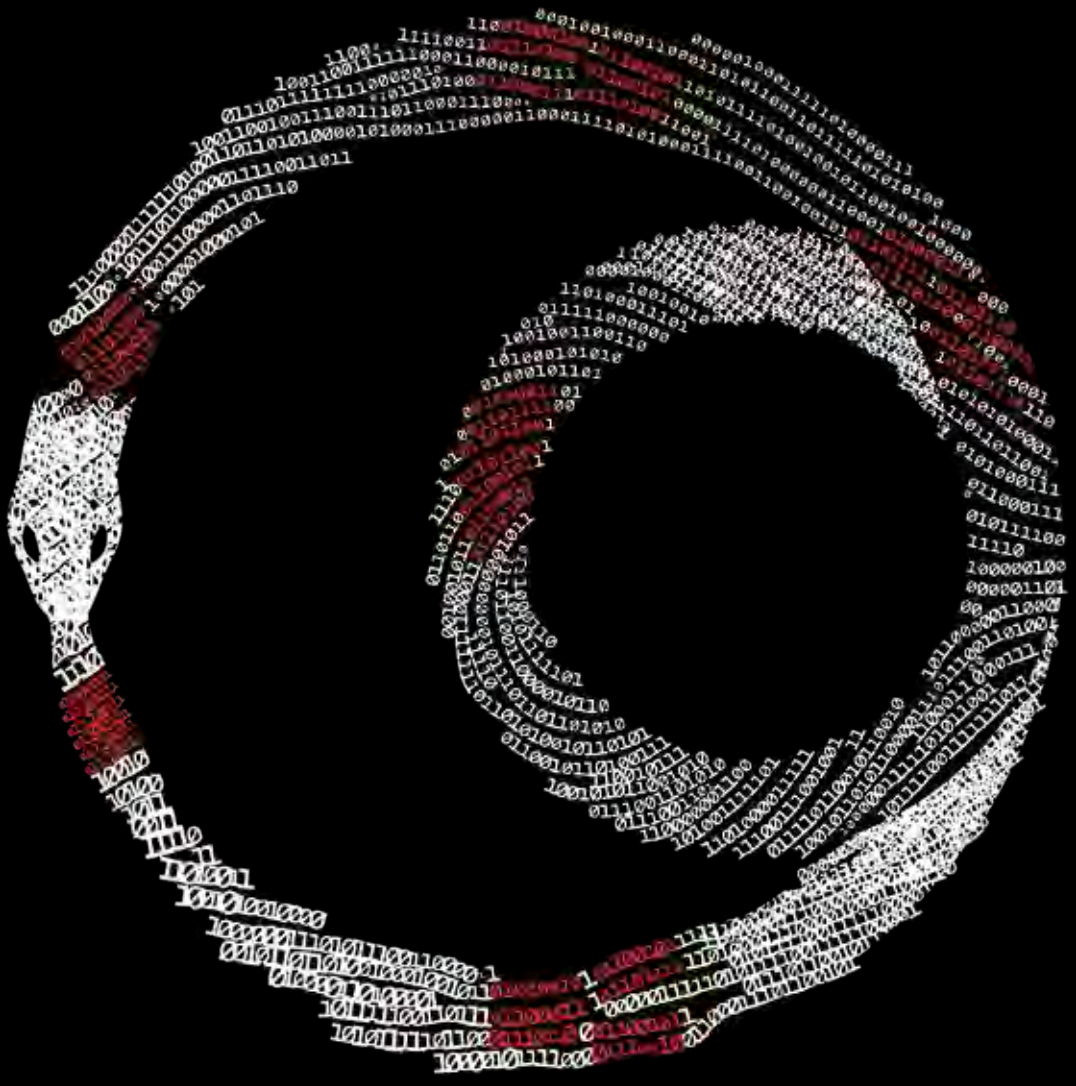
Executive Summary

Incident Preparedness and Response Report

Taming the data ~~beast~~ breach.



