INCIDENT RESPONSE PLAYBOOK:

Empower Your Teams to Handle Modern Threats

Get the best practices for tackling inevitable threats to your most valuable data and assets in this guide to cybersecurity incidents.

Insight

Regardless of industry, organisations today face evolving, mounting threats from bad actors.

These events can lead to the loss or disruption of critical assets or functions, and ultimately impact the flow of business. Cybersecurity incidents are full-company disasters, and organisations need to plan accordingly because these events are unpredictable and remain ever-present threats.

The content of this guide was developed by experts in incident response based on extensive experience supporting organisations through security emergencies.

A look at the current cybersecurity landscape for organizations:[1]

49%

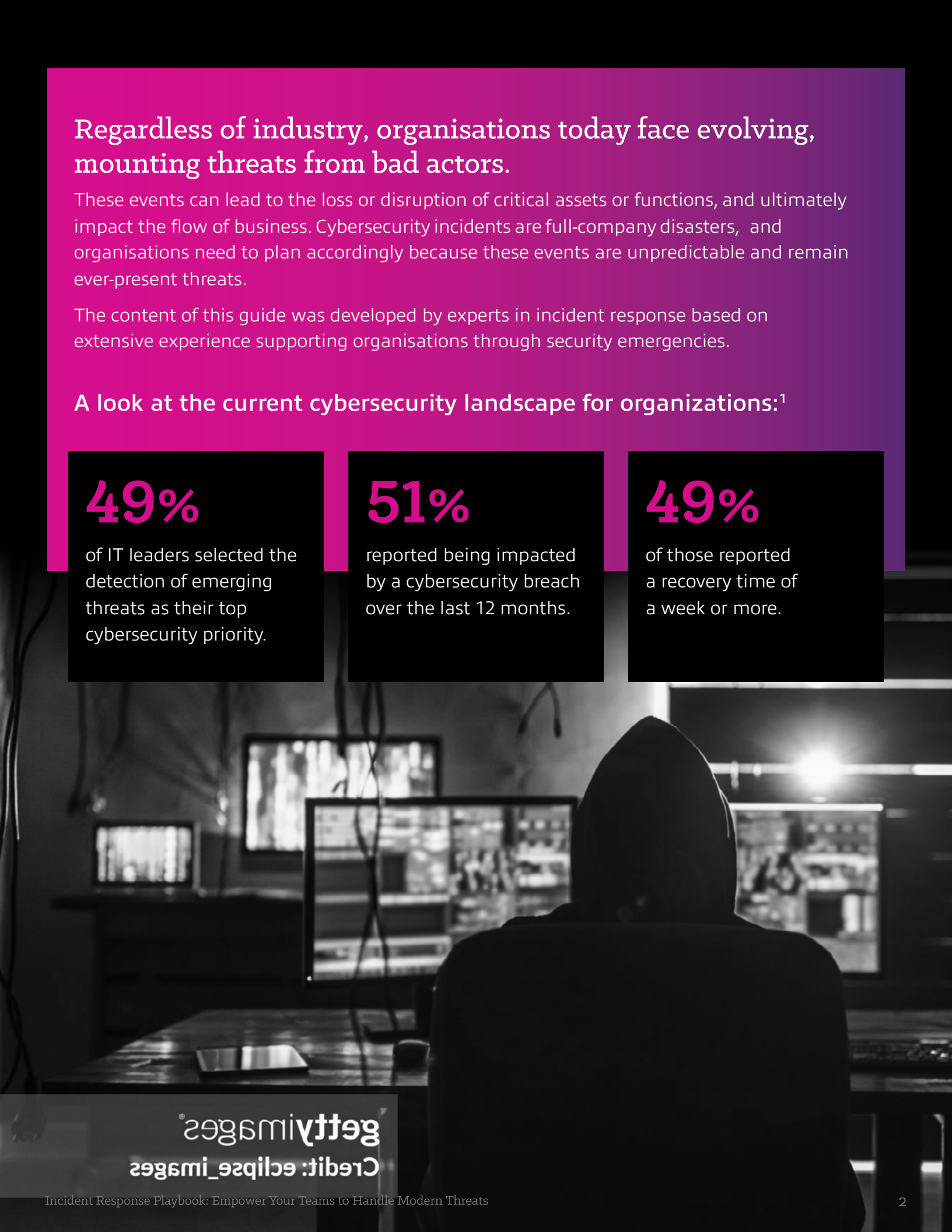
of IT leaders selected the detection of emerging threats as their top cybersecurity priority.

