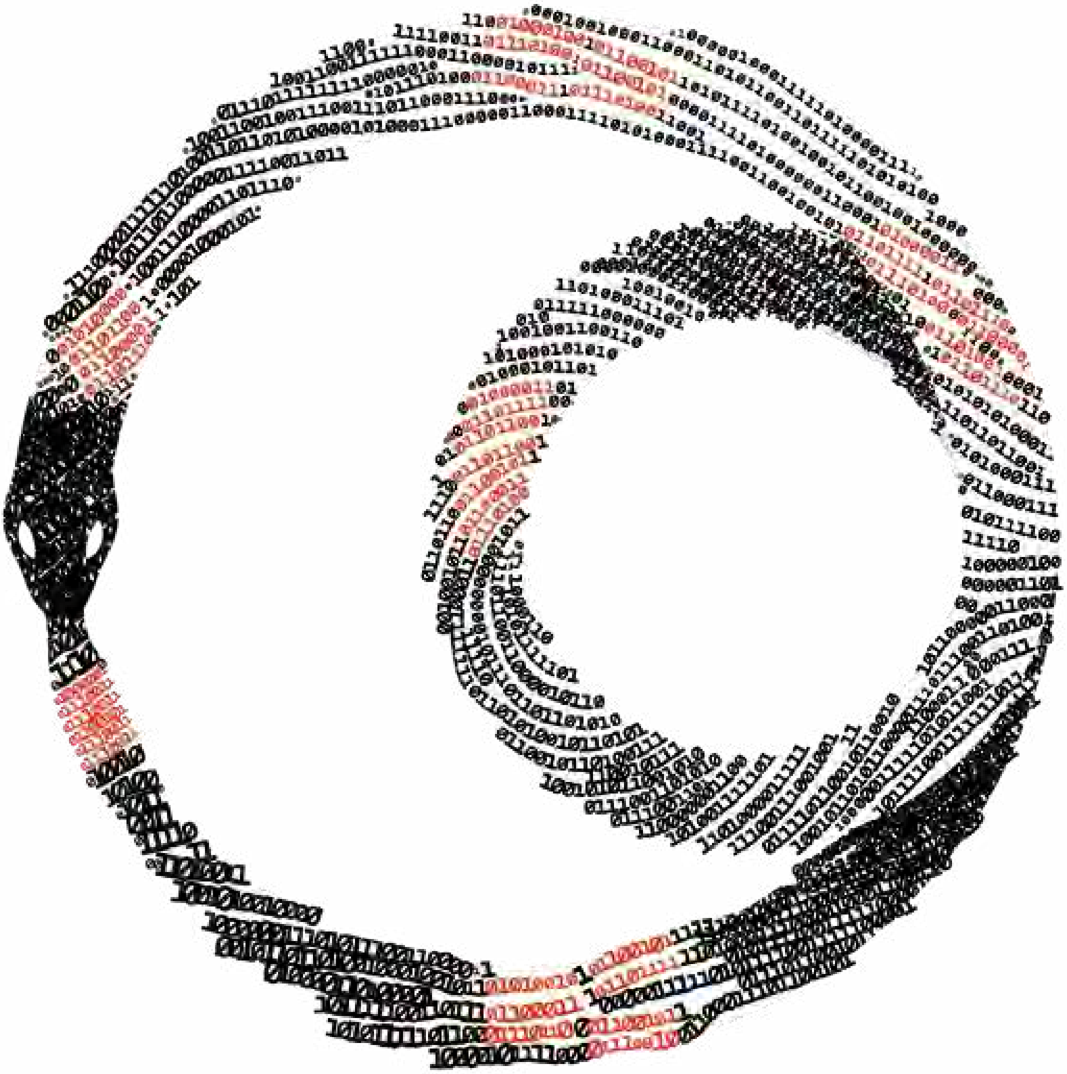
Incident Preparedness and Response Report

Taming the data ~~beast~~ breach.



verizon business ready

A publication written by practitioners for practitioners.

Table of contents

About the cover

The ouroboros (/ˌjʊərəˈbɒrəs/;[2] οὐροβόρος (< οὐρά, tail, and -βορος, devouring) is an ancient symbol depicting a serpent or dragon eating its own tail. [The ouroboros is] often taken to symbolize introspection, the eternal return or cyclicality, especially in the sense of something constantly re-creating itself. It also represents the infinite cycle of nature's endless creation and destruction, life and death.[1]

We've created a twisted ouroboros, or viper, on the cover of our VIPR Report to symbolize the incident response process. It implies that incident response for a single incident is not only a multi-phase, iterative process, but it is also one that coils back in on itself during the incident. Thus, indicating the results and findings of some phases can feed back into a previous phase or phases. For example, the Collection and analysis phase may lead to additional findings, such as indicators of compromise, which can be used for Containment and eradication, a previous phase, and so on.

A closer look at the twisted ouroboros reveals it is constructed with binary numbers. The red binary numbers symbolize the six phases of the incident response process. And yes, we intended to cross out "beast" and replace it with "breach" as a play on words and a nod to the ouroboros and response process.

[1] https://en.wikipedia.org/wiki/Ouroboros

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 because threat actors are determined, resourceful and quick. The 2019 Data Breach Investigations Report (DBIR)[2] is brimming with threat actor "success" metrics. Some of the most significant of these relate to speed: time-to-compromise (minutes) and time-to-exfiltration (minutes+) within victim organization environments.

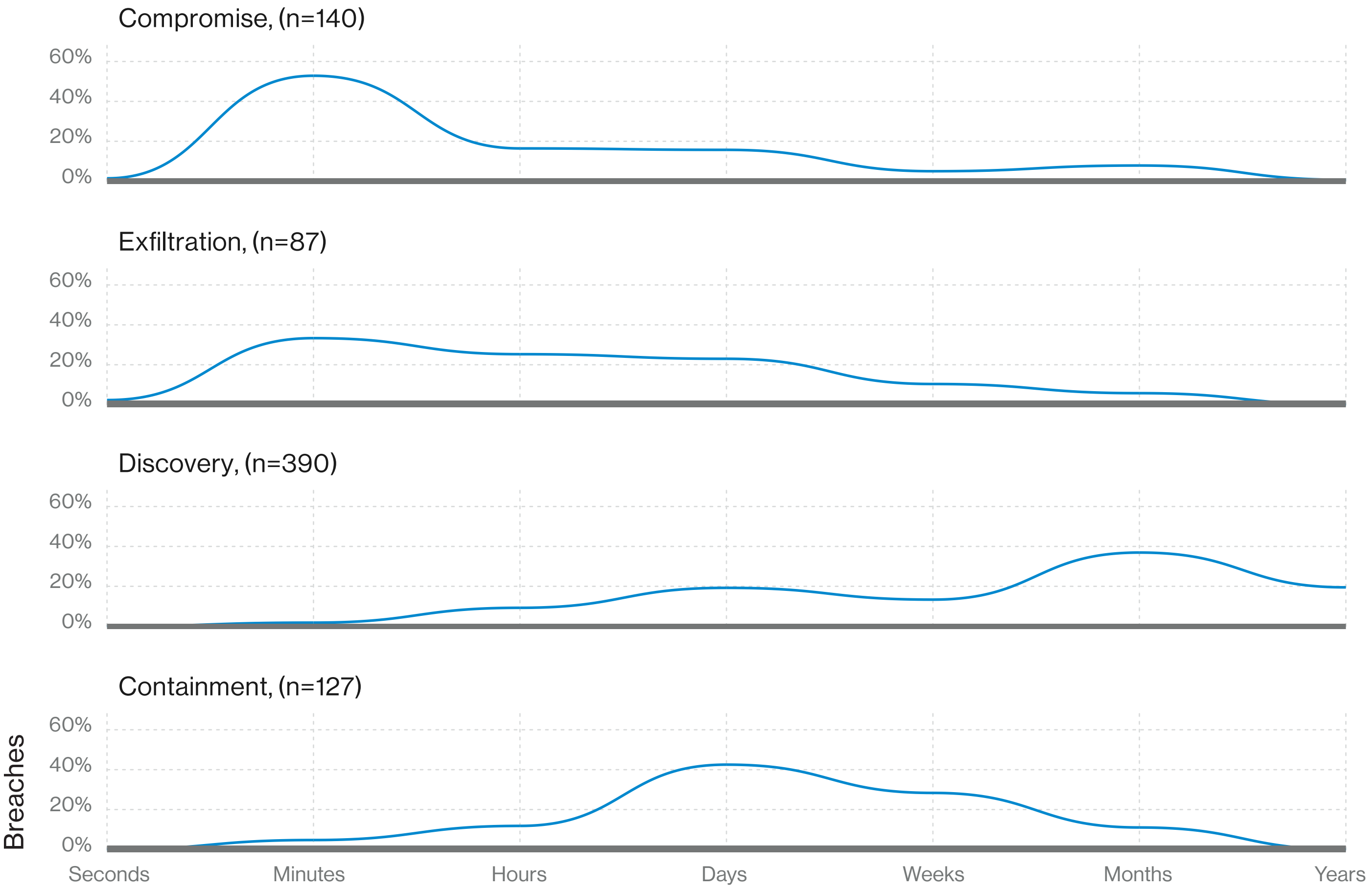


Figure 1: Data breach timelines (2019 DBIR Figure 28. Breach timelines)

The 2019 DBIR states, consistent with recent years, that:

> *"When breaches are successful, the time to compromise is typically quite short ... [and] ... the time from the attacker's first action in an event chain to the initial compromise of an asset is typically measured in minutes. Conversely, the time to discovery is more likely to be months [and] ... is very dependent on the type of attack in question. ... it goes without saying that not being compromised in the first place is the most desirable scenario in which to find oneself."*

[2] https://enterprise.verizon.com/resources/reports/dbir/

Having an efficient and effective IR Plan is the ultimate reason for our Verizon Incident Preparedness and Response (VIPR) Report. The VIPR Report is 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.

This "Taming the Data Breach" 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.

So, let's tame the data breach and see what goes into building a solid IR Plan.

Verizon Threat Research Advisory Center (VTRAC)

Each year, the VTRAC | Investigative Response Team performs cybersecurity investigations for hundreds of commercial enterprises and government agencies worldwide. Besides data breach investigations, over the years we've conducted hundreds of proactive, incident response-related assessments and data breach simulation exercises for our customers.

Our capabilities include endpoint forensics, network forensics, malware reverse engineering, threat intelligence, threat hunting, dark web research, mobile device forensics, and complex data recovery, as well as breach simulations, cyber threat briefings, IR capability assessments, and IR Plan and playbook development.

We also create and contribute to industry-recognized Verizon publications, including the DBIR,[3] Data Breach Digest,[4] Insider Threat Report,[5] Payment Security Report[6] – and this publication, the VIPR Report.[7]

[3] https://enterprise.verizon.com/resources/reports/dbir/

[4] https://enterprise.verizon.com/resources/?cs_query=data%2Bbreach%2Bdigest&page=1

[5] https://enterprise.verizon.com/resources/reports/insider-threat-report/

[6] https://enterprise.verizon.com/resources/reports/payment-security/2018/

[7] https://enterprise.verizon.com/resources/reports/incident-preparedness-and-response-report/

Assessed entity metadata

Assessments and simulations by industry[8]

Of assessed IR Plans and simulated breaches (2016 – 2018), the top customer industries were Finance and Insurance (33%), Retail Trade (17%), and Manufacturing (15%).

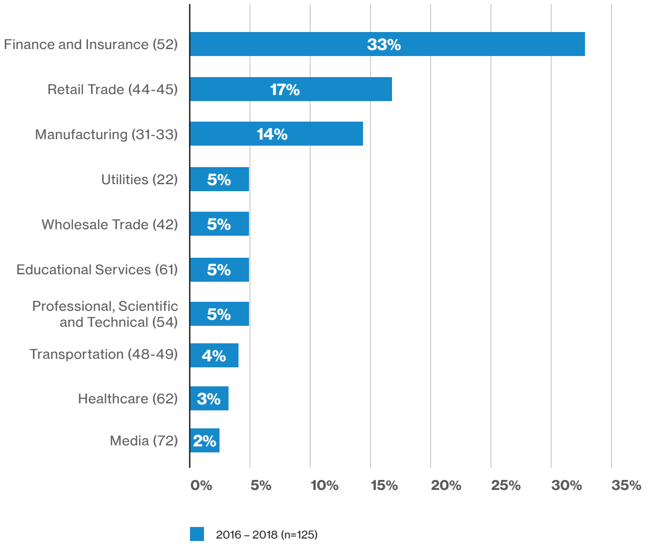


Figure 2: Assessments and simulations by industry (NAICS #)

Assessments and simulations by department

For assessments and simulations (2016 – 2018), the top customer departments requesting these services were Information Security (62%), Risk Management and Compliance (14%), Incident Response and Investigations (10%), and Information Technology (8%).

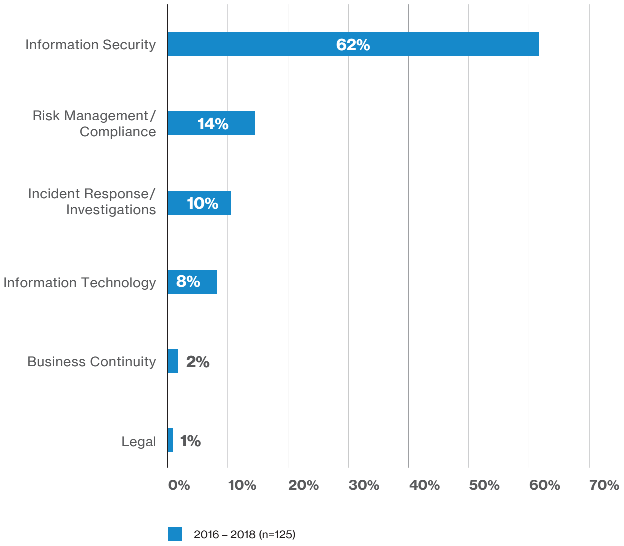


Figure 3: Assessments and simulations by department

Breach simulation themes

For breach simulation themes, of those assessed (2018), data breaches (various elements) (54%), Insider Threat (16%) and Ransomware (14%) topped the list.

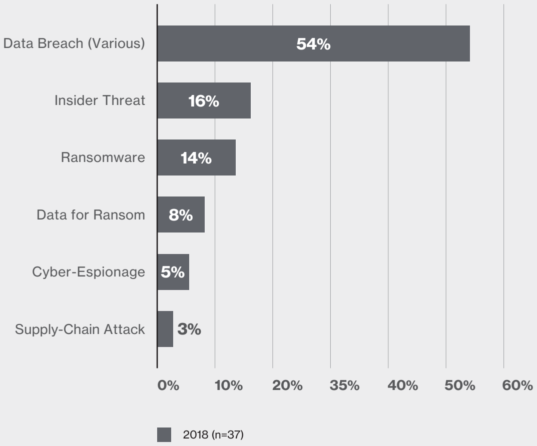


Figure 4: Breach simulation themes

[8] https://www.naics.com/

Using the VIPR Report

We've structured the VIPR Report to make it easy to use by matching its main sections with the six phases of incident response (1) Planning and preparation, (2) Detection and validation, (3) Containment and eradication, (4) Collection and analysis, (5) Remediation and recovery, and (6) Assessment and adjustment. Each section (phase) contains sub-components, and within each are IR Plan assessment observations and recommendations, as well as data breach simulation recommendations. These are reflected in standard bar charts and tri-graphs.

Below is an example of a tri-graph of eight IR Plan assessment areas with three relevant outcomes (1 – yes, in-place; 2 – partially, in-place; and 3 – no, not in-place):

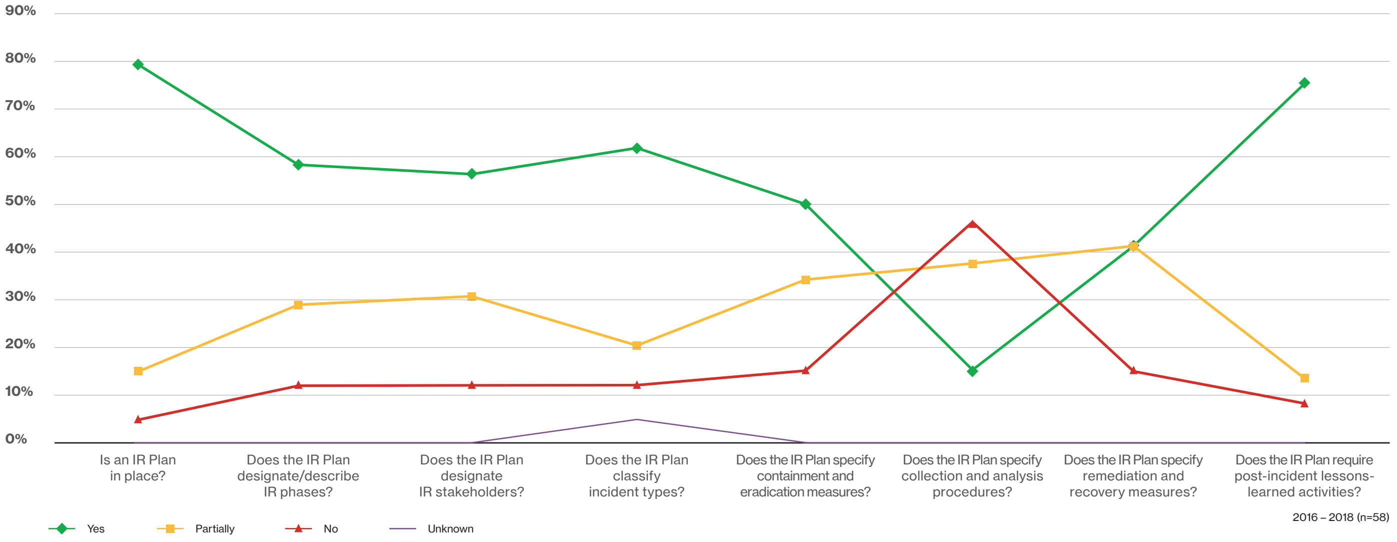


Figure 5: Plan assessments | Phases 1–6 - select IR Plan elements

Placed throughout the report are five data breach scenarios (see Using the Breach Simulation Kits (BSKs) 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.