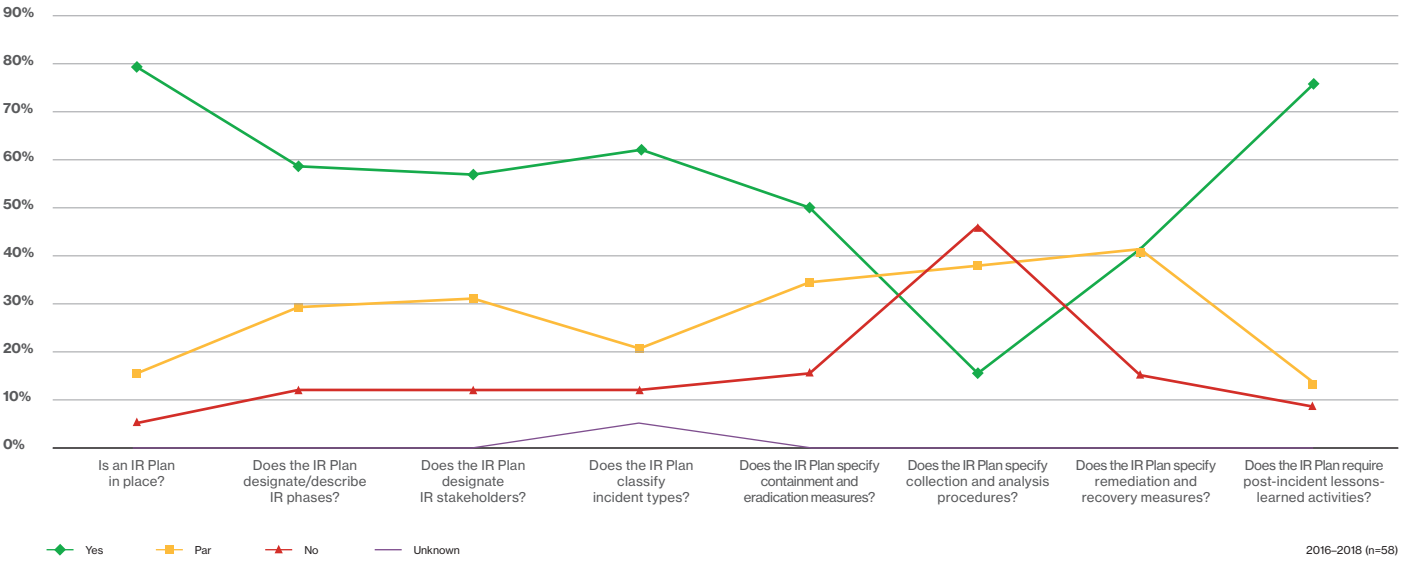
verizon business ready

The situation room

Preparing for and responding to data breaches and cybersecurity incidents is never easy. It takes knowledge of your environment and its unique threats, effective teamwork and, just as importantly, an Incident Response (IR) Plan.

That's the ultimate reason for our Verizon Incident Preparedness and Response (VIPR) Report. A data- and scenario-driven approach to incident preparedness and response, it's based on three years (2016–2018) of our IR Plan assessments and our data breach simulation recommendations.