51%

reported being impacted by a cybersecurity breach over the last 12 months.

49%

of those reported a recovery time of a week or more.



gettyimages®
Credit: eclipse_images

Back to basics

Preparing for a cybersecurity event isn't just about practicing high-intensity scenarios; it's also about reflecting and validating your existing procedures. For backups, teams should regularly restore a random environment back into production. For virtual appliances that get patched but aren't easily backed up, it's important to know the exact versions needed for restoration. Lastly, your configuration management posture should be evaluated for routers, switchers, servers, loud balancers and more.

Always assume virtual appliances won't back up properly, and have an alternative:

Open Virtualisation Appliances (OVAs) and manuals should be on standby.

Configurations should be backed up automatically.

ISO or installation media should be readily available and archived to a secure location.

Cybersecurity response best practices

01

Storage of documentation and credentials

Keeping documentation and credentials safe and accessible during a cyber incident is critical to recovery efforts. The best practice is to store documentation in at least three isolated locations, including one that is entirely outside the environment, to ensure the information can be accessed even with a compromised environment. Additionally, there should be a system in place to review this documentation. A regular cadence, such as quarterly, should be set for this review and include the opportunity to simulate rebuilding systems as practice for potential incidents.

Some critical information to protect in this manner might include:

- Application owners and build documentation
- Domain Name System (DNS) records
- Network and appliance configuration details
- Operational and regulatory processes, which outline how often procedures are done and their importance to the function of the business. This includes less frequent activities that may occur weekly, monthly, quarterly or annually.
- which maps out each employee's proficiencies as they relate to supporting an incident response situation

02

Tabletop exercises

Critical to incident response preparedness is practice. With tabletop exercises, organisations can walk through scenarios, test their readiness and identify gaps in procedure. While it's advised to do these at least once a year, doing them once a quarter gives teams a better chance to address a variety of possibilities like different tasks, communications owners or shuffling of involved teammates. Teams should also practice compounding variables such as a natural disaster occurring right after an incident or more than one data loss event happening in rapid succession.

Tabletop exercises can also validate the following:

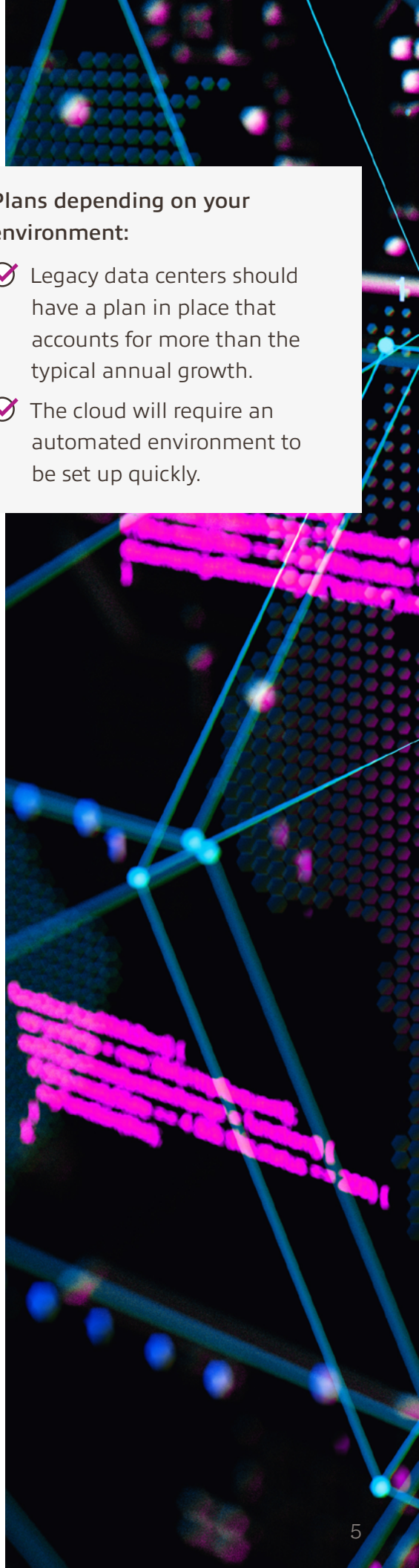
- If credentials and build book are updated
- Accuracy of automated responses
- Patch review plans
- Opportunity to red-team the outcome of the exercise