Using the breach simulation kits

The five data breach scenarios illustrate the need for an IR Plan, playbooks and their underlying components. These scenarios, together with the countermeasure worksheet (Appendix A) and solutions, form Breach Simulation Kits (BSKs). BSKs can facilitate data breach simulation workshops involving internal IR stakeholders and tactical responders, as well as external entities. Conducting a BSK workshop session is a five-step process.

Step 1 – Getting started

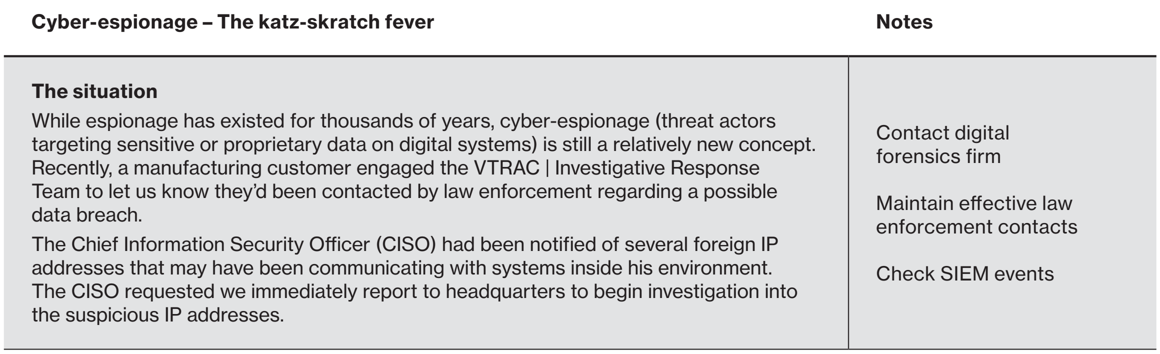
To facilitate a BSK workshop, you'll need:

- A suitable facility – a "war room" or conference room free of noise and other distractions
- A whiteboard or butcher-block paper and markers
- Printouts of scenarios and countermeasures worksheets (and highlighters) for each participant

A typical BSK workshop session consists of 1–2 scenarios and can last for 1–2 hours, depending on participant knowledge levels and experience.

Step 2 – The scenario

Begin the workshop by distributing printouts of the scenario (including situation, response and lessons learned) to participants (optional: distribute the countermeasure worksheet).



Cyber-espionage – The katz-skratch fever	Notes
The situation While espionage has existed for thousands of years, cyber-espionage (threat actors targeting sensitive or proprietary data on digital systems) is still a relatively new concept. Recently, a manufacturing customer engaged the VTRAC | Investigative Response Team to let us know they'd been contacted by law enforcement regarding a possible data breach. The Chief Information Security Officer (CISO) had been notified of several foreign IP addresses that may have been communicating with systems inside his environment. The CISO requested we immediately report to headquarters to begin investigation into the suspicious IP addresses.	Contact digital forensics firm Maintain effective law enforcement contacts Check SIEM events

Figure 6: The scenario – The situation, response and lessons learned

Give participants 10–15 minutes to read the scenario, highlight and take notes. Allow participants to talk and discuss among themselves.

Step 3 – Countermeasure worksheet

After participants have read the scenarios, facilitate a discussion by selecting a participant to walk through the situation, response and lessons learned. Discuss key observations on countermeasures. Take notes on the whiteboard or butcher-block paper (or use the countermeasures worksheet) by progressing through the six phases of incident response (include prevention and mitigation countermeasures).

Phase	Countermeasure
1 – Planning and preparation	• Create an IR playbook for cryptocurrency-related scenarios; train incident responders on efficient and effective response activities
2 – Detection and validation	• Conduct periodic threat hunting activities across the network to locate and identify any undetected cyber threat activity evading traditional cybersecurity tools • Be vigilant for anomalous activity, such as sharp increases in system CPU usage or network egress/ingress traffic volumes; monitor firewall and network appliance logs for anomalous activity

Figure 7: Countermeasure worksheet – the six phases of incident response plus mitigation and prevention

Give participants 15–20 minutes to discuss, and be sure everyone has an opportunity to speak.

Step 4 – Countermeasure solutions

Distribute countermeasure solutions (answers). Continue facilitating the discussion by comparing participant solutions to countermeasure solutions. Do they differ? Did the participants come up with more actionable items than those provided in the countermeasure solutions?

Detection and response

- If not already involved, engage law enforcement when the time is right, and third-party investigators when applicable
- Collect access logs to key servers and email; prior to system shutdown, collect in-scope volatile data and system images; examine quickly
- Utilize internal and external intelligence resources to develop actionable intelligence on threat actor modus operandi and indicators of compromise (IoCs)

Mitigation and prevention

- Provide, at least annually, user cybersecurity awareness training, emphasizing awareness and reporting suspicious emails
- Make external emails stand out; prepend markers to the “Subject:” line indicating externally originated emails
- Move beyond single-factor authentication and implement multifactor authentication; require virtual private network (VPN) access for remote connections to the corporate environment

Figure 8: Countermeasure solutions

Give participants 10–15 minutes to discuss.

Step 5 – Lessons learned

Complete the session by conducting a lessons-learned discussion, noting participant feedback (e.g., what went well, what went less smoothly and what can be improved on in the next session). Assemble feedback and countermeasure solutions in an action plan to update the IR Plan, determine additional IR resource requirements, and identify internal IR stakeholder and tactical responder training needs.

Give participants 10–15 minutes to discuss.

The IR Plan

The IR Plan describes roles, responsibilities and authorities for internal IR stakeholders. It identifies incident detection, types of attacks, and severity levels to guide internal IR stakeholders and tactical responders. The IR Plan is framed around the phases of incident response.

Phases of incident response

IR phases offer a standardized, enterprise-wide workflow for internal IR stakeholders, tactical responders and external entities. It is iterative and follows a cyclical flow from beginning to conclusion. Typical IR Plans use 4–6 IR phases.

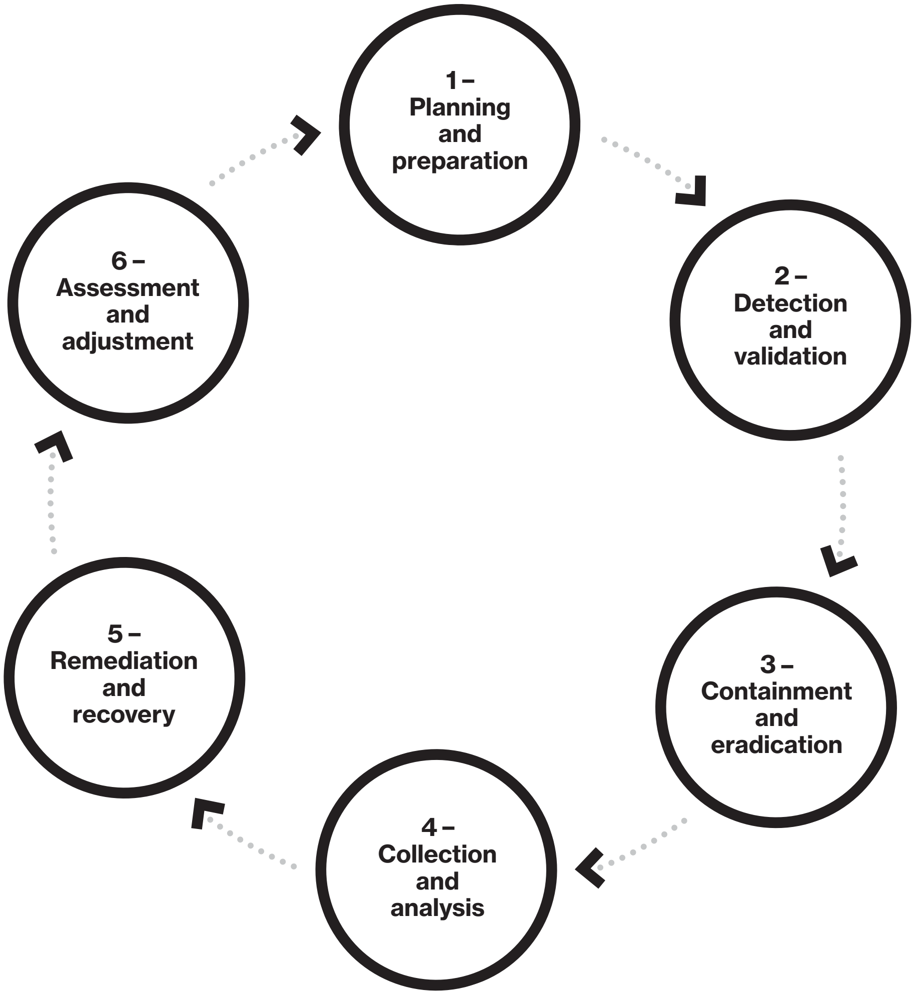

1 – Planning and preparation
2 – Detection and validation
3 – Containment and eradication
4 – Collection and analysis
5 – Remediation and recovery
6 – Assessment and adjustment

Figure 9: The phases of incident response

We're using the six-phased incident response approach above. These phases parallel those used in our IR Plan assessments and data breach simulations, and represent the six major sections of this publication.

Phase 1 – 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.

Key IR Plan elements when starting out

When embarking on any journey, we need to start with an objective. Accordingly, we present our top 10 key elements for organizations that are starting to build an IR Plan.

Number	Key element
1	Feedback loops | Constant improvement requirement
2	Metrics | Key performance indicators
3	Collection and analysis guidance
4	Trained tactical responders
5	Communication plan | Call trees
6	Incident classification | Severity levels | Playbooks
7	Detection sources and asset management
8	Standardized process flow
9	Defined stakeholder roles and responsibilities
10	Governance and standards (and compliance)

Table 10: 10 key IR Plan elements

Plan construction

Assessment observations

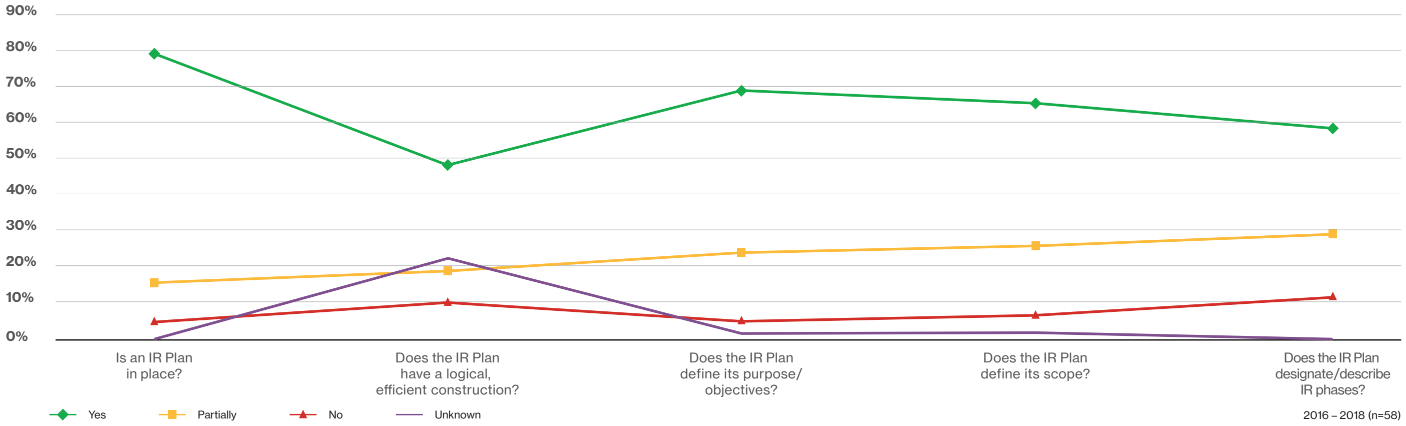


Figure 11: Plan assessments | Phase 1 - Plan construction

While most (79%) assessed organizations (2016 – 2018) had an IR Plan in place, fewer than half (48%) had a logically constructed, efficient IR Plan. Of the assessed IR Plans, most (69%) had a defined purpose and objectives, many (66%) had a defined scope, and a majority (59%) had designated or described phases of incident response.

Assessment recommendations

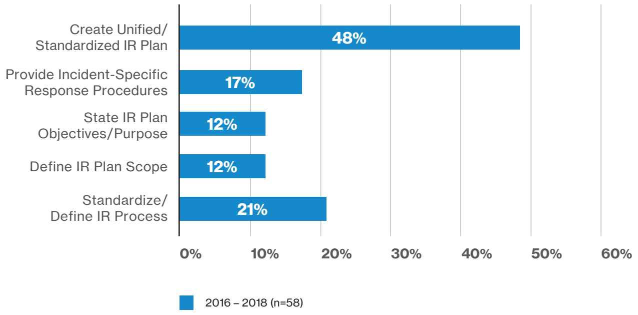


Figure 12: Plan assessments | Phase 1 - Plan construction

For assessment recommendations, 48% focused on creating a unified or standardized IR Plan, while 21% covered standardizing or defining the IR process and 17% noted providing incident-specific response procedures such as IR playbooks.

Simulation recommendations

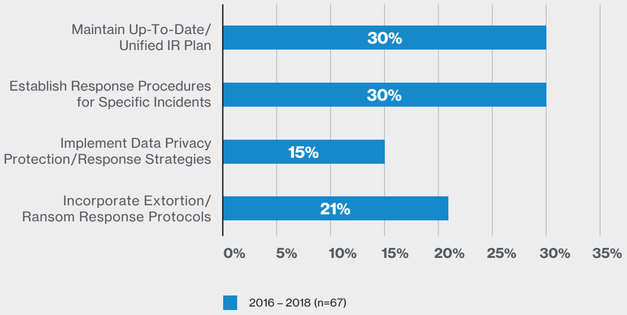


Figure 13: Breach simulations | Phase 1 - Plan construction

For breach simulations (2016 – 2018), top recommendations were maintaining (30%) an up-to-date or unified IR Plan and establishing (30%) response procedures for specific incidents (i.e., IR playbooks). The next recommendations – both currently hot cybersecurity topics – were incorporating extortion or ransom response protocols (21%) and implementing a data privacy protection or response strategy (15%).