Plan assessments
Phases 1–6 – Select IR Plan elements



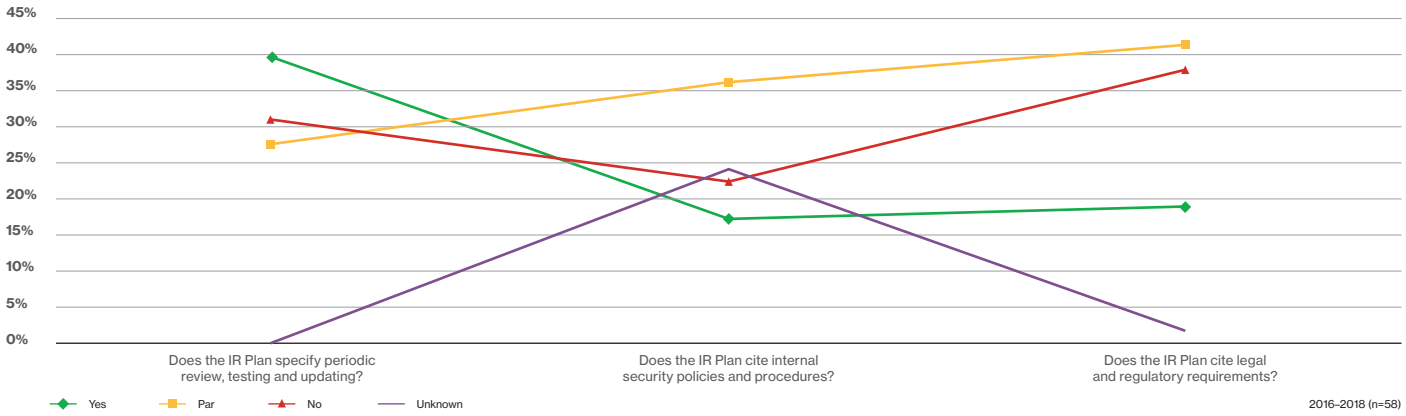
This "Taming the Data Beast" edition puts you in the shoes of various IR stakeholders so you can learn how to formulate or improve your own cybersecurity incident mitigation and response efforts.

Placed throughout the report are five data breach scenarios (see Using the Breach Simulation Kits) illustrating the need for a particular phase of an IR Plan and its underlying components. You can use this layout as a framework to create or update your own IR Plan and its associated IR playbooks. You can also use the scenarios to build out content to facilitate data breach simulation workshops and tabletop exercises.

Planning and preparation

Planning and preparing for cybersecurity incidents is crucial for an effective response. This phase covers construction of the IR Plan, including internal IR stakeholders, tactical responders, and third parties, such as service providers, regulators, and outside counsel.

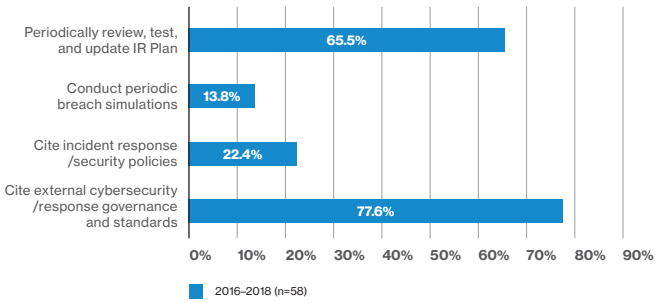
Plan assessments
Phase 1 – Plan relevancy



Assessment observations

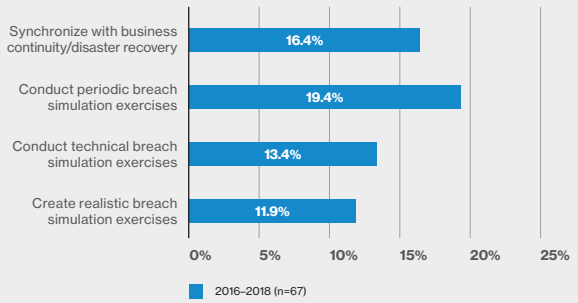
For assessed IR Plans (2016–2018), only 40% explicitly specified periodical reviewing, testing and updating IR Plans, while 31% did not. Of assessed IR Plans, 22% cited no internal security policies or procedures (30% partially did so), and 38% cited no legal or regulatory requirements (41% partially did so) for cybersecurity, incident response or data breach notification.

Assessment recommendations



Citing external governance and standards such as GLBA, ISO 27001, etc., (78%) and periodically reviewing, testing and updating the IR Plan (66%) were the top recommendations.

Simulation recommendations



For simulation recommendations (2016–2018), conducting breach simulations (20%) and conducting technical breach simulations (13%) were the top recommendations.

Detection and validation

An effective response involves detecting and classifying cybersecurity incidents early in the IR process.

