on each dimension. They compared ratings and notes, discussed differences, and reached consensus. Based on the final dimension ratings and Appendix C scoring bands, the Equifax submissions comprised 3 Strong, 3 Developing, and 3 Limited overall; the Target submissions had the same distribution. For Equifax, 2 of nine were Strong on stacked risk analysis and 4 of nine on materiality and prioritization. For Target, 4 of nine were Strong on network segmentation and 2 of nine on actionable recommendations. These descriptive counts make the findings auditable while avoiding claims that the small sample represents a broader student population or supports statistical inference. Formal inter-rater reliability was not calculated; Section 5.3 describes designs that would support it. Across both artifacts, stronger responses integrated facts with cybersecurity concepts, accountability, and consequences; developing responses made less-complete connections; and limited responses named isolated factors or generic controls.

Two case-specific patterns were visible. Stronger Equifax responses framed the breach as stacked risk involving high-materiality data, proposed plausible risk-register entries, assigned ownership, and discussed treatment priorities. Less-developed responses identified Apache Struts or sensitive-data exposure without fully explaining ownership, lifecycle stage, escalation, or prioritization. Stronger Target responses integrated third-party access, segmentation, detection failures, blast radius, and controls into an explanation of incident impact; less-developed responses did not explain how access architecture shaped detection and containment. These patterns align with the objectives and Appendix C rubrics. Because the assignments used different prompts and case-specific rubrics, the distributions should not be interpreted as a direct comparison of Equifax and Target performance.

The prospective Ring exercise in Appendix D applies the same logic to connected-device risk. Students analyze how an attack could unfold during device setup, how exposed credentials could turn a device flaw into home-network risk, and which countermeasures could reduce likelihood, blast radius, or customer harm (Bitdefender, 2019; FTC, 2023; Meeuwisse, 2017). It offers no student-work evidence yet but shows how the Table 3 Ring row could become an assessable task.

5.3 Limitations and Future Development

This paper has three limitations. First, the framework is curated, not comprehensive. Its cases illustrate recurring principles but neither exhaust relevant incidents nor constitute a formal taxonomy. Developed and demonstrated in one upper-level undergraduate course, it is an instructor-designed teaching artifact rather than a validated educational framework. Its usability across other instructors, institutions, and contexts remains unevaluated. Whether case substitutions preserve the intended relationship among takeaway, case, and objective also requires study. This remains a question for subsequent empirical evaluation.

Second, the student-work evidence is preliminary. The artifacts show post-instruction application aligned with two framework rows, not proof that the framework independently improved learning or that students can transfer a takeaway and objective to an unfamiliar incident.

Third, evidence is uneven across the exemplars: Target and Equifax have student work, while Ring lacks comparable assessment. Future development should apply the rubrics prospectively, implement the Ring exercise, and evaluate the artifact across instructors, institutions, and contexts, including

whether substituted cases preserve the intended cluster–takeaway–case–objective relationship. Testing across settings would examine whether other instructors interpret the objectives consistently and can replace cases without changing the analytical performance the framework is designed to elicit.

A more rigorous evaluation would assess integrated reasoning and cross-case transfer. A pre/post design could use different but matched case-analysis prompts aligned with the same takeaway and objective: Students analyze one incident before the framework activity and another unfamiliar incident afterward. A cross-offering comparison could give the same unfamiliar transfer case to comparable sections or successive terms, one using the framework and one not, and apply a common rubric aligned with the unchanged objective. Because the incident changes while the principle and expected performance remain stable, either design could distinguish transfer from recall. Both would also permit formal inter-rater reliability to be calculated and reported based on the authors' initial independent ratings before consensus.

5.4 Conclusion

Cybersecurity education must help students do more than recognize breaches or repeat abstract principles. Students need practice connecting durable concepts to incidents, changing technologies, and organizational consequences. This framework addresses that need through fifteen case-linked takeaways in three clusters: risk visibility and business alignment, incident response and cyber resilience lifecycle, and modern and future-facing cyber exposure.