Plan relevancy

Assessment observations

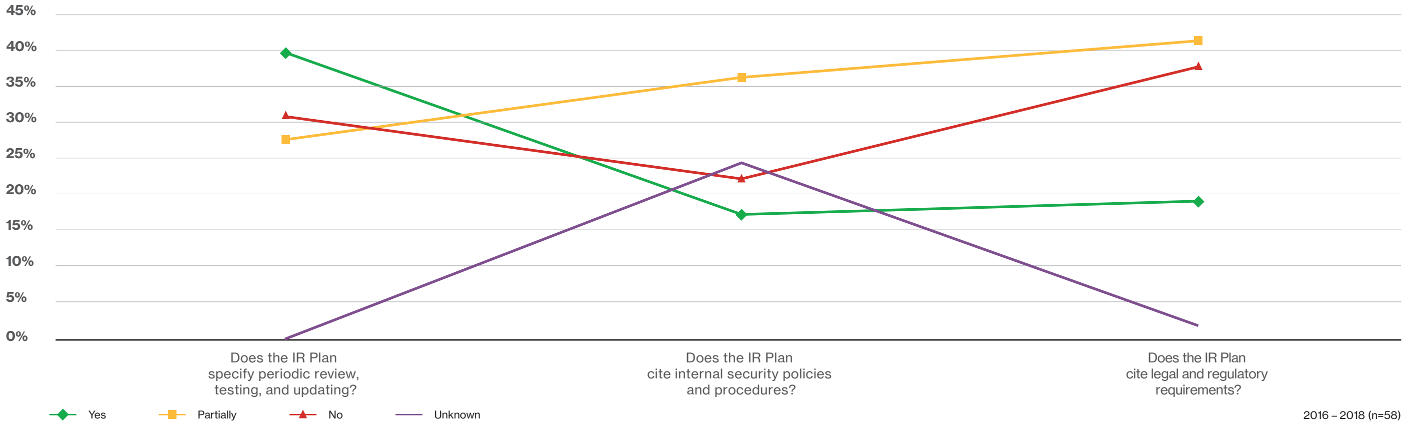


Figure 14: Plan assessments | Phase 1 - Plan relevancy

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

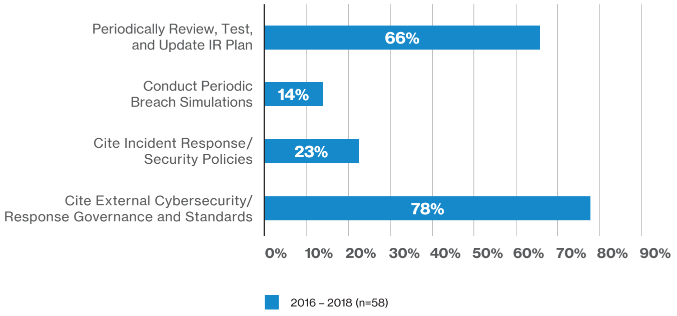


Figure 15: Plan assessments | Phase 1 - Plan relevancy

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

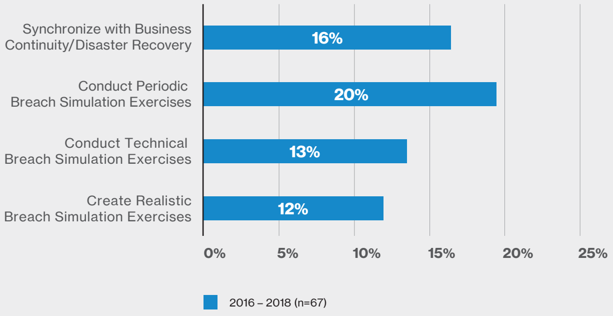


Figure 16: Breach simulations | Phase 1 - Plan relevancy

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

PCI DSS security compliance requirements for incident preparedness

The Payment Card Industry Data Security Standard (PCI DSS)[9] specifies minimum baseline requirements for documenting IR Plans and procedures. Each payment brand has additional requirements. Besides extensive access control, logging and monitoring, requirements include specifications for staffing and training, user identification, testing, continuous improvement and third-party management. These include:

- **IR Plan** (DSS Req. 12.10, 12.10.1, 12.10.2) – PCI DSS requires implementing an IR Plan and procedures to respond immediately to a cardholder data security incident. The IR Plan should be thorough and cover all elements mandated before, during and after an incident, to help an organization to respond effectively.
- **IR procedures** (DSS Req. 11.1.2, 12.5.3) – Procedures must include responding to alerts from the security monitoring system, including specifics such as detecting and responding to unauthorized wireless access points. These must be tested at least annually, and be kept current to handle emerging threats and security trends. There must also be a process to modify and evolve the IR Plan and procedures according to lessons learned after any data security incident.
- **IR staffing** (DSS Req. 10.2, 12.10.4) – The IR Plan must be disseminated, read, and understood by trained personnel, and designated personnel must be available on a 24/7 basis to respond to alerts.
- **Third-party management** (DSS Req. 12.8.3) – Proper due diligence of third parties and service providers before engagement must be maintained, including the provider's breach notification, reporting practices, IR procedures, assigned responsibilities, how PCI DSS compliance is validated, specification of evidence, and more.

Insight into industry preparedness

Most organizations have difficulty meeting DSS Req. 10.2 – the ability to reconstruct events by implementing proper audit trails. Retail organizations experience the lowest level of compliance with PCI DSS incident preparedness requirements, followed by the Financial Services industry, with a 7% gap. IT Services had a near zero control gap of approximately 1%.

Incident preparedness control gap by industry

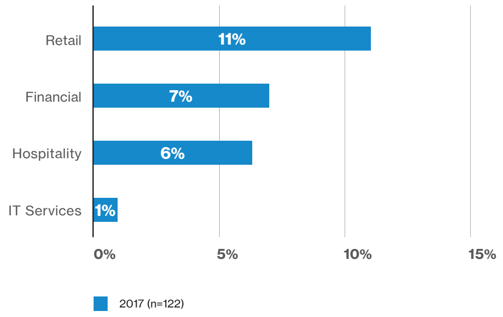


Figure 17: Incident preparedness control gap by industry

- **Retail** – Retail organizations struggle with a range of controls such as: user identification and elevation of privileges (DSS Req. 10.2.5), due diligence processes for engaging service providers (DSS Req. 12.8.3), procedures for detecting unauthorized wireless access points (DSS Req. 11.1.2), and maintaining an IR Plan (DSS DSS Req. 12.10).
- **Financial Services** – Finance organizations struggle most with implementing controls under DSS Req. 10.2 – the ability to reconstruct events through proper audit trails. This industry has the highest control gap, with an average of 21.1% controls found not in place.
- **Hospitality** – Hospitality organizations struggle most with user identification and authentication (DSS Req. 10.2.5), reviewing and testing the IR Plan (DSS Req. 12.10.4) and training to staff on breach responsibilities (DSS Req. 12.10.4).
- **IT Services** – The IT Services industry demonstrates the highest IR preparedness. The only requirements that need attention are IR procedures for unauthorized wireless access points (DSS Req. 11.1.2), and procedures to review and test the IR Plan annually (DSS Req. 12.10.2).

[9] For more insight into incident preparedness for PCI and PCI assessments, see the soon-to-be-released 2019 Verizon Payment Security Report.

Internal IR stakeholders

Assessment observations

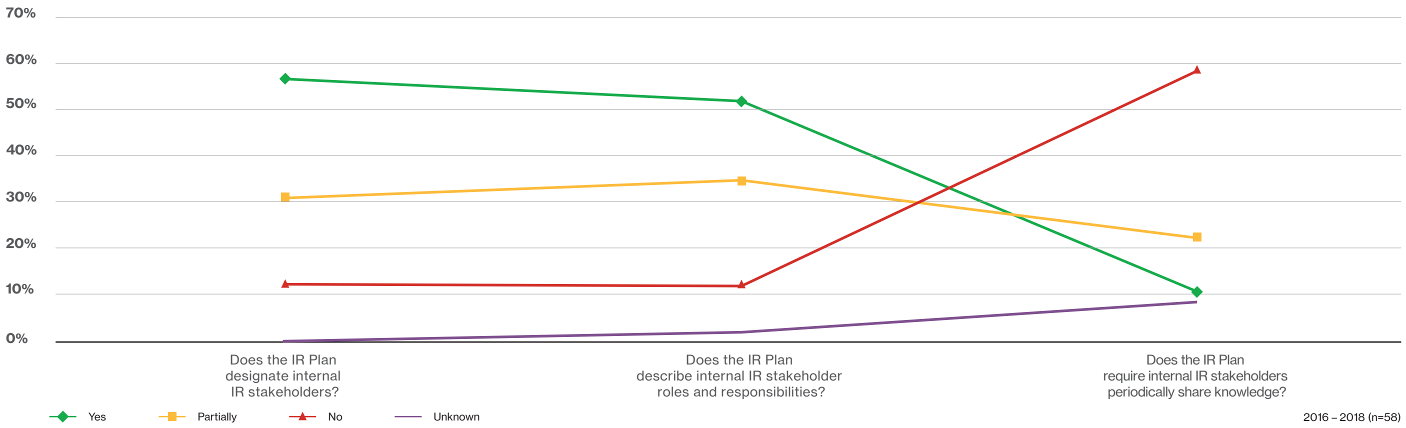


Figure 18: Plan assessments | Phase 1 - Internal stakeholders

With internal IR stakeholders (2016 – 2018),[10] 57% of assessed IR Plans fully designated internal IR stakeholders, and 52% fully described internal IR stakeholder roles and responsibilities. However, 59% of assessed IR Plans did not require internal IR stakeholders to periodically meet and discuss the cybersecurity threat landscape.

Assessment recommendations

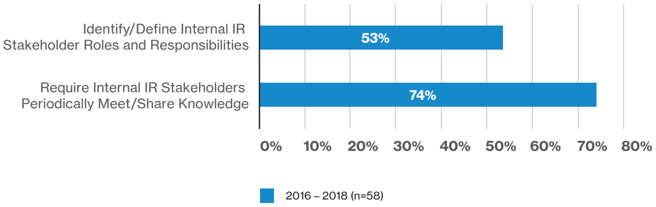


Figure 19: Plan assessments | Phase 1 - Internal IR stakeholders

For assessment recommendations, 53% covered identifying or defining internal IR stakeholder roles and responsibilities, and 74% covered requiring internal IR stakeholders to periodically meet and share cybersecurity threat landscape knowledge.

Simulation recommendations

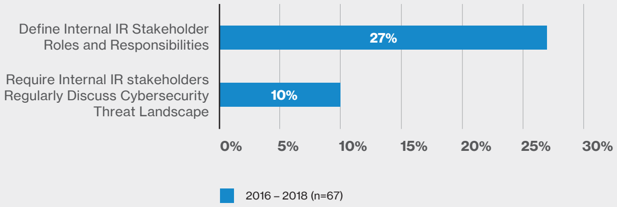


Figure 20: Breach simulations | Phase 1 - Internal IR stakeholders

For breach simulations (2016 – 2018), defining internal IR stakeholder roles and responsibilities (27%) and requiring internal IR stakeholders to regularly meet and discuss the cybersecurity threat landscape (10%) were recommended for internal IR stakeholders.

[10] For a listing of typical internal IR stakeholder roles and responsibilities, see Appendix B (IR Stakeholders) of this publication.

Tactical responders

Assessment observations

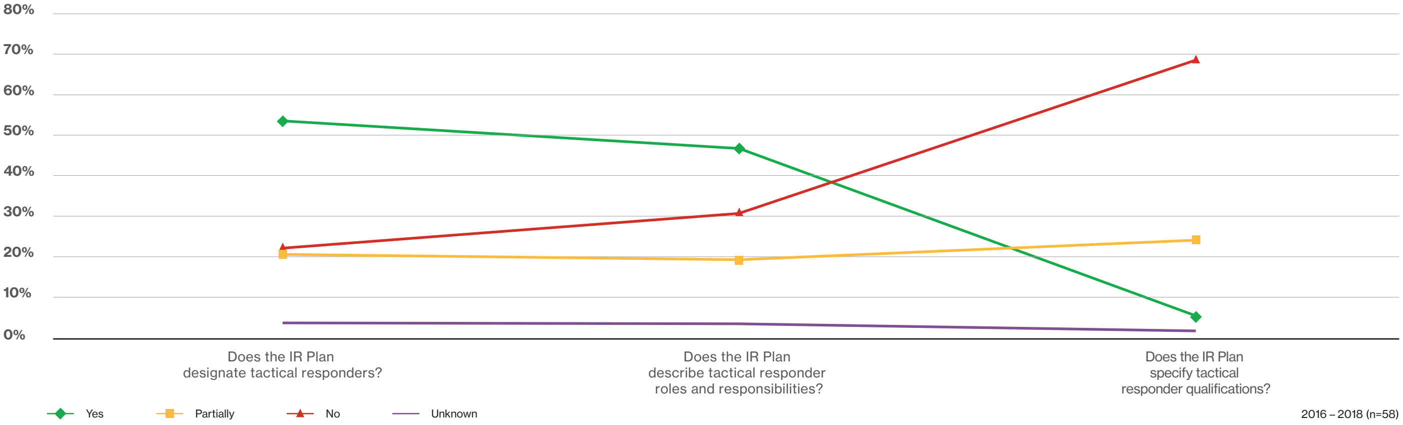


Figure 21: Plan assessments | Phase 1 - Tactical responders

Similar to internal IR stakeholders (2016 – 2018), 53% of assessed IR Plans fully designated tactical responders,[11] with 47% fully describing tactical responder roles and responsibilities. Unfortunately, 83% of assessed IR Plans specified no, or just partially specified, tactical responder qualifications (i.e., desired skills, experience, training and certifications).

Assessment recommendations

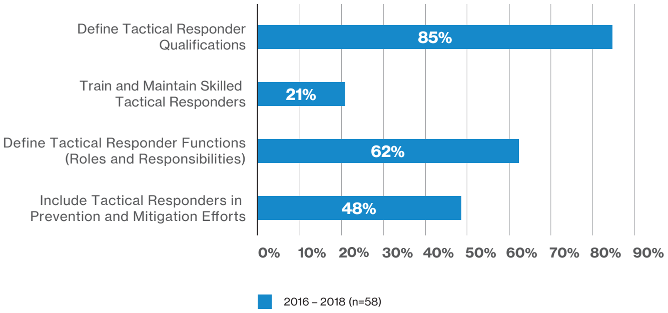


Figure 22: Plan assessments | Phase 1 - Tactical responders

Defining tactical responder qualifications (85%), tactical responder functions (roles and responsibilities) (62%), and including tactical responders in prevention and mitigation efforts (48%) were the top three tactical responder recommendations for assessments.

Simulation recommendations

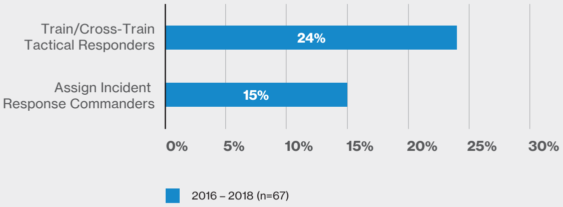


Figure 23: Breach simulations | Phase 1 - Tactical responders

Training and cross-training tactical responders (24%) and assigning incident response commanders (15%) were recommended for breach simulations (2016 – 2018).

[11] For a listing of typical tactical responder roles and responsibilities, see Appendix B (IR Stakeholders) of this publication.

A deeper dive – End users

Assessment observations

During the previous year (2018), just under one-third (29%) of assessed IR Plans described end-user security awareness training, while no (0%) IR Plans described end-user cybersecurity incident reporting training.

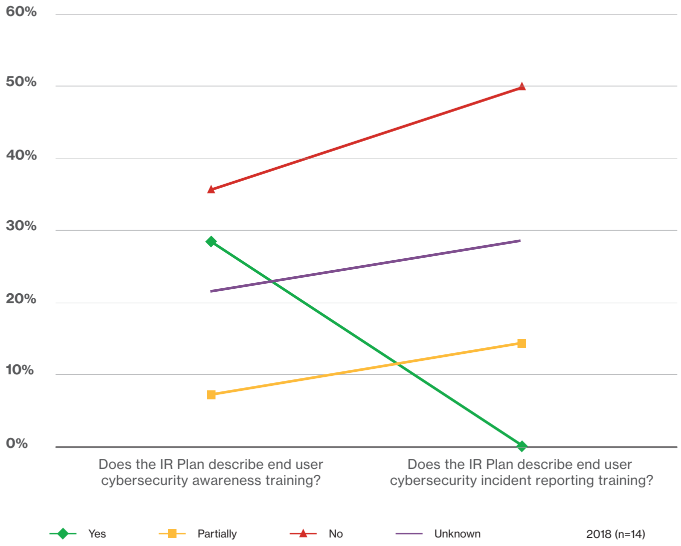


Figure 24: Plan assessments | Phase 1 - End users

Assessment recommendations

For assessed IR Plans during the previous year (2018), recommendations included conducting periodic end-user cybersecurity awareness training (50%) and sensitizing end users to report cybersecurity incidents (50%).

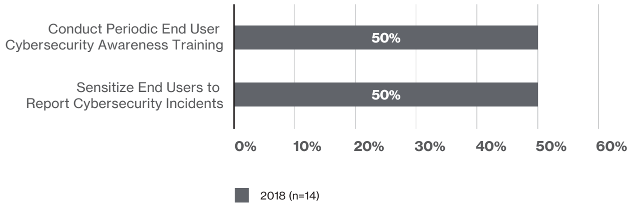


Figure 25: Plan assessments | Phase 1 - End users

Third parties

Assessment observations

For third parties,[12] during the previous year (2018), only 14% of assessed IR Plans fully or partially required periodically reviewing third-party services for incident response purposes, and only 43% fully provided third-party contact procedures.

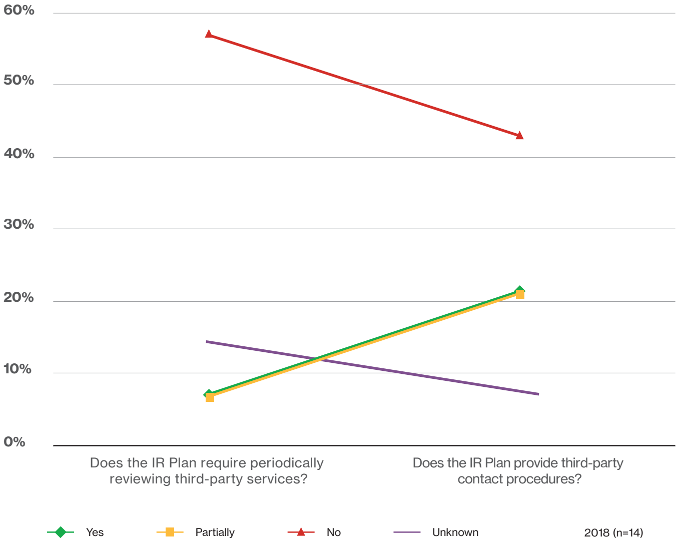


Figure 26: Plan assessments | Phase 1 - Third parties

Assessment recommendations

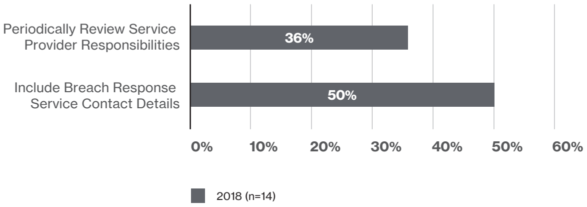


Figure 27: Plan assessments | Phase 1 - Third parties

For assessment recommendations, 50% included breach response service contract details (e.g., contact procedures for third-party digital forensic firms), and 36% covered periodically reviewing service provider responsibilities.