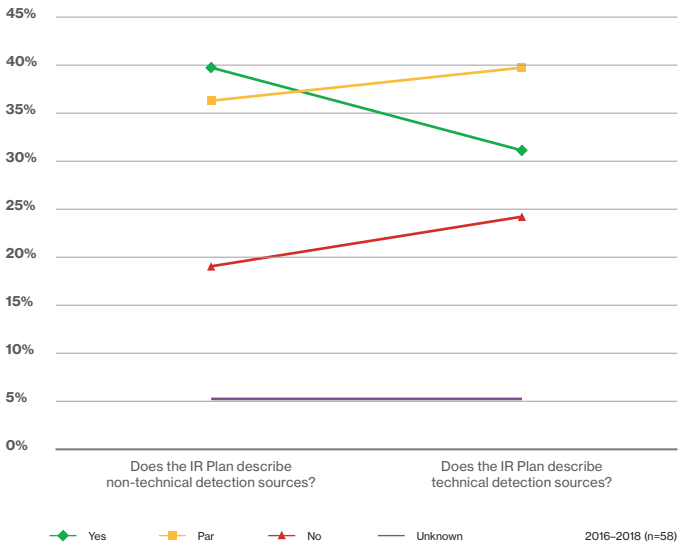
Assessment observations

For incident detection sources (2016–2018) within assessed IR Plans, 40% fully described (another 36% partially described) non-technical detection sources, while only 31% fully described (another 40% partially described) technical detection sources.

Assessment recommendations

Describe technical and non-technical incident detection sources.

Plan assessments
Phase 2 – Detection sources



Containment and eradication

This stage focuses on containing cybersecurity threats to minimize damage and eradicating threats to prevent additional damage.

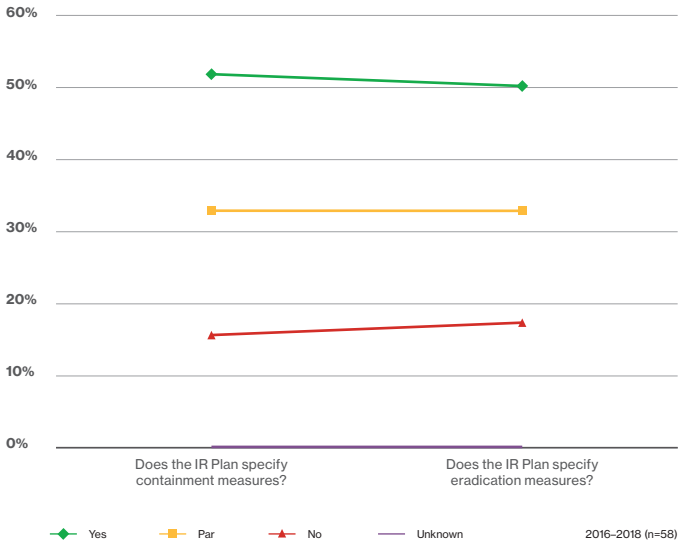
Assessment observations

Of assessed IR Plans (2016–2018) for containing and eradicating, 52% fully specified containment measures and 50% specified eradication measures. Another 33% partially specified containment measures and another 33% partially specified eradication measures.

Assessment recommendations

Provide containment and eradication measures.

Plan assessments
Phase 3 – Containing and eradicating



Collection and analysis

Collecting and analyzing evidence can shed further light on cybersecurity incidents, leading to effective containment, eradication, remediation and recovery.

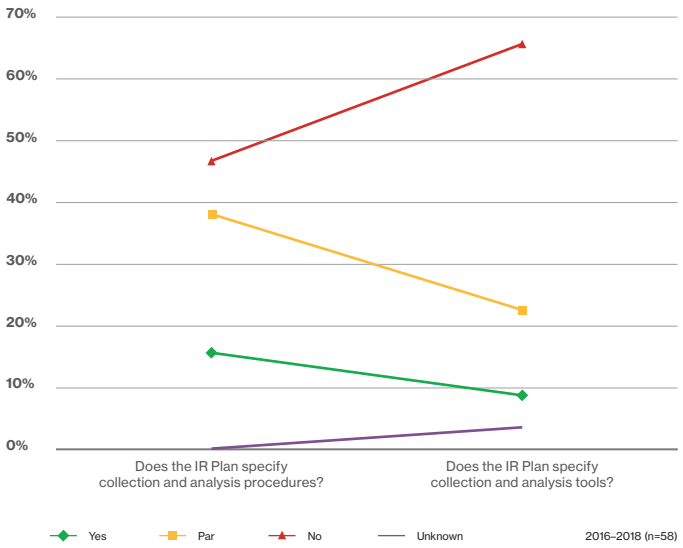
Assessment observations

For collecting evidence and analyzing data, of assessed IR Plans (2016–2018) – only 16% fully specified, with 38% partially specifying collection and analysis procedures. For tools, only 9% fully specified, with 22% partially specifying collection and analysis tools.