The contribution is this instructional artifact, not the established practice of using breach cases. Its tables translate principles into assessable objectives for discussions, team activities, exams, and written analysis; the three exemplars demonstrate application across material data exposure, third-party access, and connected-device ecosystems. Instructors can retain these cases or substitute newer ones while preserving the cluster–takeaway–case–objective relationship. The post-instruction student-work evidence shows that objectives can become assessable tasks but does not establish improved learning. This bounded claim preserves the artifact's practical teaching contribution while distinguishing current evidence from future validation. More systematic evaluation should follow the designs outlined above.

6. REFERENCES

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams—Challenges in supporting the organisational security function. *Computers & Security, 31*(5), 643–652. https://doi.org/10.1016/j.cose.2012.04.001

Ahmad, A., Maynard, S. B., Motahhir, S., & Anderson, A. (2021). Case-based learning in the management practice of information security: An innovative pedagogical instrument. *Personal and Ubiquitous Computing*, 25, 853–877.

American Hospital Association. (2024, March 15). *AHA survey: Change Healthcare cyberattack significantly disrupts patient care, hospitals' finances.* https://www.aha.org/news/headline/2024-03-15-aha-survey-change-healthcare-cyberattack-significantly-disrupts-patient-care-hospitals-finances

Anderson, A., Ahmad, A., & Chang, S. (2024). Case-based learning for cybersecurity leaders: A systematic review and research agenda. *Information & Management*, 61(7), Article 104015.

Bitdefender. (2019, November 6). *Ring Video Doorbell Pro under the scope* [White paper]. https://www.bitdefender.com/files/News/CaseStudies/study/294/Bitdefender-WhitePaper-RDoor-CREA3949-en-EN-GenericUse.pdf

Blount, J. A., Jr. (2021, June 8). *Threats to critical infrastructure: Examining the Colonial Pipeline cyber attack* [Testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs]. https://www.hsgac.senate.gov/hearings/threats-to-critical-infrastructure-examining-the-colonial-pipeline-cyber-attack/

Cai, Y., & Arney, T. (2017). Cybersecurity should be taught top-down and case-driven. In *Proceedings of the 18th Annual Conference on Information Technology Education* (pp. 103–108). Association for Computing Machinery. https://doi.org/10.1145/3125659.3125687

Capital One. (2021, April 16). *2019 Capital One cyber incident.* https://www.capitalone.com/digital/facts2019/

Cybersecurity and Infrastructure Security Agency. (2020, December 13). *Active exploitation of SolarWinds software.* https://www.cisa.gov/news-events/alerts/2020/12/13/active-exploitation-solarwinds-software

Cybersecurity and Infrastructure Security Agency. (2021, July 19). *Mitigate Microsoft Exchange Server vulnerabilities (AA21-062A).* https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-062a

Cybersecurity and Infrastructure Security Agency. (2025, July 29). *#StopRansomware: Scattered Spider (AA23-320A).* https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

Federal Trade Commission. (2023, May 31). *FTC says Ring employees illegally surveilled customers, failed to stop hackers from taking control of users' cameras.* https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users

Federal Trade Commission. (2024). *Complaint: In the matter of Marriott International, Inc., and Starwood Hotels & Resorts Worldwide, LLC.* https://www.ftc.gov/legal-library/browse/cases-proceedings/1923022-marriott-international-inc-starwood-hotels-resorts-worldwide-llc

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness—A systematic review of the literature. *Computers & Security, 46,* 18–31. https://doi.org/10.1016/j.cose.2014.06.008

Harrell, M. N. (2017). Synergistic security: A work system case study of the Target breach. *Journal of Cybersecurity Education, Research and Practice, 2017*(2), Article 4. https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss2/4

Herreid, C. F. (1994). Case studies in science—A novel method of science education. *Journal of College Science Teaching, 23*(4), 221–229.

Joint Task Force on Cybersecurity Education. (2017). *Cybersecurity Curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity* (Version 1.0). ACM, IEEE-CS, AIS SIGSEC, & IFIP WG 11.8. https://doi.org/10.1145/3184594

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In A. Kott & I. Linkov (Eds.), *Cyber resilience of systems and networks* (pp. 1–25). Springer. https://doi.org/10.1007/978-3-319-77492-3_1

Luburić, N., Sladić, G., Slivka, J., & Milosavljević, B. (2019). A framework for teaching security design analysis using case studies and the hybrid flipped classroom. *ACM Transactions on Computing Education, 19*(3), Article 21. https://doi.org/10.1145/3289238

Meeuwisse, R. (2017). *Cybersecurity for beginners* (2nd ed.). Cyber Simplicity.