Simulation recommendations

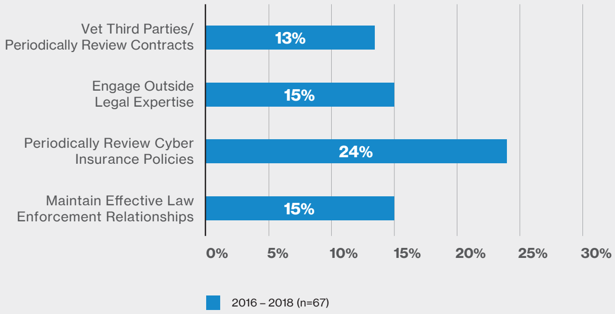


Figure 28: Breach simulations | Phase 1 - Third parties

For breach simulation (2016 – 2018) recommendations for third parties, periodically reviewing cyber insurance policies topped the list (24%), engaging outside legal expertise (15%) and maintaining an effective law enforcement relationships (15%) were second, and vetting third parties and periodically reviewing contracts was third (13%).

[12] For a listing of typical third party roles and responsibilities, see Appendix B (IR stakeholders) in this publication.

Crypto-jacking – The peeled onion[13]

The situation

This type of malware uses the processing power (e.g., CPU or graphics card) of an infected system to mine cryptocurrency, which can be used like traditional cash to purchase items, or directly exchange for currency. While mining is a legitimate process in the cryptocurrency lifecycle, using someone else's system in an unauthorized manner is not.

There are hundreds of alternative cryptocurrencies, which may be suited for mining through malware, because of either increased anonymity or the relative ease in mining on ordinary systems.

In one such non-bitcoin case, a customer who had observed many alerts originating from its firewalls called on us. The firewalls were blocking suspicious outbound traffic to The Onion Router (Tor) network and triggering alerts. The customer believed it had the situation under control because the firewalls were blocking the traffic.

The company asked us to determine the cause of the traffic, confirm that the situation was under control, and verify there were no indications of data exfiltration or lateral movement in the network.

Investigative response

Before engaging us, the customer obtained full packet captures (FPCs) of network traffic and dumped the physical memory from a system generating the suspicious outbound traffic. We dove into the network FPCs and memory, and soon provided actionable intelligence on other potentially compromised systems on the network. These IoCs included system names, IP addresses, malware file hashes and file names, and malicious process names.

While a review of active network connections revealed a majority of traffic was blocked by the firewall, successful connections were occurring to resources in the Tor network. This was due to the firewall's filtering being based on IP address blacklisting, which didn't encompass all Tor addresses used by the malware.

Notes:

[13] https://enterprise.verizon.com/resources/casestudies/2018/data-breach-digest-2018-the-peeled-onion.pdf

Crypto-jacking – The peeled onion *cont.*

Our client also observed that additional network connections were being made to a mining pool associated with the Monero cryptocurrency. All malicious network activity was identified as originating from the Microsoft “powershell.exe” process running on the sample system, as well as other infected systems.

Meanwhile, our VTRAC | Network Forensics Team reviewed the FPCs and confirmed that the malware used a propagation method similar to well-known ransomware instances, leveraging digital tools leaked by “The Shadow Brokers” hacking group.

Examining an image of the sample system confirmed it wasn’t patched against a known vulnerability, making the propagation possible. This was contrary to our customer’s belief that it was properly secured.

We then further assisted our customer by analyzing firewall logs to identify other systems beaconing to the Tor network and requiring remediation. Notably, this analysis identified over 300 infected devices.

We assisted the customer with a remediation plan that involved providing samples of the malware to its antivirus vendor, patching vulnerable systems, eradicating the malware and rebuilding key systems, which were based on legacy operating systems.

Lessons learned

During the investigation, it was discovered that hundreds of systems within the network hadn’t received the latest Microsoft Windows patches. Prompt patching could have averted this incident.

On this occasion, the malware targeted cryptocurrency mining; more nefarious malware could have leveraged the same vulnerabilities and made a more significant impact on the business.

Notes:

Countermeasure solutions

Detection and response

- Create an IR playbook for cryptocurrency-related scenarios; train incident responders on efficient and effective activities
- Conduct periodic threat hunting activities across the network to locate and identify any undetected cyber threat activity evading traditional cybersecurity tools
- Be vigilant for anomalous activity, such as sharp increases in system CPU usage or network egress and ingress traffic volumes; monitor firewall and network appliance logs for anomalous activity
- Block access to command and control (C2) servers at the firewall level; deploy group policy objects (GPOs) to block known malicious executable files and disable macros
- Employ enterprise and host-based antivirus solutions with up-to-date signatures to detect and eradicate threats as they arise
- Analyze malware functionality for detection and response, as well as mitigation and prevention

Mitigation and prevention

- Block and alert internet connections to cryptocurrency mining pools; include Tor networks, unless there's a valid business reason not to do so
- For critical systems and servers, deploy file integrity management (FIM) and application white listing (AWL) solutions; add intrusion prevention system (IPS) rules; disallow internet browsing
- Establish a patch management program; apply security patches as soon as possible; confirm patching succeeded
- To the extent possible, remove local admin, force standard user use for web browsing activity and force escalation for privileged user use in other context
- Conduct regular security assessments; evaluate defensive architecture design based on sandboxing, web browser separation and virtualization for select activities

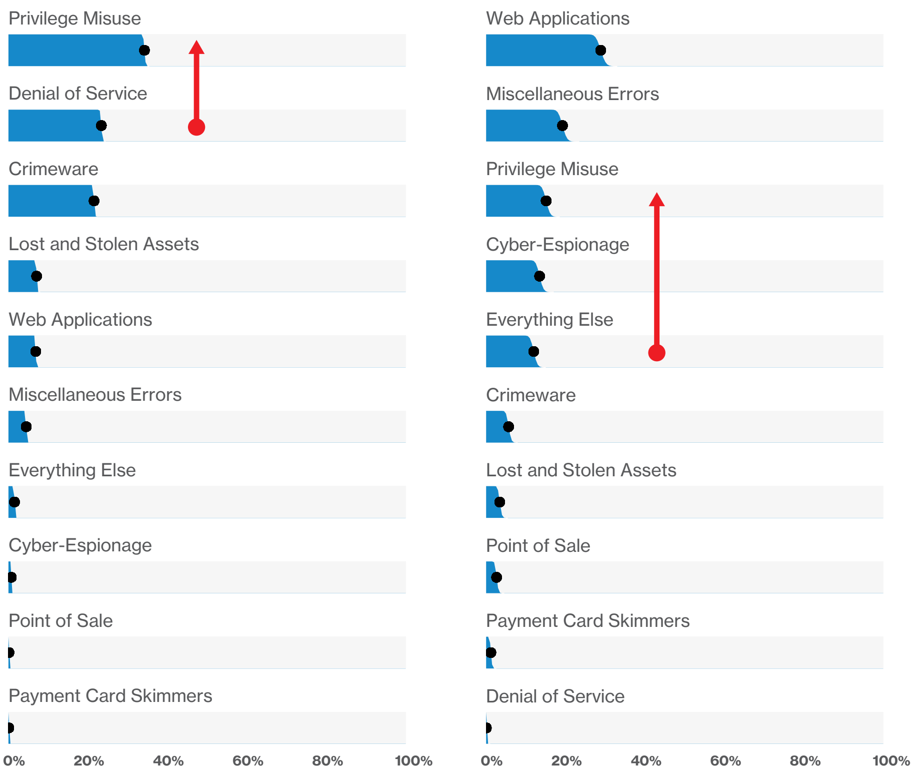
Phase 2 – Detection and validation

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

Insider threats – Moving up the stacks

Readers of the 2019 DBIR may have noticed changes in the cybersecurity incident and data breach patterns from the 2018 DBIR to the 2019 edition. Among incident pattern shifts, we've seen insider and privilege misuse (the insider threat) moving from second to first position for incidents (DBIR figure 35), and from fifth to third position for breaches (DBIR figure 36).

If you're in the Healthcare (59%), Educational Services (45%), Information (44%), and Financial and Insurance (36%) industries, you'll want to pay particular attention to internal threats. Can anyone say "Insider Threat Playbook?"[14]



Incidents
2019 DBIR Figure 35. Incidents per pattern (n=41,686)

Breaches
2019 DBIR Figure 36. Breaches per pattern (n=2,013)

Figure 29: 2019 DBIR incidents per pattern

[14] https://enterprise.verizon.com/resources/reports/insider-threat-report/

Incidents and events

Assessment observations

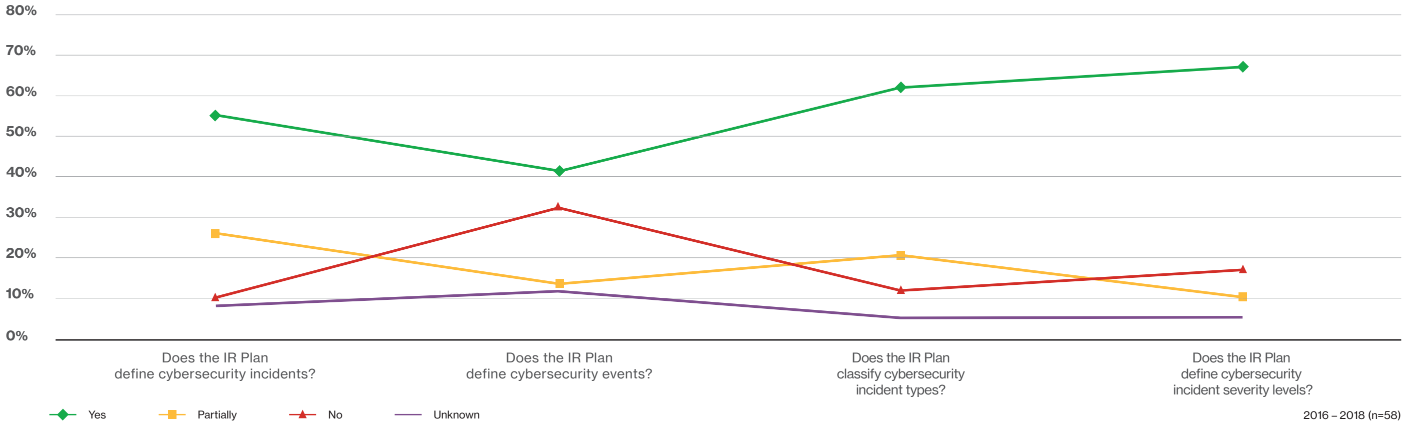


Figure 30: Plan assessments | Phase 2 - Incidents and events

Of assessed IR Plans (2016 – 2018), 55% fully defined cybersecurity incidents, 41% fully defined cybersecurity events, 62% fully classified cybersecurity incident types, and 67% fully defined cybersecurity incident severity levels.

Assessment recommendations

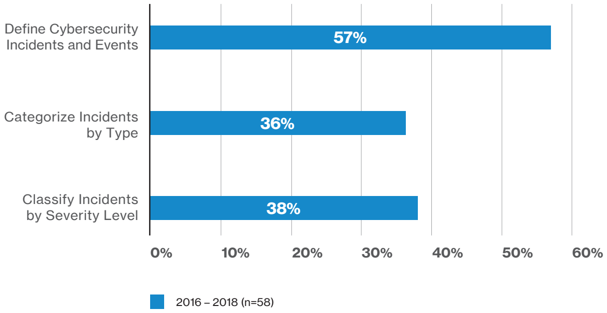


Figure 31: Plan assessments | Phase 2 - Incidents and events

For assessments, defining cybersecurity incidents and events (57%) categorizing incidents by type (36%), and classifying incidents by severity level (38%) were recommended for incidents and events.

Simulation recommendations

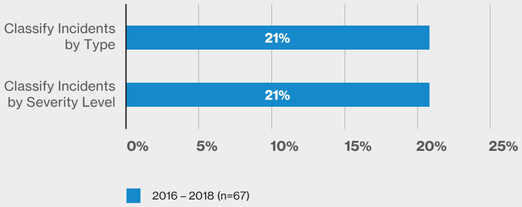


Figure 32: Breach simulations | Phase 2 - Categorizing incidents

For incidents and events associated with breach simulations (2016 – 2018), classifying incidents by type (21%) and classifying incidents by severity level (21%) both were similarly recommended.

Classifying incidents

Differentiating incidents from events is crucial to developing an effective IR process. In simple terms, an incident is an exceptional situation requiring IR stakeholder action, while an event is a regular occurrence not requiring IR stakeholder action. Examples of incidents include malware outbreaks; internal scans, probes and attempted access; and unauthorized access to critical systems. Examples of events include single-host antivirus detection, external port scans and social engineering attempts.

For cybersecurity incidents, we recommend identifying six to eight incident types. By defining incident types, stakeholders can prepare for incidents, focus efforts and quickly engage resources when they occur. These incident types can also determine topics for specific playbooks (i.e., run books) that support the overall IR Plan.

In our IR Plan assessment efforts, we've seen organizations define incidents using various industry-accepted standards. For example, the US-CERT Federal Agency Incident Categories[15] define incidents as Exercise/Network Defense Testing, Unauthorized Access, DoS, Malicious Code, Improper Usage, Scans/Probes/Attempted Access, [under] Investigation). The NIST Special Publication 800-61 Revision 2 Attack Vectors[16] classifies incidents as External/Removable Media, Attrition, Web, Email, Impersonation, Improper Usage, Loss or Theft of Equipment, Other).

The VERIS framework Threat Actions, in a manner, categorizes incidents as Malware, Hacking, Social, Misuse, Physical, Error and Environmental. Given the consistency over the years, DBIR incident patterns described on the next page may serve as a starting point for classifying incidents.

[15] http://www.us-cert.gov/government-users/reporting-requirements
[16] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

DBIR incident patterns

In our 2014 DBIR, we identified nine incident patterns representing the most likely threats. In our 2019 DBIR, this heuristic continued to hold true, with 98.5% of security incidents and 88% of confirmed data breaches falling into these patterns.[17]

Pattern	Description
Insider and Privilege Misuse	Any unapproved or malicious use of organizational resources; trusted actors leveraging logical or physical access in an inappropriate or malicious manner
Cyber-Espionage	Unauthorized network or system access linked to state-affiliated actors or exhibiting the motive of espionage; targeted attacks from external actors hunting for sensitive internal data and trade secrets
Web Application Attacks	Incidents in which a web app was the vector of attack; web app-related stolen credentials or vulnerability exploits
Crimeware	Instances involving malware that did not fit into a more specific pattern; malware incidents, typically opportunistic and financially motivated (e.g., banking Trojans, ransomware, command and control (C2) malware)
Point of Sale (POS) Intrusions	Remote attacks against the environments where card-present retail transactions are conducted; attacks on PoS environments leading to payment card data disclosure
Denial of Service (DoS) Attacks	Any attack intended to compromise the availability of networks and systems; non-breach-related attacks affecting business operations
Payment Card Skimmers	Incidents in which a skimming device was physically implanted (tampering) on an asset that reads magnetic stripe data from a payment card; physical tampering of automated teller machines (ATMs), fuel-pumps, PoS terminals
Physical Theft and Loss	Incidents where an information asset went missing, whether through misplacement or malice, physical loss or theft of data, or IT-related assets
Miscellaneous Errors	Incidents in which unintentional actions directly compromised a security attribute of an asset; an error directly causing data loss

Table 33: DBIR incident classification patterns

[17] https://enterprise.verizon.com/dbir2019/

Detection sources

Assessment observations

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

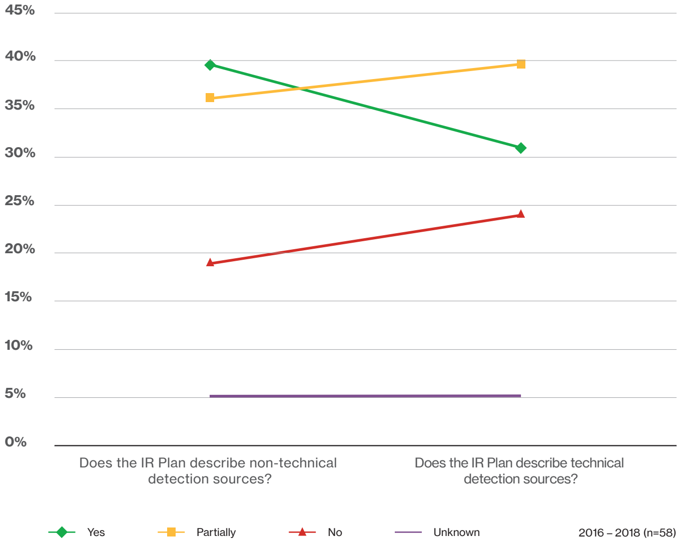


Figure 34: Plan assessments | Phase 2 - Detection sources

Assessment recommendations

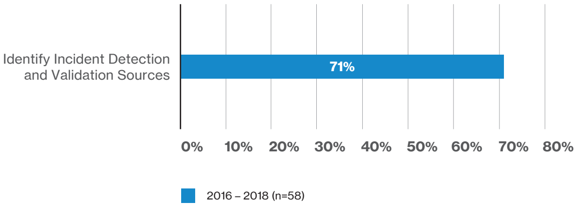


Figure 35: Plan assessments | Phase 2 - Detection sources

For assessments, identifying incident detection and validation sources (71%) was the main recommendation for detection sources.