Assessment recommendations

Specify evidence collection and data analysis tools and procedures.

Plan assessments
Phase 4 – Collecting and analyzing



Remediation and recovery

This stage has two objectives: remediate vulnerabilities exposed during the incident to prevent or mitigate future issues, and recover by restoring operations to normal.

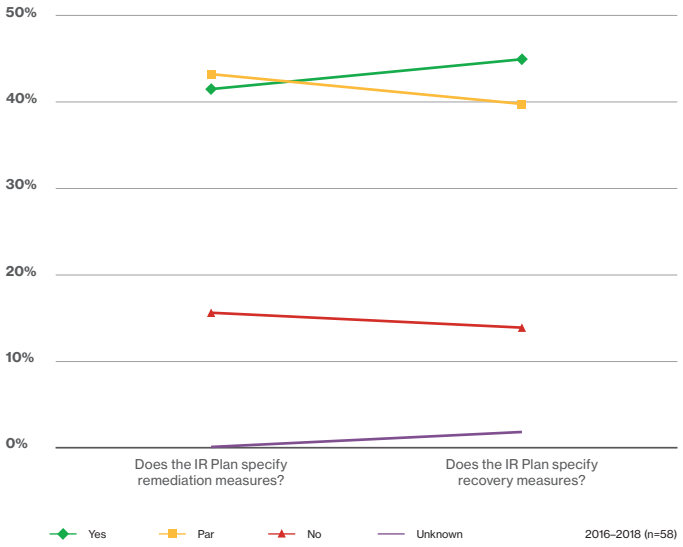
Assessment observations

Of assessed IR Plans (2016–2018) for remediating and recovering, only 41% fully specified remediation measures (with 43% partially specifying) and 45% fully specified recovery measures (with 40% partially specifying).

Assessment recommendations

Provide remediation and recovery measures.

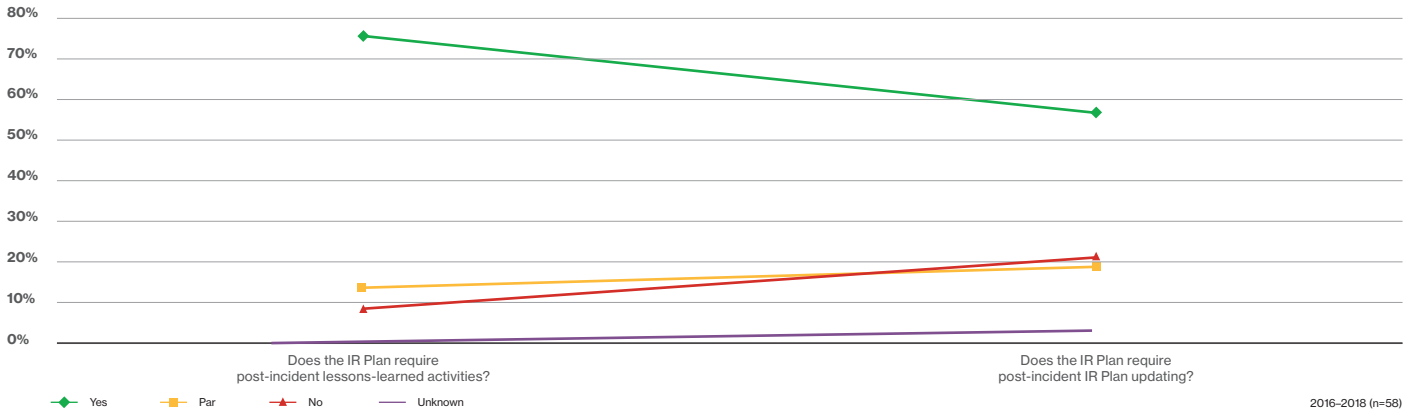
Plan assessments
Phase 5 – Remediating and recovering



Assessment and adjustment

The final stage of the IR process is reviewing IR activities to identify systemic weaknesses and deficiencies, and improve cybersecurity controls and practices.