03 Capacity planning

Regardless of the operating environment, there is a possibility that in a cybersecurity event, a significant portion or infrastructure cannot be immediately reused. Additionally, if the origin of the threat is unknown, your team has no way of knowing if loss will occur as soon as you restore. As part of planning your incident response, it should be determined which members of the team can restore platforms, troubleshoot apps as issues arise and drive the forensic isolation of platforms. During an incident, leaders should also keep in mind a temporary ramp-up of labor will be needed until recovery efforts show to be successful.

Plans depending on your environment:

- Legacy data centers should have a plan in place that accounts for more than the typical annual growth.
- The cloud will require an automated environment to be set up quickly.



04 A deeper look at performance

For many organisations, planning for an impact on performance is usually based on the worst they typically experience from their environment at peak usage of their applications. However, the "worst" that is possible during a cybersecurity event will likely be different than what is seen in a fully functional environment. Instead, teams should evaluate performance and response plans based on the worst-case scenario, taking a security incident into account.

Put your performance to the ultimate test:

- Run a full restore of all systems at once.
- Simulate having no bandwidth available for your network.
- Run malware scans on all data restored.
- Push an influx of inbound makeup client data through APIs and Virtual Private Networks (VPNs).
- Mimic continued active threat activity such as Distributed Denial of Services (DDoS) or security probing.

05

Backup vs. replication

To set a strong cybersecurity posture, it's important for leaders and response teams to understand the difference between backup and replication as this is commonly misunderstood. A backup is used as a point-in-time copy of data. Replication, on the other hand, is designed to have a highly available environment. While it's true that replication is faster for recovery, depending on the circumstances and timing of the incident, the use of it for recovery can result in replicating the malware/security incident and forcing further downtime. Backups can save data loss up to a certain point in time, but they can take longer for restoration.

Having access to both methods will help diversify and support recovery efforts immensely. Organisations should also keep in mind that the most complex applications in their environment are often the ones that are hardest to restore based on the number of integrations, changes in owners, duration of the application in their environment and undocumented one-time processes.

Validated environments have:

- Storage snapshots
- Snapshot replication
- Isolated storage backup
- Immutable off-site storage

06

Communication management

Critical to response and recovery efforts is communication. Before an event occurs, an organisation should have a good idea of who will own the communication of different aspects of response. For example, who will communicate with executive teams and/or legal? Additionally, normal means of communication such as email might be unavailable, so alternatives need to be quickly accessible.

Communication best practices:

- Establish an emergency response plan.
- Have alternative form(s) of communication available and prepared to be deployed.
- Set expectations with stakeholders for recovery timeline and communication frequency ahead of an incident.
- Prioritise communication of response teams and deprioritise non-response-related communication.

07 Administrative access

While this may present a significant logistical challenge, you should assume your entire environment is impacted during a cybersecurity event, including VPNs, DNS, Active Directory® (AD), Multi-Factor Authentication (MFA) and more. With this in mind, the response team should have a standby plan in place with automated deployment that is only turned on for tests and real incidents.