Simulation recommendations

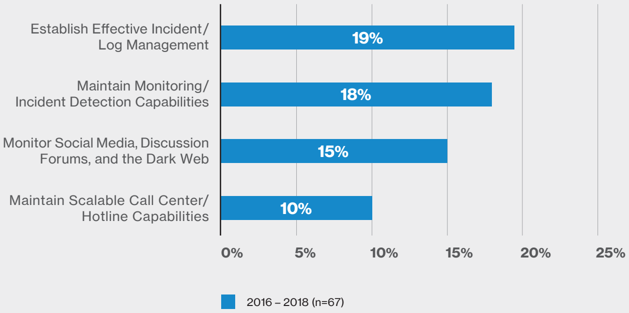


Figure 36: Breach simulations | Phase 2 - Detection sources

For breach simulations (2016 – 2018), recommendations were establishing effective incident and log management (19%), maintaining monitoring and incident detection capabilities (18%), monitoring social media, discussion forums and the dark web (15%), and maintaining scalable call center and hotline capabilities (10%).

A deeper dive – Advanced detection

Simulation recommendations

For advanced detection over the previous year (2018), the top three recommendations were conducting threat-hunting activities (8%), implementing an endpoint detection and response (EDR) solution (5%), and implementing a file integrity monitoring (FIM) solution (5%).

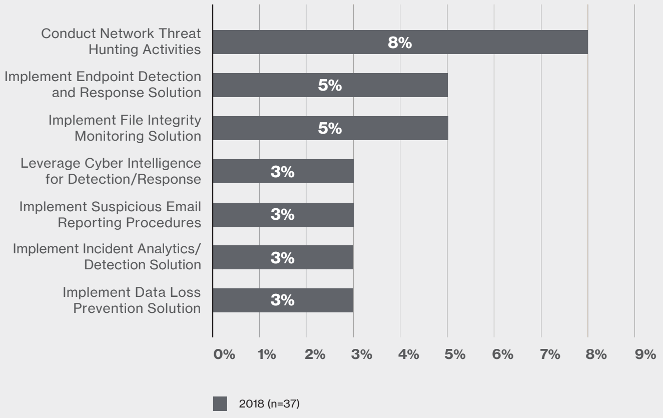


Figure 37: Breach simulations | Phase 2 - Advanced detection

A deeper dive – Scoping and triaging

Assessment observations

Of assessed IR Plans (2016 – 2018), 45% provided incident scoping guidance and 23% provided no scoping guidance. Similarly, for incident triaging, 43% provided incident triaging guidance and 24% provided no triaging guidance.

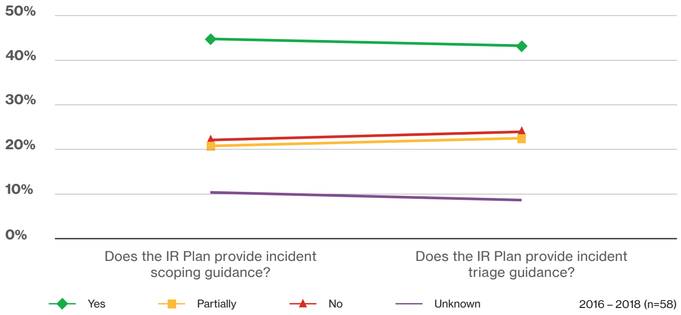


Figure 38: Plan assessments | Phase 2 - Scoping and triaging

Assessment recommendations

For assessed IR Plans (2016 – 2018), establishing an initial incident scoping checklist was recommended (50%).

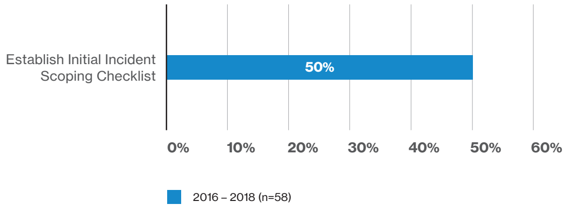


Figure 39: Plan assessments | Phase 2 - Scoping and triaging

Effective detection and response

The expansion of existing technologies such as the Internet of Things (IoT), wireless and global IP, as well as the dawn of new technologies including 5G, artificial intelligence (AI) and next-gen cloud and edge computing, are rapidly expanding organizations' attack surfaces. This demands a ready and capable security operations center (SOC) and cyber incident response team (CIRT). The saying, "an ounce of prevention is worth a pound of cure," is especially true in detection (SOC) and response (CIRT), with prevention being the SOC and CIRT the cure. An organization's security policy gives these teams the authority and ability to carry out their duties; working together, they can ensure IT health through quick triage and response. The following is a high-level view on the basics to create effective detection and response.

- **Information requirements** – The SOC and CIRT both need information to quickly and effectively triage events, and respond to incidents. At a minimum, these teams require:
    - Asset inventory – Virtual and physical systems, their purpose, associated ports and protocols, dependencies, POCs, and applications
    - High-value assets – People, hardware, software, intellectual property and systems critical to the organization
    - Network visibility – Ingress and egress points, DMZ, network diagrams, data flows
    - Conditions – Notification of changes that may affect response, such as updated firewall rules, commissioning and decommissioning servers, network and network protocol changes, planned outages, patching schedules, etc.

- **Services catalog** – A services catalog[18] should be created for both SOC and CIRT, which includes a charter or mission statement. This clears up confusion regarding what the SOC and CIRT do, what their responsibilities are, and what support they can give to other teams in a cybersecurity capacity. By using the services outlined in both the service catalogs, a process flow can be created regarding how triaged security events are to be transferred from the SOC to CIRT for investigation. The service catalogs and process flows will also help prevent a blurring of lines of responsibility that can exist between the SOC and CIRT.

- **Security Information and Event Management (SIEM)** – An organization's SIEM platform is a vital tool for detection and response, as well as internal threat hunting. SIEMs collect logs from devices and applications, such as servers, firewalls, AV, etc. Through use cases (UC), the SIEM aggregates data in the logs and triggers security event alerts upon meeting UC conditions. In turn, the SOC triages their alerts. Care and feeding of the SIEM is crucial to alert on security events for triage. Examples include:
    - Logging critical systems into SIEM, such as DNS, DHCP, firewall, active directory, endpoint protection, anti-virus
    - Ensuring UCs reflect risks to the organization's industry and its global footprint
    - Creating detailed SIEM UC playbooks, run books and triage steps, and updating as needed
    - Regularly reviewing UCs for relevance, and adding new ones to reflect changing risks
    - Regularly reviewing logs to reduce duplication

- **IR Plan** – With vital information in line, the services catalog approved by stakeholders and circulated across the organization, and the SIEM up and running, this information can be used to create and update the IR Plan.

- **After-action feedback loop** – To keep the IR Plan timely, and to evaluate the effectiveness and status of the cybersecurity posture, root cause analysis (RCA) should be performed on each incident. In turn, results and lessons learned should be shared with teams such as network, systems administration, etc. Red team activities should also test the SOC's effectiveness in detecting and responding to major threats faced by the organization. Results from Red team engagements should be treated the same as an RCA on any successful attempts.

[18] For example, see those security services covered in NIST SP 800-35, Guide to Information Technology Security Services (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-35.pdf).

Tracking and reporting

Assessment observations

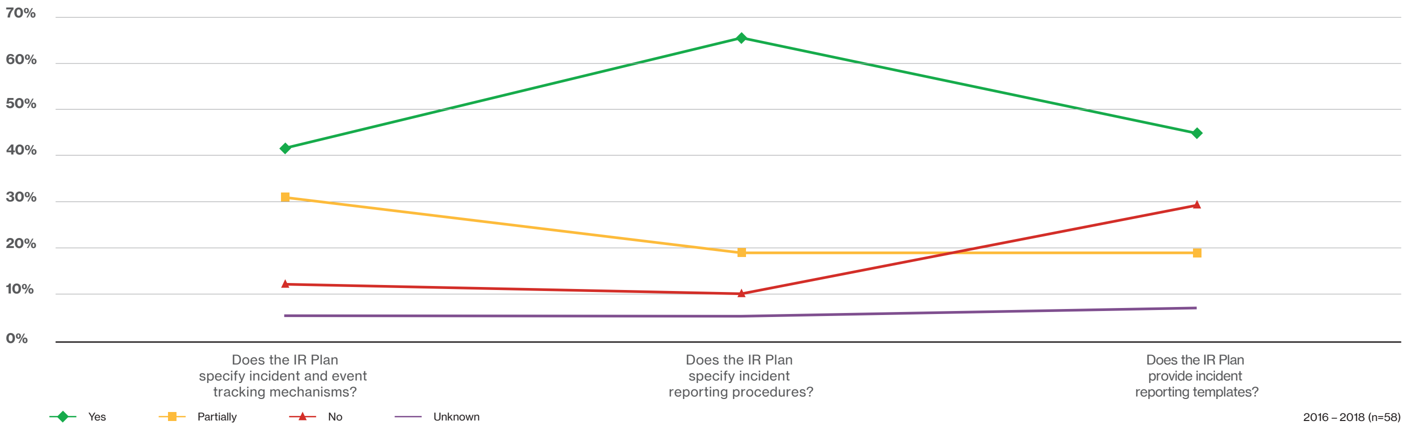


Figure 40: Plan assessments | Phase 2 - Tracking and reporting

For tracking and reporting incidents, of assessed IR Plans (2016 – 2018), 42% fully specified (and 40% partially specified) incident and event tracking mechanisms, and 66% fully specified (and 19% partially specified) incident reporting procedures.

Assessment recommendations

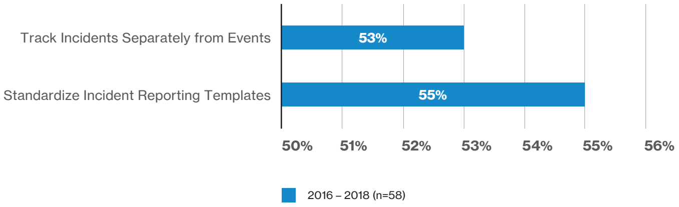


Figure 41: Plan assessments | Phase 2 - Tracking and reporting

For assessments, tracking incident separately from events (53%) and standardizing incident reporting templates (55%) were both recommended.

Simulation recommendations

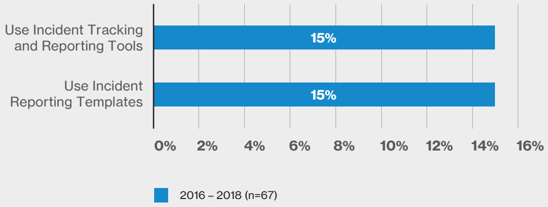


Figure 42: Breach simulations | Phase 2 - Tracking and reporting

For breach simulations (2016 – 2018), recommendations for tracking and reporting included using incident tracking and reporting tools (15%) and using incident reporting templates (15%).

Escalating and communicating

Assessment observations

For assessed IR Plans (2016 – 2018), in terms of communicating, only 40% fully (and 43% partially) specified IR stakeholder escalation criteria, while only 45% fully (and 31% partially) specified IR stakeholder notification procedures.

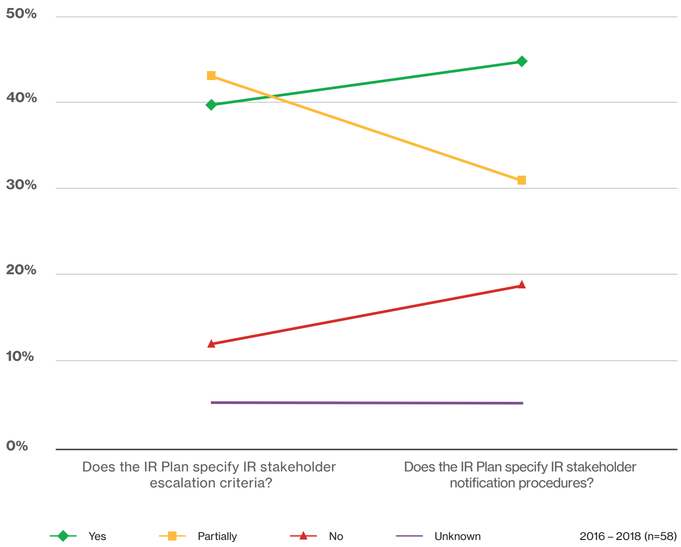


Figure 43: Plan assessments | Phase 2 - Escalating and communicating

Assessment recommendations

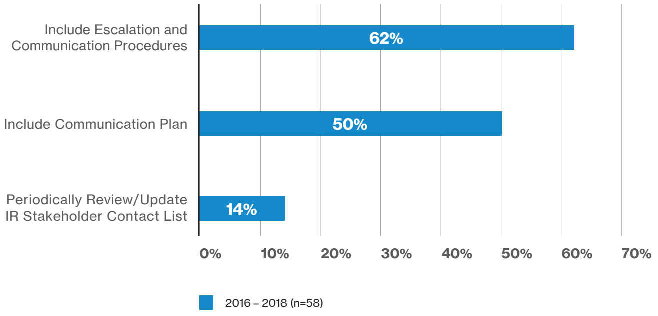


Figure 44: Plan assessments | Phase 2 - Escalating and communicating

In terms of escalating and communicating recommendations, for assessments, the top recommendation was including escalation and communication procedures (62%), then including a communication plan (50%), and periodically reviewing and updating IR stakeholder contact list (e.g., call trees) (14%).

Simulation recommendations

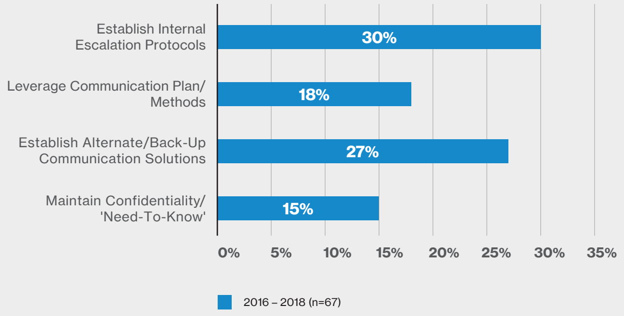


Figure 45: Breach simulations | Phase 2 - Escalating and communicating

Escalating and communicating recommendations from breach simulations (2016 – 2018) included establishing internal escalation protocols (30%), establishing alternate or backup communication solutions (27%), leveraging communication plan/ methods (18%) and maintaining confidentiality or need-to-know (15%).

A deeper dive – External notifications

Simulation recommendations

For breach simulations (2016 – 2018), the top recommendation for external notifications was maintaining external contact and notification procedures (22%) followed by creating external notification methods and templates (13%).

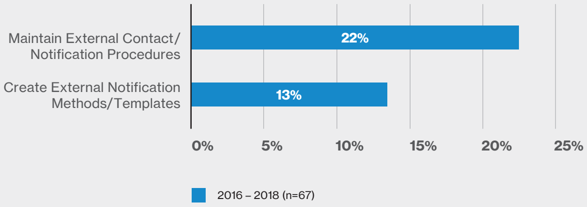


Figure 46: Breach simulations | Phase 2 - External notifications

Escalation and notification matrix

An escalation and communication matrix determines who should be contacted, how soon, and how often, if a data breach or cybersecurity incident occurs. This matrix depends on pre-defined incidents (e.g., crimeware, DoS, web app attack), assigned severity levels for each incident (e.g., high, medium, low), and identified IR stakeholders with need-to-know and need-to-be-informed status. Below is an example of an escalation and notification severity matrix.

Tier	Definition	Escalation	Timing
1 – High	Severe cybersecurity concern or severe impact on business operations	1. Executive management 2. All IR stakeholders 3. Third parties 4. Information security	1. Immediately 2. Immediately 3. As necessary 4. Immediately
2 – Medium	Significant, or potential to be severe, cybersecurity concern, or significant impact on business operations	1. Executive management 2. Relevant IR stakeholders 3. Third parties 4. Information security	1. 1 – 2 hours 2. As necessary 3. As necessary 4. Immediately
3 – Low	Minimal, with potential to be significant, cybersecurity concern or impact on business operations	1. CIRT or CERT	1. Immediately

Table 47: Escalation and notification matrix example

Insider threat – The card shark[19]

The situation

While most attacks come from outside sources such as hacking or spear phishing, we occasionally see attacks coming from within a victim organization's own network environment.

One case involved payment card data compromise, with unauthorized automated teller machine (ATM) withdrawals that resulted in significant financial loss. The VTRAC | investigative response team was engaged to conduct a payment card industry (PCI) forensic investigation.