Microsoft. (2018, February 5). Overview of Petya, a rapid cyberattack. *Microsoft Security Blog*. https://www.microsoft.com/en-us/security/blog/2018/02/05/overview-of-petya-a-rapid-cyberattack/

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119.

Office of the Privacy Commissioner of Canada, & U.K. Information Commissioner's Office. (2025, June 20). *Joint investigation into a data breach at 23andMe by the Privacy Commissioner of Canada and*

the UK Information Commissioner (PIPEDA Findings #2025-001). https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST SP 800-61 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020). *Workforce framework for cybersecurity (NICE Framework)* (NIST SP 800-181 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181r1

Philippou, E., Frey, S., & Rashid, A. (2020). Contextualising and aligning security metrics and business objectives: A GQM-based methodology. *Computers & Security, 88,* Article 101634. https://doi.org/10.1016/j.cose.2019.101634

Plachkinova, M., & Maurer, C. (2018). Security breach at Target [Teaching case]. *Journal of Information Systems Education, 29*(1), 11–20. https://jise.org/Volume29/n1/JISEv29n1p11.html

Prince, M. (2004). Does active learning work? A review of the research. *Journal of Engineering Education, 93*(3), 223–231. https://doi.org/10.1002/j.2168-9830.2004.tb00809.x

Quinn, S., Chua, J., Ivy, N., Gardner, R., Scarfone, K., Smith, M., & Witte, G. (2025, December). *Integrating cybersecurity and enterprise risk management (ERM)* (NIST IR 8286 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8286r1

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (NIST SP 800-160 Vol. 2 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1

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

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76,* 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

U.S. Attorney's Office, Northern District of Georgia. (2018, December 5). *Atlanta U.S. Attorney charges Iranian nationals for City of Atlanta ransomware attack.* https://www.justice.gov/usao-ndga/pr/atlanta-us-attorney-charges-iranian-nationals-city-atlanta-ransomware-attack

U.S. Department of Health and Human Services, Office for Civil Rights. (2018, October 15). *Anthem pays OCR $16 million in record HIPAA settlement following largest health data breach in history.* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/anthem/index.html

U.S. Government Accountability Office. (2017). *Information security: OPM has improved controls, but further efforts are needed* (GAO-17-614). https://www.gao.gov/products/gao-17-614

U.S. House Committee on Oversight and Government Reform. (2018). *The Equifax data breach* (Majority staff report). https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf

U.S. Senate Committee on Commerce, Science, and Transportation. (2014). *A "kill chain" analysis of the 2013 Target data breach.* https://www.commerce.senate.gov/2014/3/rockefeller-staff-report-details-target-s-missed-opportunities-to-stop-massive-data-breach

APPENDIX A

In-Class Exercise Based on the Equifax (2017) Data Breach

CS 342 (Cybersecurity)
Bentley University
Section 1
Prof. David Yates

In-Class Exercise (90–120 minutes).

Review and background. Review two things already covered in class: (1) the Chapter 12 material from Meeuwisse (2017), including the slides, and (2) a reputable summary of the Equifax breach. Then watch the assigned short case video.

Academic-integrity note. This in-class exercise is open-book, but your submission must be written in your own words. Do not use generative-AI tools to develop or write your answers, and do not copy from AI-tool outputs or any other online source.

Instructions. Answer the following two questions, which draw on Chapter 12 of your textbook (*Risk-Based Cybersecurity and Stacked Risk*). Strong answers use concepts from this chapter to interpret the antecedents and implications of the Equifax breach. Be explicit as you apply chapter concepts to causation, prioritizing the strongest case-supported concepts.

1. [16 points] Stacked risk, materiality, and why Equifax was a high-priority target. Using the concepts and vocabulary from Chapter 12 in Meeuwisse, explain how the Equifax breach reflects stacked risk rather than a single isolated failure. Identify the three most important risks that had accumulated around Equifax's high-value systems and data, and explain why those risks should have been treated as especially urgent in terms of probability, impact, proximity, and materiality. Be explicit about why Equifax's data holdings made this a strong example of risk-based cybersecurity management rather than "protect everything equally."