Alternatives to compromised access:

- Air-gapping of access through jump boxes with local authentication
- A secondary authentication and authorisation system in place
- Logging and alarming for failed login attempts or other suspicious behavior
- Plans for accessing route, switch, storage, virtualisation configurations and more

08 The importance of automation

Automation doesn't just make day-to-day workflows easier; it can also be a huge help in the event of a cybersecurity incident. If automation is part of daily practice for release updates, it creates automated documentation of how your environment is configured. Credential management can be streamlined. Automation can also support the provisioning of environments, servers, containers and applications, which may be necessary if these systems are impacted by a cyber event. Organisations should make sure they understand how restoring application-specific data in complex applications such as Oracle, SAP or SQL Server® fits into automating these processes.

Incident response automation deploys machine learning technology to generate actionable insights like threat detection, analysis and response. These tools can help prevent and handle cybersecurity events while teams focus on other high-priority incident response tasks.

09

Business Continuity/Disaster Recovery (BC/DR) tests

In addition to tabletop exercises, BC/DR tests are immensely valuable to incident response teams in determining preparedness. Unlike tabletops, these are meant to actually exercise the process of restoration. Once a year, these exercises should be unscheduled to test the team's preparedness. When conducting this activity, new roles and a leader should be rotated each time to flex different skill sets in the group.
Most importantly, failure should be embraced as normal and a learning experience; in real-life incident response situations, there will be failures along the way, and it's the best way for teams to learn for next time.

BC/DR best practices:

Identify impacted systems and their importance.

Ensure crucial business processes are prioritised and uninterrupted.

Shuffle roles to enable different skill sets to shine.

Value failure as a learning experience.

10

Staffing and development

It goes without saying that incident response is one of the most stressful work environment scenarios. Preparing for an event goes beyond having systems in place; it also means preparing employees for the inevitable possibility of a real threat being carried out. Expectations should be established that outline different roles and how long individuals can work before handing off their tasks. Additionally, teams (including non-IT teams) should be trained in emergency response to help curb additional chaos that could ensue from an event.

Training tips:

- Set expectations around emergency situations and organisation response policies.
- Train non-IT teams to level the playing field and reduce spillover into other departments.
- Understand varying skill sets at your disposal and what could be valuable during recovery.

11

Documentation of cyber event response

During and after a cybersecurity incident, there should be documentation of the path to recovery. This documentation doesn't need to be formal, but it should include important details and commands that were run during the incident, as well as the reasoning behind the decisions that were made. This information can be used for future training, to guide recovery if a similar event occurs in the future or for a legal course of action.

What should be documented?

- Forensic elements of the cybersecurity incident
- What teammates completed which actions
- Why certain actions or decisions were made and their results
- What future fixes should be made or how the process differed from existing plans and documentation

Why Insight for your incident response support

A robust security strategy is more important than ever for organisations to stay ahead of sophisticated threats. Our end-to-end IT security services help companies bolster their security posture, respond to real-time threats and recover from incidents. With a roster of technical experts who have helped countless clients overcome cybersecurity challenges, your organisation can achieve the protection it needs to stamp out vulnerabilities.