Investigative response

After arriving onsite, we were granted immediate access with no security or identification checks. This was unexpected and unusual, considering the circumstances. We were also informed that most of the staff we wanted to interview had been replaced, and that new hires were still getting familiar with the environment.

Our initial security information and event management (SIEM) log analysis identified a malicious system in the environment. This system was neither corporate-owned nor "known," raising multiple questions such as how the system made its way onto the network, where it was located, how it gained access into the PCI environment and why no one noticed the initial alerts.

All we had to go on was that a rogue system connected to the network, and indications that it had accessed critical PCI server databases and conducted unauthorized withdrawals. We still didn't know how the system came to be on the network or exactly how the attack occurred, so we focused on gathering more information.

We conducted interviews and collected technical information, such as the network topology, to fully scope the incident and identify possible intrusion vectors. This process revealed that the entire network structure was flawed from the ground up.

Despite a few internal firewalls, the network was essentially flat. In addition, full network access was available to any connected device due to the lack of even rudimentary access controls. In-place network monitoring was misconfigured, and while there was a SIEM in place, no one was reviewing and investigating alerts.

Notes:

[19] https://enterprise.verizon.com/resources/casestudies/2018/data-breach-digest-2018-the-card-shark.pdf

Insider threat – The card shark *cont.*

These fundamental design flaws across the network were an open door for attack – and made it trivial for a threat actor to fly under the proverbial radar.

We reviewed physical security controls at the location where the attacker's system connected during the attack. The location was a main data center, a large office building with a publicly accessible area.

To our surprise, the data center's access was secured with just a standard keyed door. Once inside, all offices were easily accessible. This lax security posture included no ID verification, no access control lists, and no one consistently occupying security desks. We quickly realized that accessing employee areas from public areas would be relatively easy due to weak physical security.

We also identified major flaws in the organization's digital security posture. These included easily guessable passwords, unchanged administrator account passwords, shared user and admin accounts, database access by default user accounts, and administrator privileges for every database user account.

Forensic analysis revealed an attacker with physical access used this suspect system to connect to an application server via an administrator account. The attacker generated scripts to manipulate the database, executing these on the night of the incident. Unfortunately, the suspect system was never found and was not available for analysis.

Lessons learned

In the end, it was obvious what led to the compromise:

- **Step 1**: Gain physical access. Weak physical security controls allowed the attacker to introduce an unauthorized system into the organization's premises.
- **Step 2**: Obtain logical access. Insufficient network access controls and poor network segmentation enabled the attacker to connect to the internal network, and access critical server and database systems.
- **Step 3**: Leverage privileged access. Weak password policies enabled the attacker to log on with admin privileges and manipulate the target databases to complete the attack.

Finally, lack of proper network monitoring prevented the organization from detecting the attacker at an early stage.
At the end of this investigation, it remained unknown whether the attacker had insider support. Potential answers to many questions vanished with the undiscovered suspected system.

Notes:

Countermeasure solutions

Detection and response

- Properly configure network security monitoring software (e.g., SIEM, Intrusion Detection System (IDS)) based on use cases; regularly review outputs and events
- Train employees on cybersecurity policies and procedures, and sensitize them to report suspicious cybersecurity and physical security incidents; conduct periodic mock incident tabletop exercises to test responders and stakeholders
- Include an IR playbook within the IR Plan; hold After Action Reviews (AARs) after incidents and capture lessons learned for future improvements
- Proactively assess for payment card fraud; contact acquirers and card brands; conduct internal checks and audits (cover all 12 PCI DSS requirements); engage law enforcement when the time is right

Mitigation and prevention

- Restrict physical access: Employ physical security measures such as identity cards, card swipes and turnstiles; further restrict access to sensitive areas; monitor via closed-circuit camera system; prohibit personal devices on the network
- Restrict logical access: Segment the network; prevent rogue system connection to the network; implement multi-factor authentication (MFA); use complex passwords for all user accounts; apply the principle of least privilege for access to sensitive data

Phase 3 – Containment and eradication

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

Using Cyber Threat Intelligence

As with all intelligence, cyber threat intelligence (CTI) – or more formally a CTI program – involves gaining insight into data breaches and cybersecurity incidents. CTI allows organizations to make informed decisions to protect their environments and respond to attacks. Analysis often hinges on threat actor tactics, techniques and procedures (TTPs), motivations, and access to intended targets. By studying these TTPs, it is often possible to make informed and forward-looking strategic, operational, and tactical assessments.

Use cases

- **TTP reuse** – Given the reuse of attack TTPs, whether you are dealing with an opportunistic attack or something specifically targeting your organization, adversaries will likely use something that has been seen before.
- **MTTD and MTTR** – Two key metrics for measuring the effectiveness of an organization's security capabilities are its mean time to detect (MTTD) and mean time to respond (MTTR). The MTTD is the average time it takes an organization to identify threats that could impact the organization. The MTTR is the average time it takes an organization to analyze the threat and mitigate any risk. Having a robust CTI program allows an organization to substantially reduce both metrics.
- **Active controls** – Threat intelligence gives you information to block malicious activity using active controls. When blocking traffic you must be very careful, but some activities are malicious and should be stopped immediately. These decisions should be carefully analyzed from a risk standpoint.
- **Security monitoring** – A shortcoming of security monitoring is the need to know what threat you are facing. CTI expands your vantage point, using indicators found by other organizations to look for undetected malicious activity within your environment.
- **Incident response** – Once adversary activity is detected, you have a lot of ground to cover to find the root of the attack and quickly contain it. CTI offers clues about business risk of an attack, with perspective on attackers, motives and tactics – so your organization can focus its response.

Containing and eradicating

Assessment observations

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

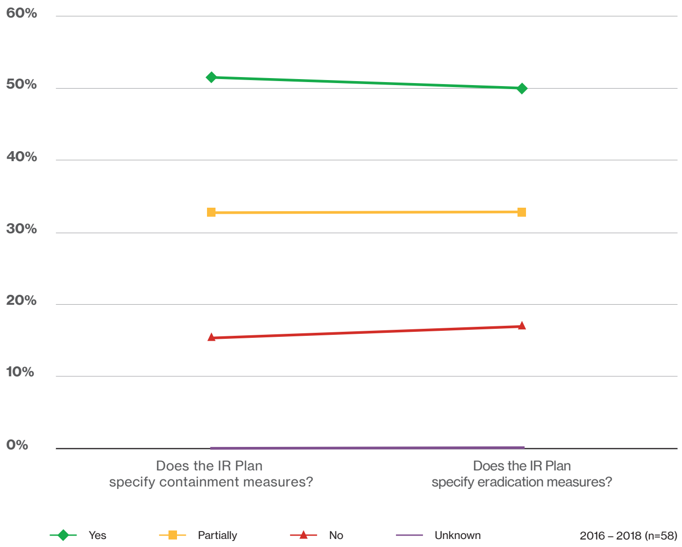


Figure 48: Plan assessments | Phase 3 - Containing and eradicating

Assessment recommendations

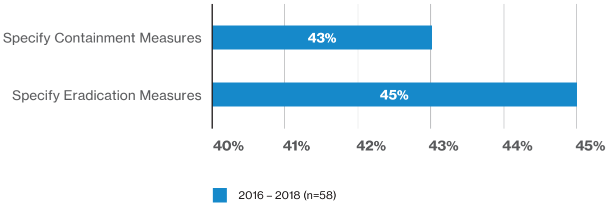


Figure 49: Plan assessments | Phase 3 - Containing and eradicating

For assessment recommendations, specifying containment measures (43%) and specifying eradication measures (45%) were made.

Simulation recommendations

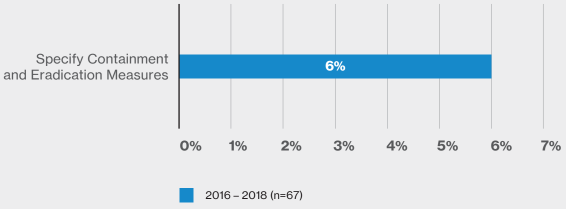


Figure 50: Breach simulations | Phase 3 - Containing and eradicating

Specifying containment and eradication measures (6%) were recommended for containing and eradicating following the breach simulations (2016 – 2018).

A deeper dive – Critical assets

Assessment observations

During the previous year (2018), only 7% of assessed IR Plans provided critical asset response requirements (with 57% providing no critical asset response requirements). Similarly, only 7% specified critical asset logging and monitoring (with 79% specifying no critical asset logging monitoring).

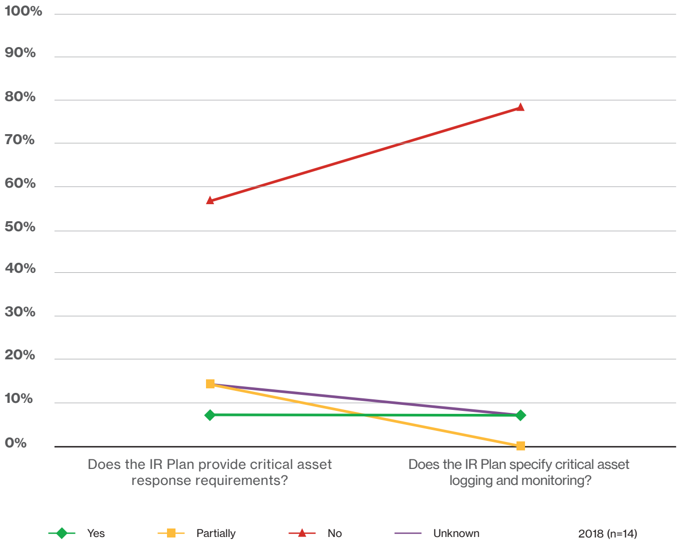


Figure 51: Plan assessments | Phase 3 - Critical assets

Assessment recommendations

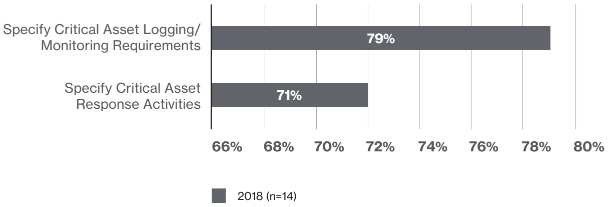


Figure 52: Plan assessments | Phase 3 - Critical assets

During the previous year (2018), for critical assets in assessed IR Plans, the most prevalent recommendation was specifying critical asset logging and monitoring requirements (79%), followed by specifying critical asset response activities (71%).

Simulation recommendations

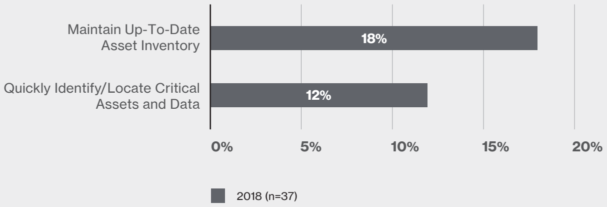


Figure 53: Breach simulations | Phase 3 - Critical assessments

For breach simulations over the previous year (2018), critical asset recommendations included maintaining up-to-date assets inventory (18%) and quickly identifying and locating critical assets and data (12%).

ICS attack – The eclectic slide[20]

The situation

It was late in the evening when I got the call: “We’re going to need you to come into the office.” As Security Operations Center (SOC) Lead Analyst in critical infrastructure protection (CIP), I was used to such after-hours calls. What was unusual was the next statement: “Law enforcement called and they believe we may be compromised.”

When I arrived, the office was in a frenzied state. Because it was not clear how (or even if) we’d been compromised, we assumed the worst and avoided communicating through typical corporate channels. This made it difficult to share information with colleagues not physically present in the office.

We were also informed that any new information we found or received from the FBI was “TLP Red” and couldn’t be shared publicly.

The first indicator of compromise (IoC) was an email address, which law enforcement believed was involved in a spear phishing attack against various organizations in the energy sector.

Sure enough, after searching our email appliance, we found that this specific address had sent several emails. Each targeted an executive or lead engineer at our electrical plant.

The emails came with an attached Microsoft Word “resume” for recipients to open. I reviewed the attachment in our malware analysis environment and saw nothing out of the ordinary – no web links, no macros and no additional processes being spawned. I called the VTRAC | Investigative Response Team to assist.

Investigative response

VTRAC investigators examined the suspicious attachments and soon presented their findings. They found that the threat actor was using a Microsoft Word template hosted on the internet and communicating with a command and control server. This technique, later coined “template injection” was a novel way of leveraging the software to download a malicious payload.

When opened, the document “searched” for a specific, malicious template via the server message block (SMB) protocol hosted on the threat actor’s server.

Notes:

[20] https://enterprise.verizon.com/resources/casestudies/2018/data-breach-digest-2018-the-peeled-onion.pdf

ICS attack – The eclectic slide *cont.*

Once downloaded, the malicious template used macros to spawn a Microsoft PowerShell (command prompt) instance to steal user account credentials.

It turned out that the targeted users had not corresponded with the threat actor. However, they all had very public profiles on a popular professional social media networking website. The threat actors likely used these profiles to select their targets.

Armed with this additional information, we immediately asked targeted users to change their account passwords. We then forensically collected the systems and volatile data associated with these users.

Some engineers had access to highly privileged operational technology (OT) systems within the plant. This was an issue, as none of the SOC analysts had taken the North American Electric Reliability Corporation (NERC) CIP training required to access the plant systems.

With time of the essence, and no SOC analyst accessing these systems, we created a PowerShell script to search for IoCs, and then loaded them on to a USB device. We identified a plant engineer with the appropriate level of system access, made a one-time exception and had him plug the USB device into the OT systems to run the script and scan for any IoCs.

Lessons learned

While we found no additional IoCs, we identified several improvements that could be made to our incident response approach. During our after-action review, we set out to accomplish these enhancements as soon as possible.

First, we set up an alternate communication method separate from the corporate network. This provided the SOC analysts with a way to communicate securely should our corporate network be compromised.

Next, we educated end-users to be careful with information they share online, as threat actors can use it to identify high-priority attack targets. Then we implemented firewall rules to block external SMB connections to unknown public addresses.

Last but not least, we made a requirement that all SOC analysts and cybersecurity incident responders take required NERC CIP training and undergo additional background screening as an enhanced security measure.

Notes:

Countermeasure solutions

Detection and response

- Establish a method for reliable, secure, alternative communications before a cybersecurity incident occurs; incorporate this into the IR Plan
- Increase logging and alerting for configuration changes, to include user account creation and modification; enable enhanced logging for PowerShell script triggered actions
- Comply with industry training and certification requirements; train SOC analysts and incident responders to respond in the Industrial Control System (ICS) environment

Mitigation and prevention

- Isolate OT networks; use dedicated OT systems; disable email and internet access, and access to networks at security-levels lower than the OT environment
- Implement firewall rules blocking SMB connections to unknown public internet spaces; add detections for Microsoft Office and other user applications spawning PowerShell child processes
- Sensitize employees to the security implications of posting sensitive information on social networking sites

Phase 4 – Collection and analysis

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

Top five victim-controllable investigative challenges

In previous publications such as the Data Breach Digest and Insider Threat Report, we've presented "Top five victim controllable investigative challenges." We've included these oldies-but-goodies as they continue to consistently appear in our investigations and plague incident response efforts. They include:

- **Logs, logs, logs** – Specifically, non-existence or not enough (rolling over too quickly), or difficulty in promptly locating or retrieving
- **Network topologies and asset inventories** – Lacking or being severely outdated
- **Baseline images and trusted processes** – Lacking entirely, being inaccurate or outdated
- **"Dual-use" tools** – Tools (e.g., PsExec, PowerShell) left on the system prior to its breach (storing them in the Windows Recycler isn't a security option), or with no detection of their use
- **Self-inflicted anti-forensics** – Rebuilding systems first, then calling forensic experts; containing and eradicating but not properly documenting actions; pulling the power cable and not the network cable; and shallow investigations by unqualified IT team members

Collecting and analyzing

Assessment observations

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

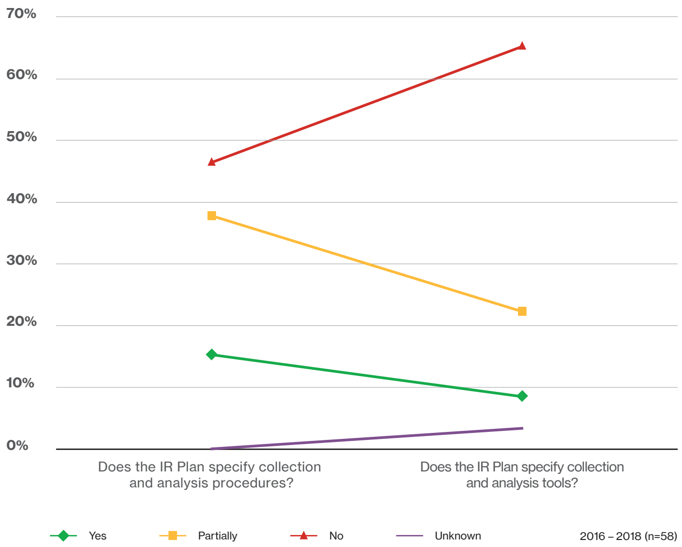


Figure 54: Plan assessments | Phase 4 - Collecting and analyzing

Assessment recommendations

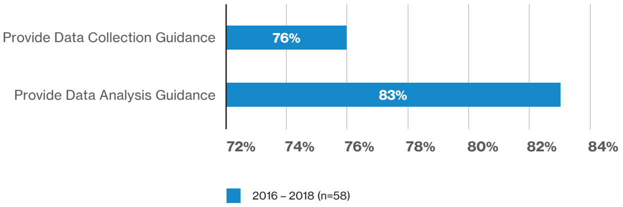


Figure 55: Plan assessments | Phase 4 - Collecting and analyzing

For collecting and analyzing, two recommendations were made for assessments: providing data analysis guidance (83%) and providing data collection guidance (76%).