2. [24 points] Risk register, risk assessment, and treatment priorities. Imagine you were brought into Equifax shortly before the breach was discovered and asked to improve risk management using Chapter 12's methods. Identify the three most important entries that should have appeared in a shared risk register, and for each specify the likely risk owner, the relevant lifecycle stage, and the best treatment option (for example, prevention, reduction, acceptance, contingency, or transfer). Then explain what kind of risk assessment should have been performed on the affected systems and data flows, and how that assessment might have changed priorities before the breach became material.

APPENDIX B

Final-Exam Question Assessing Knowledge of the Target (2013) Data Breach

CS 342 (Cybersecurity)
Bentley University
Section 1
Prof. David Yates

This item is drawn from the course final exam. The exam was open-book and open-notes; students completed it individually, and the use of generative-AI tools was prohibited. Only the Target question is reproduced here; the exam's other questions are omitted because they are unrelated to this paper's argument.

[140 points] Target (2013) data breach. Meeuwisse (2017, pp. 27–30) summarizes how the 2013 Target breach exploited a third-party HVAC vendor's credentials and led to massive data exfiltration.

(i) Using Chapters 3 and 12 through 16 in your main textbook, briefly describe how third-party access and lack of network segmentation contributed to this Target breach.
(ii) Briefly describe one obvious failure within each of the following NIST CSF 2.0 functions: Identify, Protect, and Detect.
(iii) Propose three specific and actionable recommendations that might have prevented this breach.
(iv) Explain how the measures from part (iii) could have minimized the blast radius and shortened security-incident detection time.

Hint. The best answers can be derived from your assigned course materials.

APPENDIX C

The rubrics in this appendix were applied post hoc to analyze levels of integrated cybersecurity reasoning in student responses to the Equifax exercise (Appendix A) and Target final-exam question (Appendix B), respectively. They were not the original grading rubrics used in the course.

Post Hoc Coding Rubric for the Equifax (2017) Case: Stacked Risk, Materiality, and Risk Ownership

The rubric below operationalizes the Table 1 Equifax learning objective: *"Students will be able to evaluate how risk ownership, escalation authority, and treatment priorities shape whether known risks are managed before they become material failures."* Six dimensions correspond to the elements of the in-class exercise in Appendix A and to the Equifax case framing used in the paper (Meeuwisse, 2017; U.S. House Committee on Oversight and Government Reform, 2018). Each dimension is scored on a three-level scale. This rubric is offered as a starting point and is intended to be adapted to the course textbook and prior course coverage.

Dimension	Strong (3)	Developing (2)	Limited (1)
Stacked risk analysis	Explains the breach as stacked risk, showing how a handful of risks (e.g., an unpatched Apache Struts vulnerability, no comprehensive IT asset inventory, lack of segmentation, expired certificates and limited monitoring, and concentrated high-value data) accumulated around the same high-value systems rather than a single isolated failure. Note: Appendix A constrains the number of risks to three.	Identifies more than one contributing risk but treats them as separate problems, without showing how they compounded around the same high-value systems and data. Note: Appendix A constrains the number of contributing risks to three.	Names a single cause (e.g., "the Apache Struts flaw") and treats the breach as an isolated technical failure rather than accumulated, stacked risk.
Materiality and prioritization	Uses probability, impact, proximity, and materiality to explain why Equifax's data holdings made these risks especially urgent, and argues explicitly for risk-based prioritization rather than "protect everything equally."	References some prioritization concepts (e.g., impact or materiality) but applies them loosely, without connecting them to why these specific risks warranted urgent, prioritized treatment.	Does not use prioritization concepts, or asserts that the data was sensitive without explaining materiality, probability, impact, or proximity.
Risk-register entries	Identifies specific, plausible risk-register entries for the most important accumulated risks, each phrased as a concrete risk rather than a generic control or a restatement of the incident. Note: Appendix A constrains the number of entries to three.	Proposes register entries that are partially formed: vague, overlapping, or phrased as controls or events rather than as risks with a clear source and consequence. Note: Appendix A constrains the number of entries to three.	Provides no register entries, or lists undifferentiated "problems" that could not be tracked or owned in a shared risk register.
Risk ownership, accountability, and escalation	Assigns a plausible risk owner to each entry and explains who should have been accountable for recognizing, treating, and, where appropriate, escalating the known	Assigns ownership in general terms (e.g., "IT" or "management") without clarifying accountability or how	Does not address ownership or escalation, or treats the breach as no one's specific