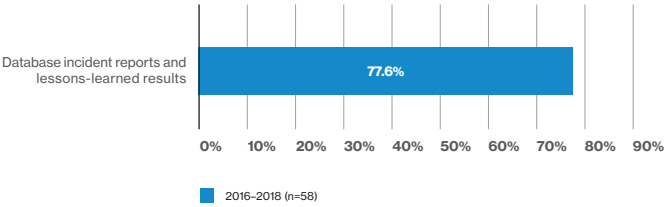
Plan assessments
Phase 6 – Lessons learned



Assessment observations

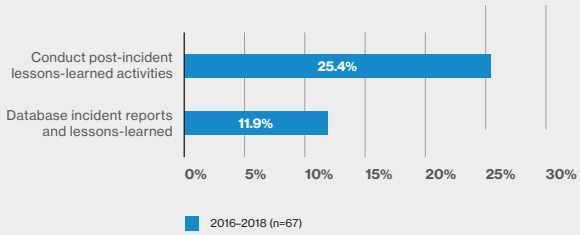
Of assessed IR Plans (2016–2018), 76% fully required (14% partially) post-incident lessons-learned activities and 60% fully required (19% partially) post-incident IR Plan updating (based on lessons-learned activity).

Assessment recommendations



For lessons learned, assessment recommendations included databasing the post-incident lessons learned (78%).

Simulation recommendations



For breach simulations (2016–2018), conducting post-incident lessons learned activities (25%) was most recommended, followed by databasing incident reports and lessons learned (12%).

Takeaways

We hope you'll take the time to read the entire 2019 VIPR Report, which is full of insights, data and IR Plan best practices. Nevertheless, to summarize crucial points, here are our top 20 takeaways for building an effective breach response capability and solid IR Plan.

Phase	Key Takeaway
1 – Planning and Preparation	1. Construct a logical, efficient IR Plan 2. Create IR playbooks for specific incidents 3. Periodically review, test and update the IR Plan 4. Cite external and internal cybersecurity and incident response governance and standards 5. Define internal IR stakeholder roles and responsibilities 6. Require internal IR stakeholders to periodically discuss the cybersecurity threat landscape 7. Train and maintain skilled tactical responders 8. Periodically review third-party cybersecurity services and contact procedures
2 – Detection and Validation	9. Define cybersecurity events (along with incidents) 10. Classify incidents by type and severity level 11. Describe technical and non-technical incident detection sources 12. Specify incident and event tracking mechanisms 13. Specify escalation and notification procedures
3 – Containment and Eradication	14. Provide containment and eradication measures
4 – Collection and Analysis	15. Specify evidence collection and data analysis tools and procedures 16. Specify evidence handling and submission procedures
5 – Remediation and Recovery	17. Provide remediation and recovery measures
6 – Assessment and Adjustment	18. Conduct post-incident lessons-learned activities (feed results back into the IR Plan) 19. Establish data and document retention policy 20. Track incident and incident response metrics

Data breach and cybersecurity resources

https://enterprise.verizon.com/resources/

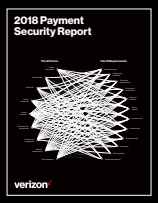
2019 Incident Preparedness and Response Report: Taming the data ~~beast~~ breach.

2019 Data Breach Investigations Report

2019 Insider Threat Report: Out of sight should never be out of mind.

2019 Mobile Security Index: It's time to tackle mobile security.

2018 Data Breach Digest (18 scenarios)



2018 Payment Security Report

2019 CISO's Guide to Cloud Security: What to know and what to ask before you buy.

5 Considerations for Evaluating a Modern Enterprise Security Platform

Download the Verizon Incident Preparedness and Response report

enterprise.verizon.com/resources/reports/vipr/

verizon business ready