Simulation recommendations

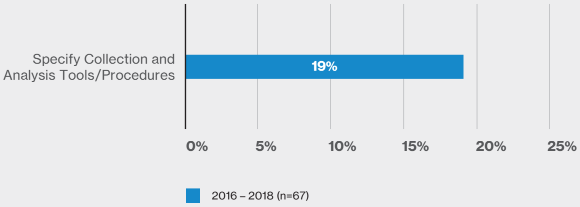


Figure 56: Breach simulations | Phase 4 - Collecting and analyzing

For breach simulations (2016 – 2018), the recommendation for collecting and analyzing was specifying collection and analysis tools and procedures (19%).

Data breaches in the cloud

The white paper “CISO’s Guide to Cloud Security: What to know and what to ask before you buy,”[21] provides a four-step process on choosing a cloud security platform. Step 1 – Assess your situation; Step 2 – Define your requirements; Step 3 – Identify your use cases; Step 4 – Determine metrics for success. For Step 3, key questions to ask for typical use cases include:

Use case	Questions to ask
Intrusion detection	• Does the product use advanced techniques like machine learning, custom threat intelligence, cross-customer analysis, and automated retrospective analysis to complement signatures and rules to reduce false positives? • Can it distill thousands of alarms and prioritize them for rapid investigations with one-click access to full-packet capture (PCAP) data? • Will it provide investigators a full history of a breach beyond the PCAP that triggered an event? • Is it capable of correlating suspicious activity with security events found by other products in your stack for context on why an event was generated? • Does it provide pervasive visibility on any network segment, including those not owned by the organization, such as the public cloud?
Security analytics	• Can the cloud security platform you’re evaluating make information and analysis available on-demand for effective forensic investigation and incident response? • Can it visualize millions of data points to make it easier for analysts to tease out not-yet-identified attacks buried in massive amounts of data? • Does it provide sophisticated analytics for any network, whether traditional enterprise, cloud, industrial control operational technology, IoT or 5G network? • Does it take a data-centric approach to detection by training machine learning models with billions of attributes? • Are integration points available to infuse analysis data from other security-stack products for better context into events and observations?
Incident response	• Can the cloud security platform you’re evaluating provide pervasive visibility from the network to the endpoint, for investigations free from blind spots? • Does it provide an unlimited, full-fidelity forensic window correlated with data from complementary security products? • Does it include a robust feature set, and can it work with the products in your existing security stack to help shorten the detection-investigation-resolution workflow?
Threat hunting	• Can the cloud security platform you’re evaluating capture full-fidelity PCAP and store it in the cloud long enough for threat hunters to access to data beyond breach windows? • Can it build a unified, highly contextual, and easily searchable haystack that provides threat hunters with the depth of information they need to test their hypotheses? • Is it capable of high-speed, on-demand analysis so threat hunters can build and test complex searches of thousands of attributes quickly, even across massive data sets? • Does it visually provide threat hunters instant access to nearly infinite points of data without having to pivot between multiple user interfaces?

Table 57: Cloud security platform use cases

[21] https://enterprise.verizon.com/resources/whitepapers/cisos-guide-to-cloud-security-final.pdf

Evidence handling

Assessment observations

Of assessed IR Plans (2016 – 2018), only 26% fully specified (and 36% partially specified) evidence-handling procedures and 21% fully specified (and 24% partially specified) evidence submission and chain of custody forms use.

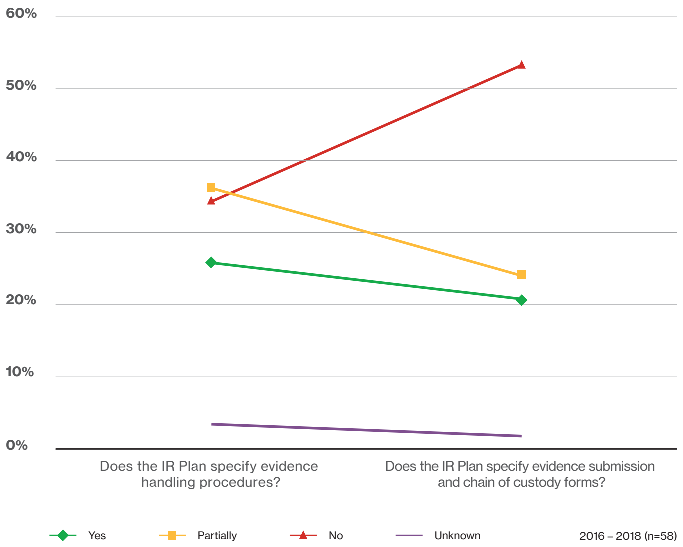


Figure 58: Plan assessments | Phase 4 - Evidence handling

Assessment recommendations

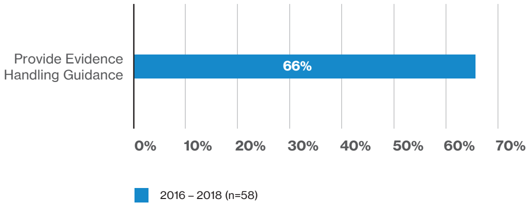


Figure 59: Plan assessments | Phase 4 - Evidence handling

For assessments, providing evidence-handling guidance was recommended (66%).

Simulation recommendations

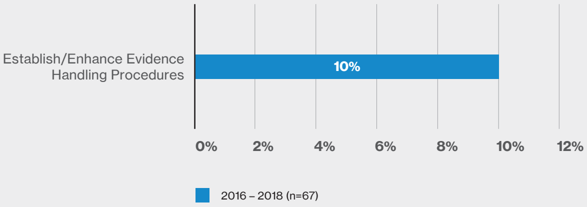


Figure 60: Breach simulations | Phase 4 - Evidence handling

For breach simulations (2016 – 2018), establishing and enhancing evidence-handling procedures (10%) was recommended.

Cyber-espionage – The katz-skratch fever[22]

The situation

While espionage has existed for thousands of years, cyber-espionage—threat actors targeting sensitive or proprietary data on digital systems—is still a relatively new concept. Recently, a manufacturing customer engaged the VTRAC | Investigative Response Team after it was contacted by law enforcement about a possible data breach.

The Chief Information Security Officer (CISO) was notified that several foreign IP addresses might have been communicating with systems inside his environment. The CISO requested we immediately report to headquarters to investigate these suspicious IP addresses.

Investigative response

Our VTRAC I Investigative Response Team understood the potential severity as we deployed to the customer's headquarters the next day. After an initial briefing with the CISO, we started our triage of several in-scope servers and other equipment believed to be involved in this incident. After collecting several memory dumps and full disk images, we reviewed the digital evidence.

That evening, we discovered a unique software program on one of the primary systems. Well-known by penetration testers and IT security professionals, Mimikatz is a powerful credential theft tool. It scrapes memory of the process responsible for Microsoft Windows Local Security Authority Subsystem Service (LSASS) authentication, revealing clear text passwords and NT LAN Manager (NTLM) hashes.

Notes:

[22] https://enterprise.verizon.com/resources/casestudies/2018/data-breach-digest-2018-the-katz-skratch-fever.pdf

Cyber-espionage – The katz-skratch fever *cont.*

With this information, the threat actor could traverse multiple systems in a network. Knowing this was a critical piece of the investigative puzzle, we immediately shared the file's metadata with our VTRAC | Cyber Intelligence Team.

By the next morning, the VTRAC intelligence analysts informed us this file was routinely used by a specific nation-state to attack U.S. companies. Additional queries revealed the threat actor had intentionally targeted one employee, a senior IT system administrator, who had access to multiple servers including domain controllers across the engineering division.

The investigation also revealed a key component of the attack. Specifically, the system administrator received a phishing email about his 401(k) retirement plan, which appeared to originate from his plan administrator. The email contained a PDF attachment, which upon opening, silently installed Mimikatz.

Lessons learned

To summarize the lessons learned from this engagement, recommendations were made for mitigation and prevention, as well as for detection and response.

Notes:

Countermeasure solutions

Detection and response

- If not already involved, engage law enforcement when the time is right, as well as third-party investigators when applicable
- Collect access logs to key servers and email; prior to system shutdown, collect in-scope volatile data and system images; examine quickly
- Use internal and external intelligence resources to develop actionable intelligence on threat actor modus operandi and IoCs

Mitigation and prevention

- At least annually, provide users with cybersecurity awareness training; emphasize awareness and reporting suspicious emails
- Make external emails stand out; prepend markers to the “Subject:” line indicating externally originated emails
- Move beyond single-factor authentication and implement multi-factor authentication; require virtual private network (VPN) access for remote connections to the corporate environment

Phase 5 – Remediation and recovery

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

A brief VERIS framework refresher

The VERIS (Vocabulary for Event Recording and Incident Sharing) framework is a resource for incident response assessment and metrics comparison. Besides this publication, VERIS serves as a common contextual database answering the who (threat actors), what (victim assets), why (threat motives) and how (threat actions) for our cybersecurity incidents and data breaches.

VERIS provides a common language for describing incidents and breaches in a structured and repeatable manner. Learn more here:

- **github.com/vz-risk/dbir/tree/gh-pages/2019** – DBIR figures and figure data
- **veriscommunity.net** – Information on the framework with examples and enumeration listings
- **github.com/vz-risk/veris** – The full VERIS schema
- **github.com/vz-risk/vcdb** – Access the VERIS Community Database on publicly disclosed breaches
- **http://veriscommunity.net/veris_webapp_min.html** – Record your own incidents and breaches

Remediating and recovering

Assessment observations

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

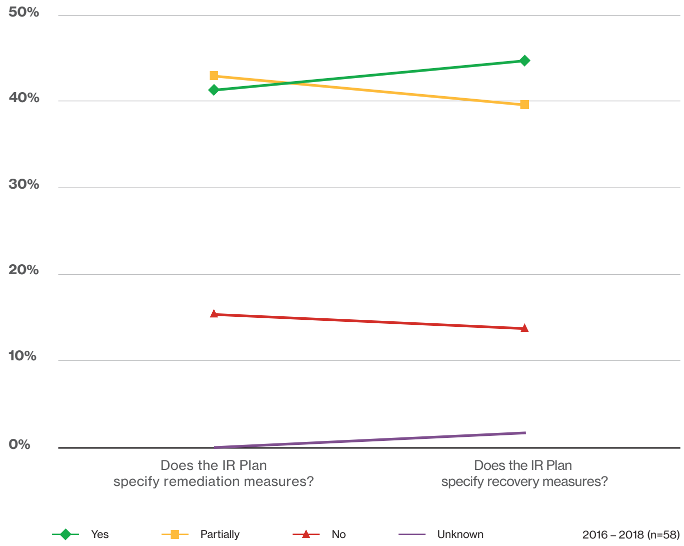


Figure 61: Plan assessments | Phase 5 - Remediating and recovering

Assessment recommendations

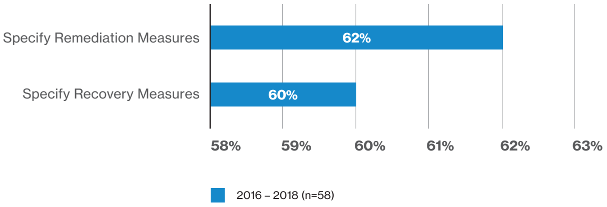


Figure 62: Plan assessments | Phase 5 - Remediating and recovering

Recommendations for remediating and recovering for assessments included specifying remediation measures (62%) and specifying recovery measures (60%).

Simulation recommendations

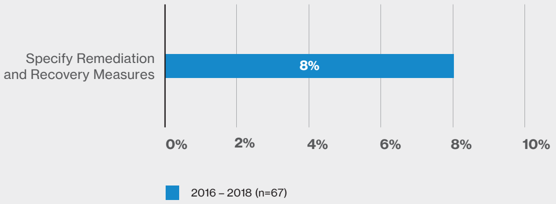


Figure 63: Breach simulations | Phase 5 - Remediating and recovering

Specifying remediation and recovery measures (8%) was recommended for breach simulations (2016 – 2018).

Cloud storming – The slivered lining[23]

The situation

It was a normal workday when I inspected the alarmed access and egress points at our corporate office. As I was walking through the hallways, I received a phone call from law enforcement. The officer informed me that certain systems on our network were likely compromised, because they were contacting an IP address identified as malicious.

With a timeframe and the malicious IP address in hand, I engaged our Information Technology (IT) Security team as well as our Chief Information Security Officer (CISO). Our initial network review revealed two systems – one in California and one in Virginia – communicating with the malicious IP address.

Investigative response

The IT Security team determined these two systems contained intellectual property that could severely affect our business if exposed to competitors. Our CISO triggered our retainer service with the VTRAC | Investigative Response Team, bringing them to assist with the investigation.

Within 24 hours, the VTRAC investigators were onsite at each data center to collect evidence from the two systems. Using the leads provided by our IT Security team, the VTRAC investigators identified an active open source remote access trojan (RAT). Malware analysis of the RAT revealed domain names resolving to the malicious IP address.

Leveraging the VTRAC | Cyber Intelligence team, they found the RAT was associated with an advanced persistent threat (APT) group. The APT was commonly associated with attacks aimed at stealing intellectual property and leveraging managed service providers (MSPs) as attack vectors. The MSP cyberattack stream was essentially:

- **Step 1**: Infiltrate MSP
- **Step 2**: Compromise MSP accounts
- **Step 3**: Choose victim from MSP customer pool
- **Step 4**: Gain access to victim network
- **Step 5**: Exfiltrate intellectual property via MSP network

With a list of APT-associated indicators of compromise (IoCs), our IT Security team quickly scanned our network for other potentially compromised systems. The scans identified multiple infected systems. Even worse, many infections dated back a few years.

Notes:

[23] https://enterprise.verizon.com/resources/casestudies/2018/data-breach-digest-2018-cloud-storming.pdf

Cloud storming – The slivered lining *cont.*

The most common malware found by the scans were backdoor tools used by the APT to maintain persistence on the network. Further analysis found multiple compromised user accounts, including administrator accounts. In addition, the threat actors were observed accessing our network via an IP address associated with our MSP.

VTRAC investigators determined the threat actors had leveraged our MSP accounts and network to gain access into our environment. This also correlated to attack vectors used by the APT.

With evidence pointing to an APT attack, and given the lengthy time of compromise, it was highly possible other systems in our network (with various credentials) were at risk. Most important, it was possible that our intellectual property was already being exfiltrated.

We set about identifying and then rebuilding all affected systems. For those areas of the network we found "lacking in adequate visibility," we expanded our logging and monitoring capabilities.

We decided that an effort to understand the full extent of the threat actors' actions in our network would have been too resource-intensive. So, we committed our efforts to determining whether data exfiltration had occurred and to securing the company's network. Our containment, eradication and remediation efforts succeeded, as we observed no additional APT-related activity in our network after the initial detection.

Although the investigation uncovered no evidence of data exfiltration, given the time we were compromised, our executives were concerned the threat actors may have accessed our intellectual property. We continue to work with the VTRAC investigators to monitor relevant online forums and marketplaces on the dark web to see if any of our data ends up in the public or available for sale by the threat actors.

Lessons learned

A call from law enforcement turned into a major incident that could have put our company in jeopardy. Even though our stakeholders responded, we still learned several lessons from this incident.

Notes:

Countermeasure solutions

Detection and response

- Proactively review logs of all internet-facing systems and applications; conduct threat-hunting activities; collect and analyze affected systems and associated system logs
- Employ a file integrity monitoring (FIM) solution to assist with detection efforts; employ an intrusion detection system (IDS); collect and analyze network logs
- Take affected systems offline; restore systems from baseline images and rebuild all affected systems; expand network logging and monitoring capabilities for areas lacking in network visibility
- Leverage threat intelligence; consult with legal counsel; contact law enforcement when the time is right

Mitigation and prevention

- Systematically monitor and test security posture from all angles; provide additional security and monitoring on critical systems; conduct periodic threat-vulnerability scanning
- Review, reconcile, manage and monitor all third-party account access
- Enhance user account security by requiring regular password changes, including local administrator accounts; monitor and manage privileged accounts
- Harden systems; disable and remove unnecessary applications; create baseline images; classify critical assets

Phase 6 – Assessment and adjustment

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

Measuring incidents and response

Metrics track incident occurrences and response activities for senior management. In turn, these metrics can offer insight into cyberattack trends, the need for additional resources, training gaps, and so on.