Dimension	Strong (3)	Developing (2)	Limited (1)
	risk before it became a material failure (e.g., unclear security reporting structure and ambiguous patch-management ownership).	escalation would have functioned.	responsibility.
Lifecycle stage and treatment options	Locates each risk in a relevant lifecycle stage and selects an appropriate treatment option (e.g., prevention, reduction, acceptance, contingency, or transfer), justifying the choice for that specific risk.	Names treatment options or lifecycle stages but applies them inconsistently, or selects a treatment without justifying why it fits the risk.	Does not reference treatment options or lifecycle stages, or applies them only as labels without connecting them to specific risks.
Risk-assessment logic	Describes the kind of risk assessment that should have been performed on the affected systems and data flows, and explains how that assessment could have changed priorities before the breach became material.	Mentions that a risk assessment should have occurred but does not specify what it would examine or how it would have shifted pre-breach priorities.	Does not address risk assessment, or treats it only as a compliance step disconnected from prioritization and the breach outcome.

Scoring. Sum dimension scores (range 6–18). Suggested bands: 15–18 Strong overall, 11–14 Developing, 6–10 Limited. Instructors should expect to adapt level descriptors to local course textbook coverage and to the specific phrasing of the assignment prompt.

Post Hoc Coding Rubric for the Target (2013) Case: Third-Party Access, Segmentation, and Incident Impact

The rubric below operationalizes the Table 2 Target learning objective: *"Students will be able to explain how third-party credentials, weak network segmentation, and Identify/Protect/Detect failures can expand blast radius and delay detection."* Six dimensions correspond to the elements of the exam prompt in Appendix B and to the Target case framing used in the paper (NIST, 2024; U.S. Senate Committee on Commerce, Science, and Transportation, 2014). Each dimension is scored on a three-level scale. Again, this rubric is offered as a starting point and is intended to be adapted to the course textbook and prior course coverage.

Dimension	Strong (3)	Developing (2)	Limited (1)
Third-party access analysis	Identifies HVAC vendor credentials as the entry vector and analyzes the underlying issues: vendor identity management, least privilege, vendor oversight, and access review.	Identifies the vendor-credential entry vector but does not extend the analysis to identity management, least privilege, or vendor oversight.	Identifies that a vendor was compromised or that credentials were stolen, without locating the issue in vendor access architecture.
Network segmentation	Explains how weak segmentation allowed lateral movement from the vendor-access environment toward payment systems, and connects segmentation to containment.	Mentions segmentation weakness but does not connect it to lateral movement or containment.	Does not identify segmentation as a contributing factor, or treats it only as a generic "network security" issue.
Identify / Protect / Detect failures	Maps specific failures to Identify (asset and vendor inventory), Protect (access controls, segmentation),	Names one or two CSF functions but does not map specific failures consistently across Identify, Protect, and	Does not reference the CSF functions, or applies them only as labels without

Dimension	Strong (3)	Developing (2)	Limited (1)
	and Detect (alert triage, escalation), referencing NIST CSF 2.0 functions.	Detect.	identifying specific failures.
Actionable recommenda-tions	Recommends specific, named controls (e.g., a vendor risk-management program, network microsegmentation, monitoring and alert-escalation procedures) and links each to a specific failure. Note: Appendix B asks for three recommendations.	Recommends general controls (e.g., "better monitoring," "stronger segmentation") without naming specific mechanisms or linking to specific failures. Note: coverage may include fewer than three, vague, or unlinked recommendations.	Provides generic or non-actionable recommendations (e.g., "Target should improve security").
Blast-radius reduction	Explains how each recommended control would reduce blast radius by limiting lateral movement, narrowing scope of compromise, and reducing affected systems or records.	Notes that controls would "reduce impact" without analyzing the specific mechanism (lateral movement, scope of compromise).	Does not address blast radius, or conflates it with severity in general.
Detection time	Explains how each recommended control would shorten detection time through earlier alerting, faster triage, or reduced attacker dwell time.	Notes that controls would "catch attackers faster" without analyzing alerting, triage, or dwell time.	Does not address detection time, or treats detection only as binary (detected / not detected).