How we help

Before an event

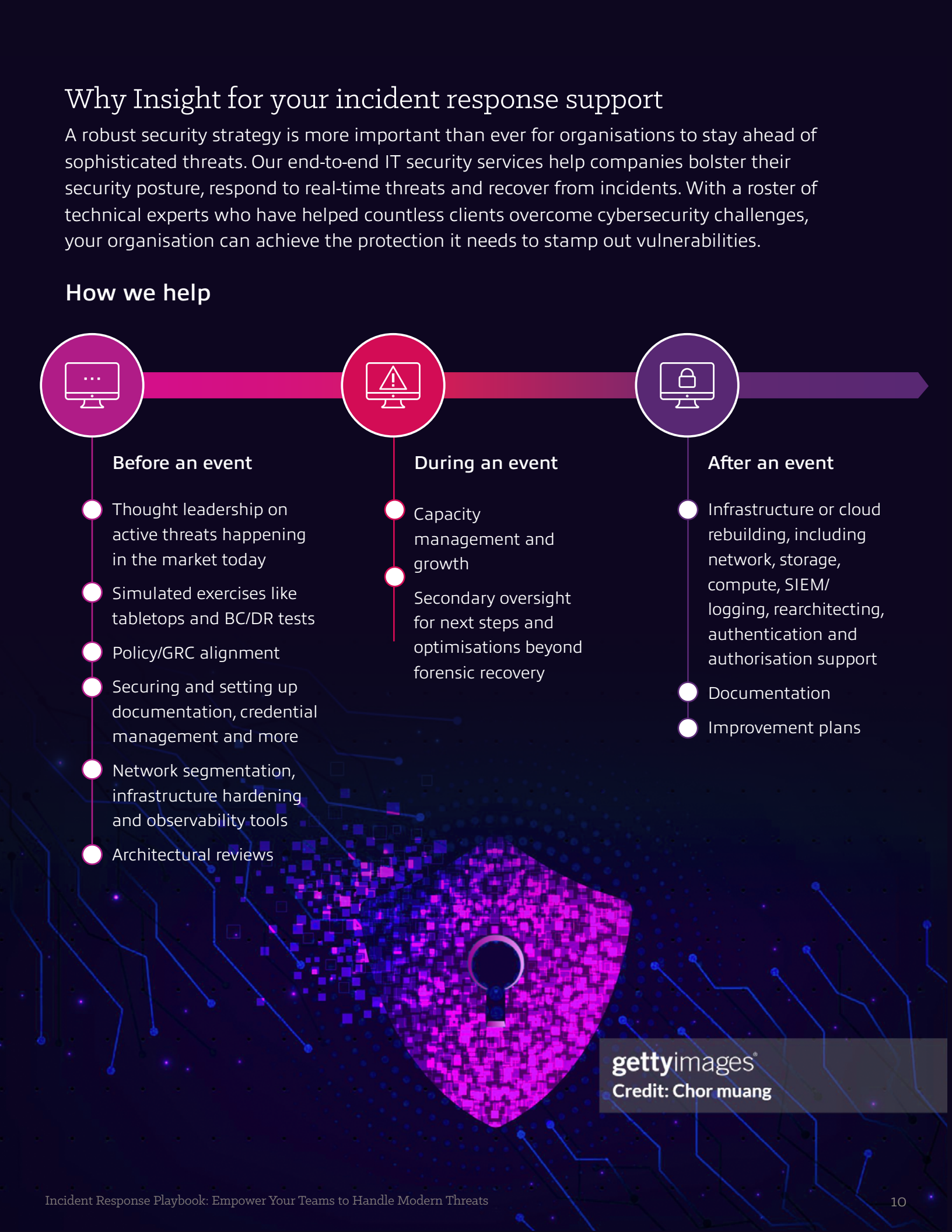
- Thought leadership on active threats happening in the market today
- Simulated exercises like tabletops and BC/DR tests
- Policy/GRC alignment
- Securing and setting up documentation, credential management and more
- Network segmentation, infrastructure hardening and observability tools
- Architectural reviews

During an event

- Capacity management and growth
- Secondary oversight for next steps and optimisations beyond forensic recovery

After an event

- Infrastructure or cloud rebuilding, including network, storage, compute, SIEM/ logging, rearchitecting, authentication and authorisation support
- Documentation
- Improvement plans



Plan, practice and recover with confidence.

Don’t get caught unprepared for today’s constantly evolving threats — our experts have helped countless clients overcome cybersecurity challenges.

SEE HOW WE CAN HELP.

Insight

Source:
[1] MarketPulse Research by Foundry Research Services. (February 2023). The Path to Digital Transformation: Where Leaders Stand in 2023. Slide 11. Commissioned by Insight.