Metrics also help establish key performance indicators (KPIs) to measure how incident response supports key business objectives as part of an organization's cybersecurity strategy. Examples of cybersecurity incident and response metrics are:

- **# Incidents/year** – Total incidents per year
- **# Incidents by type/year** – Total incidents by category (priority, impact, urgency) per year
- **# Hours/incident** – Total resolving incident and incidents handled within the Service Level Agreement for that incident
- **# Days/incident** – Total time spent resolving incident
- **Monetary cost/incident** – Total estimated monetary cost per incident, including containment, eradication, remediation, and recovery, as well as collection and analysis activities
- **# Systems affected/incident** – Total systems affected per incident

Lessons learned

Assessment observations

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

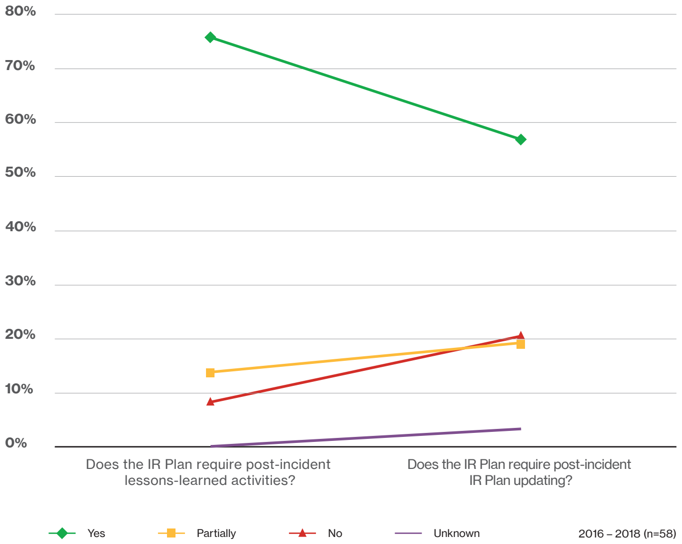


Figure 64: Plan assessments | Phase 6 - Lessons learned

Assessment recommendations

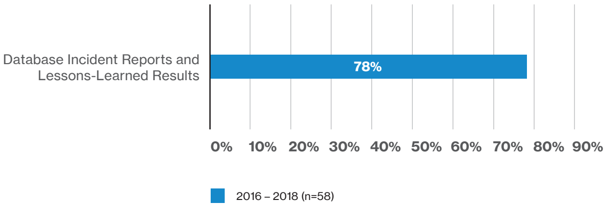


Figure 65: Plan assessments | Phase 6 - Lessons learned

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

Simulation recommendations

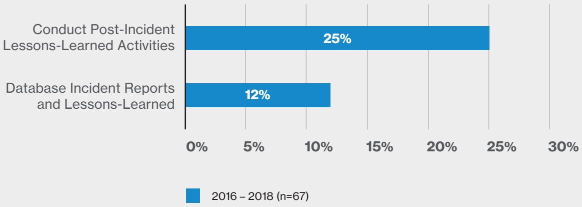


Figure 66: Breach simulations | Phase 6 - Lessons learned

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

Measuring success

Assessment observations

In terms of measuring success of assessed IR Plans (2016 – 2018), only 24% fully required (and 26% partially required) data and reporting retention. Similarly, only 24% fully required (and 12% partially required) incident and response metrics tracking.

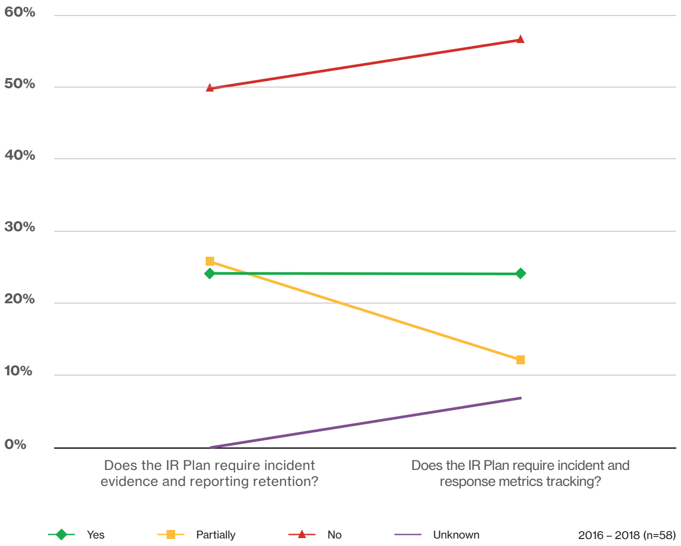


Figure 67: Plan assessments | Phase 6 - Measuring success

Assessment recommendations

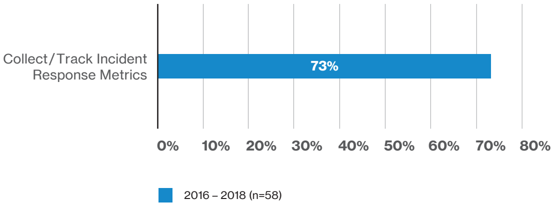


Figure 68: Plan assessments | Phase 6 - Measuring success

Collecting and tracking incident response metrics (73%) was recommended for assessments.

Simulation recommendations

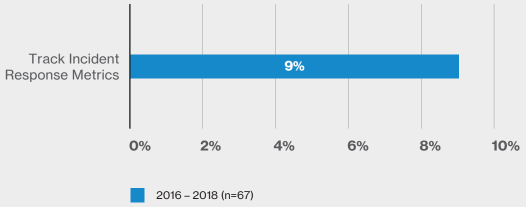


Figure 69: Breach simulations | Phase 6 - Measuring success

For breach simulations (2016 – 2018), tracking incident response metrics (9%) was recommended in terms of measuring success.

Takeaways

Now that you've finished the entire 2019 VIPR Report, we want you to have the most important takeaways. Here are our top 10 IR Plan assessment and top 10 breach simulation recommendations.

Assessment recommendations

In looking at overall IR Plan assessment recommendations, defining tactical response qualifications (85%), providing data analysis guidance (83%), citing external cybersecurity response governance and standards (78%), and databasing incident reports and lessons learned results (78%) top the list.

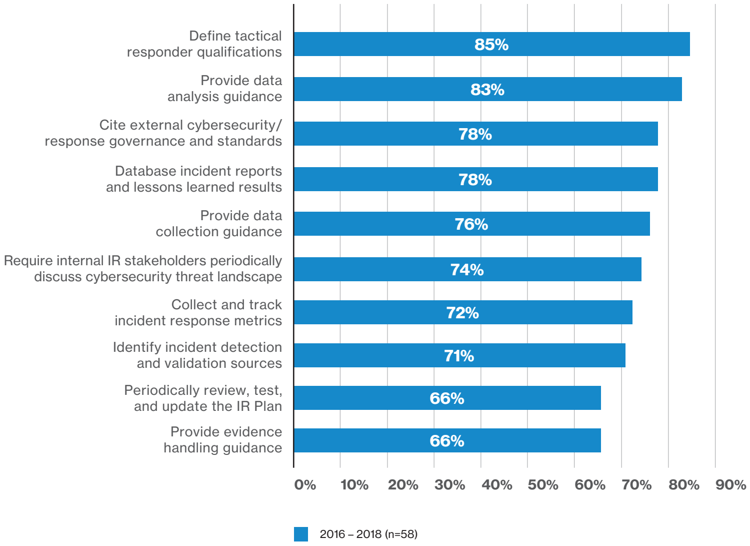


Figure 70: Plan assessments | Top 10 recommendations

Simulation recommendations

For breach simulation recommendations, maintaining an up-to-date, unified IR Plan (30%), creating IR playbooks for specific incidents (30%), establishing internal escalation protocols (30%), and defining internal IR stakeholder roles and responsibilities (27%) top the list.

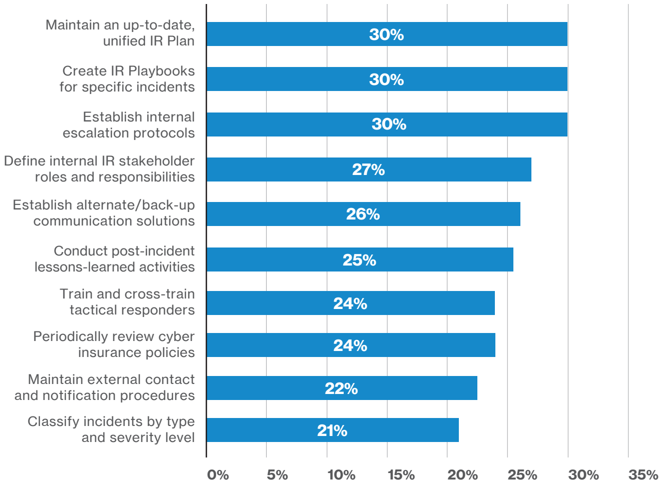


Figure 71: Breach simulations | Top 10 recommendations

Takeaways *cont.*

Here are our top 20 takeaways for building an effective and efficient breach response capability and a 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 periodically discuss 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. Feed lessons-learned results back into the IR Plan 19. Establish data and document retention policy 20. Track incident and incident response metrics

Table 72: Top 20 key takeaways

Appendix A – Countermeasure worksheet

Phase	Countermeasure
1. Planning and preparation	
2. Detection and validation	
3. Containment and eradication	
4. Collection and analysis	
5. Remediation and recovery	
6. Assessment and adjustment	
0. Mitigation and prevention	

Table 73: Breach simulation countermeasure worksheet

Appendix B – IR stakeholders

IR stakeholders fall into three groups: internal IR stakeholders, tactical responders (a subset of internal IR stakeholders) and external entities.

Internal IR stakeholders

Internal IR stakeholders consist of management and hands-on tactical responders.

Role	Responsibility
Chief Information Officer	Responsible for enterprise Information Technology (IT) strategy, networks, systems and applications for an organization
Chief Information Security Officer	Manages cybersecurity strategic goals, personnel allocation, infrastructure implementation, policy enforcement, emergency planning
Legal Counsel	Provides legal advice and recommendations on cybersecurity incidents and response activities
Human Resources	Provides guidance and assistance for cybersecurity incidents involving employee activity or employee personally identifiable information (PII)-related breaches
Corporate Communications	Manages internal and external communications for cybersecurity incidents
Incident Commander	Leads tactical responders (see Appendix B - Tactical responders)
Information Technology/ Information Security	Manages aspects of information technology (IT) and information security
Physical Security	Assesses the impact of physical aspects of cybersecurity incident
Governance, Risk, Compliance	Evaluates the IR plan for Governance, Risk, Compliance (GRC) purposes
Data Privacy and Protection	Ensures sensitive and protected data (e.g., PII, protected health information (PHI), payment card information (PCI)) is identified, processed and secured under applicable laws and regulations
Data Loss Prevention	Monitors, detects, blocks sensitive data at-rest, in-use or in-motion through data loss prevention (DLP) solution
Business Continuity Planning	Implements business continuity planning (BCP) associated capabilities
Disaster Recovery Planning	Implements disaster recovery planning (DRP) and associated capabilities
Help Desk or Hot Line	Receives and communicates cybersecurity incident-related information
End Users	Serves as first line of cybersecurity defense; an incident detection trigger

Table 74: Internal IR stakeholders

Tactical responders

Tactical responders cover a wide range of technical specialties.

Role	Responsibility
Incident Commander	Leads tactical responders; represents tactical responders at stakeholder meetings; updates stakeholders on response progress
SOC Analyst	Monitors for, and initially responds to, cybersecurity incidents detected by the Security Operations Center (SOC)
CERT or CIRT Responder	Responds to, and handles, cybersecurity incidents as part of the computer emergency response team (CERT) or cyber incident response team (CIRT)
SIEM Technician	Manages and leverages security information and event management (SIEM) response and analysis capability
EDR Technician	Manages and leverages endpoint detection and response (EDR) solution
NDR Technician	Manages and leverages network detection and response (NDR) solution
Malware Reverse Engineer	Deconstructs malicious software (malware) to understand its capability and impact to an environment, asset or data
Internal Investigator	Investigates allegations of employee misconduct

Table 75: Tactical responders

Third parties

Third parties are external experts advising and providing support to internal IR stakeholders.

Role	Responsibility
Digital Forensics Firm	Supports the tactical responders with forensics investigation activities
Law Enforcement	Investigates cybersecurity incidents involving criminal activities
Security Vendors	Advises and assistance on cybersecurity and response solutions
Data Storage Providers	Hosts and stores data, back-ups and log data
Internet Service Providers	Provides internet connectivity
Cyber Insurance Carrier	Insures data breach and other cybersecurity incidents
Outside Counsel	Supports internal Legal Counsel with specialized legal advice
External Public Relations	Supports internal Corporate Communications and Public Relations
US-CERT or Regional CERT	Responds to cybersecurity incidents and analyzes threat actions
Industry ISACs	Shares physical threat, cybersecurity threat, and vulnerability information

Table 76: Third parties

Appendix C – Mobile device incident preparedness

The 2019 Verizon Mobile Security Index[24] provides countermeasures to implement and maintain mobile device security through assessing, protecting, detecting and responding.

		Baseline	Better	Best
Assess Understand your devices, your data, who has access and what the threats are	**Implement**	• Ensure mobile is included in all your security plans and policies • Understand risk factors including geo-location, industry, size and critical data streams • Understand and manage your employees' data usage	• Take a full accounting of your assets to determine risks and potential exploits • Track updates and patches, and coordinate deployment • Define guidelines for acceptable use, including file transfer	• Measure your environment against applicable regulatory frameworks • Establish a security-first employee focus and culture • Implement a risk evaluation and scoring framework
	Maintain	• Regularly assess defenses to confirm that detection capabilities meet set standard	• Test employee mobile security awareness at least once a year	• Perform regular, at least quarterly, 360-degree reviews of mobile threat landscape and security posture
Protect Harden assets, protect data and secure the emerging mobile perimeter	**Implement**	• Deploy a device enrollment policy • Implement a strong password policy and verify adherence • Limit Wi-Fi to approved networks • Prevent employees from installing apps downloaded from the internet • Establish formal policies for corporate-liable and bring your own device (BYOD) detailing employees' responsibilities	• Implement a unified endpoint management (UEM) system to preconfigure devices with approved apps, limit additions to company app store and set and manage policies • Deploy a private network solution to any device that gathers or accesses sensitive data • Leverage voice, messaging and file encryption solutions	• Implement device segmentation, keeping personal and work data and applications separate • Change device procurement policies to favor cellular over Wi-Fi • Develop governance policies for transferring data between IoT devices
	Maintain	• Regularly review access to systems and data	• Identify users out of compliance or misusing assets	• Use activity-based monitoring to block malicious behavior

[24] https://enterprise.verizon.com/resources/reports/2019/msi-2019-report.pdf

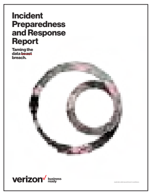
Appendix C – Mobile device incident preparedness *cont.*

		Baseline	Better	Best
Detect Identify vulnerabilities and anomalies quickly to enable speedy response to reduce impact	**Implement**	• Deploy mobile threat detection software to scan for vulnerabilities • Implement log monitoring to spot signs of attacks and device misuse	• Introduce a solution to identify and prevent complex phishing attacks– including those happening outside email • Implement processes to identify devices out of compliance	• Introduce data visibility and content control tools • Deploy secure productivity apps to protect collaboration • Implement secure IoT device visibility and management platform
	Maintain	• Provide regular security training on the dangers associated with mobile devices and how to spot warning signs of an incident	• Review apps to identify anomalies such as excessive permissions and potentially dangerous behavior like scanning corporate networks	• Use data loss prevention (DLP) tools to limit data transfer, provide early warning and enable forensics
Respond Remediate issues, recover operations and enable forensic analysis	**Implement**	• Implement policies to contain attacks by locking down private information and isolating infected, lost or stolen devices	• Create an IR Plan that informs employees of what to do in the event of an incident • Implement push messaging to tell users and admins what to do in the event of an incident	• Automate corrective actions to reduce response time and limit exposure • Implement employee-friendly policies and solutions tailored to BYOD security
	Maintain	• Remind employees how to report any suspicious activity – make it an easy-to-remember email address or phone number	• Exploit the complete range of unified endpoint management (UEM) capabilities to identify the full range of threats and trigger responses	• Run regular response exercises on areas of concern (e.g., phishing)

Table 77: 2019 Mobile Security Index Mobile Security – Baseline, better, best (excerpt, page 23)

Data breach and cybersecurity resources

Click on the cover below to view that report online

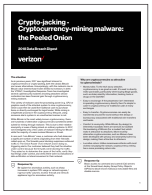

Incident Preparedness and Response Report
Taming the data beast breach.
verizon

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

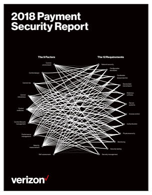
2019 Data Breach Investigations Report

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

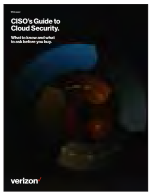
2019 Mobile Security Index: It's time to tackle mobile security.


Crypto-jacking - Cryptocurrency-mining malware: the Peeled Onion
2018 Data Breach Digest
verizon

2018 Data Breach Digest (18 scenarios)



2018 Payment Security Report


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

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.
verizon

5 Considerations for Evaluating a Modern Enterprise Security Platform

Download the Verizon Incident Preparedness and Response report
enterprise.verizon.com/resources/reports/vipr/