Scoring. Sum dimension scores (range 6–18). Suggested bands: 15–18 Strong overall, 11–14 Developing, 6–10 Limited. Instructors should expect to adapt level descriptors to local course textbook coverage and to the specific phrasing of the assignment prompt.

APPENDIX D

In-Class Exercise Based on the Ring (2019) Security Vulnerability

CS 342 (Cybersecurity)
Bentley University
Section 1
Prof. David Yates

Before class, read the Bitdefender white paper on the Ring Video Doorbell Pro Wi-Fi credential-exposure vulnerability (Bitdefender, 2019). Imagine you have been hired as a cybersecurity consultant after public disclosure of the vulnerability. Working from your team's assigned perspective, analyze (i) how the attack could unfold during device setup or reconfiguration (Team 1) and (ii) what defenses would have reduced the incident's likelihood and/or limited its impact (Teams 2–4). Connect your analysis to course material on attack surfaces and technical cybersecurity.

Logistics. Teams are assigned in class, with approximately 15 minutes to work. Choose a spokesperson and a note-taker. Keep the discussion conceptual, and state any important assumptions.

Report-out. Follow the output format in your team prompt. Aim for clarity over completeness, prioritize what matters most, explain your reasoning, and assume today's best practices. Target three to four minutes per team.

Team 1: Attack method (how the exploit could work). Based on the facts in the Bitdefender white paper, produce a five-to-seven-step attacker sequence from device disruption to possible household-network compromise. The paper describes a nearby attacker who makes the device appear offline, triggers reconfiguration, observes an open setup access point, and captures Wi-Fi credentials sent over an insecure local channel. Also include (a) what the attacker learns or gains at each step, (b) which step changes the problem from a "doorbell vulnerability" into a "home-network risk," and (c) where the user, vendor, app, router, or device might have detected or disrupted the activity earlier. Report-out: your sequence and the single most important breaking point (one control or design decision) that would have stopped the chain, with a one-to-two-sentence rationale. Identify which Meeuwisse (2017) defense points are involved: data, device, application, network, system, and/or communication channel.

Team 2: Defensive measure 1 (secure setup and prevent credential exposure). Identify your top three ranked design or control gaps that could allow device setup to expose a household Wi-Fi password. Focus on encrypted provisioning, authenticated setup mode, avoiding plaintext credential transfer, secure defaults, app warnings, forced updates, and minimizing what sensitive information the device ever receives or stores. Report-out: your top three ranked preventive actions and how each would have reduced the likelihood of exploitation.

Team 3: Defensive measure 2 (limit blast radius and detect/contain). Assume the Wi-Fi password has been exposed and, absent additional protections, a nearby attacker may connect to the residential network. Identify your top three ranked gaps that allow Wi-Fi access to become broader compromise. Emphasize guest or IoT network segmentation, router/firewall rules, least privilege, disabling unnecessary local services, router/device logging, anomaly alerts, and quick credential rotation. Report-out: your top three ranked actions that would shrink blast radius and shorten time-to-detect/contain, mapping each to where it breaks the attacker sequence.

Team 4: Defensive measure 3 (vendor response and customer-harm reduction). This case shows how a consumer IoT vulnerability can move from a device-design flaw to a home-network risk when Wi-Fi credentials are exposed. Assume Bitdefender has privately reported the vulnerability and Ring must reduce customer harm before and after public disclosure. Identify your top three ranked response actions: (1) a vendor patch/update action, (2) an app/customer-guidance action, and (3) a post-exposure customer-recovery action. For each, explain who owns it, when it should happen, what harm it reduces, and which Meeuwisse defense point it addresses. Consider coordinated vulnerability disclosure, secure update deployment, app warnings during reconfiguration, customer notification, secure setup instructions, Wi-Fi password rotation, rejoining devices, and isolating IoT devices on a

guest or segmented network. Report-out: your top three response actions and how each reduces customer harm even if credentials were exposed.