TrustedImpact
PROTECTING DIGITAL

The “Other” Security Fundamentals

Why PenTesting alone won't keep you ‘roadworthy'

ABSIA

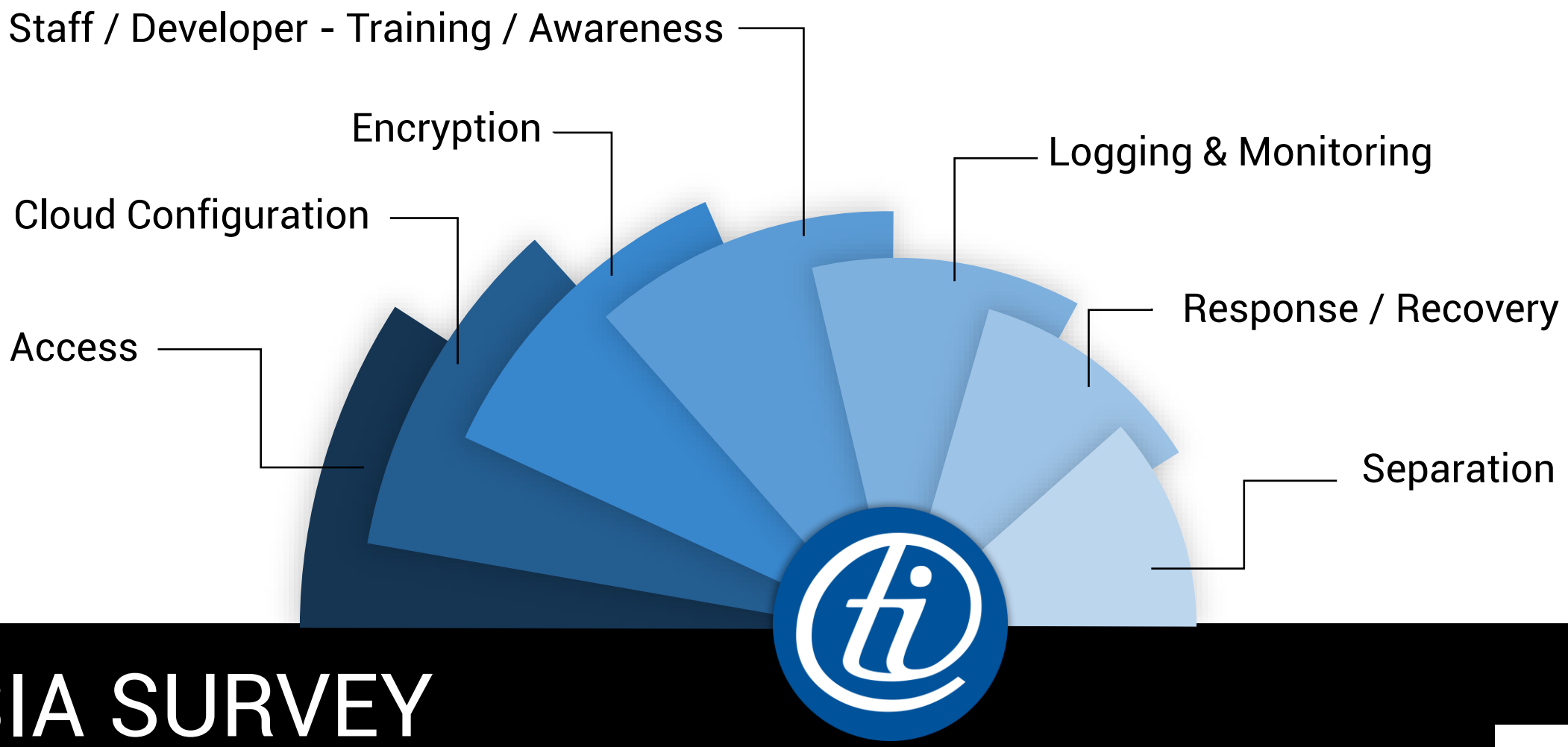
ABSIA Survey Results – Introduction

In late September 2020, ABSIA organised a webinar with members to explore and capture the results of several key security questions.

The following pages present the following:

1. The question topics
2. An editorial summary of the results – “Key Takeaways"
3. Numeric results and representation of responses
4. The specific survey questions

Survey Results – Question Topics



ABSIA SURVEY

Survey Results – Key Takeaway's

Members protect their systems against external threats, but don't particularly help their users protect themselves.

The majority store passwords properly and have account lockouts/logouts in place. However, user protection mechanisms such as password complexity, Multi-Factor Authentication and Suspicious Activity Alerting aren't well enforced.

Thanks to the Pandemic, "digital" is here to stay. It's prudent to protect all users, but these days the increase in "first time digital" users are skyrocketing and likely the most vulnerable – those who are less aware of cybersecurity risks and often do not know the basics such as not re-using passwords. McKinsey found that "*Fully 75 percent of people using digital channels for the first time indicate that they will continue to use them when things return to 'normal'.*

If the users of your software get hacked, exposed, defrauded via your software / platform – even if it's their own fault – the collateral brand damage can be significant. Pay it forward and help your users become more secure – it can be a differentiator for your software, reduce the risk of brand damage and will pay off for both them and you.

Members do a good job securing access for developers.

Developer access is granular to the individual, and a majority have a range of 'controls' in place to minimise the risk compromise.

Overall awareness training is high, but developer-specific training is low.

ALL respondents indicated they have a recurring awareness program for all employees to reduce the risk of phishing and scams. However, only one-quarter indicate they undergo developer, security and code-specific training.

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. The fact that these issues continue to be the causes behind a majority of the world's most significant breaches, shows that we continue to write flawed software; even though we've known about the issues since 2003.

Developer focused and code-specific training didn't really exist a few years ago, but it's evolved significantly. It's time to (re)consider conducting a base level of security focused, code-specific developer training.

Survey Results – Key Takeaway's (cont.)

Members monitor their systems, but few keep the evidence for very long.

67% of respondents have abuse scenario's defined and alerting in place. However, it was interesting to most that the majority keep logs between 1 to 6 months and only one-third keep them for the minimum of 7 years under the National Archives of Australia's *Administrative Functions Disposal Authority Express Version 2* publication (which is referred to by the ACSC Information Security Manual (ISM)).

On average, companies take 197 days (6.6 months) to identify and 69 days to contain a breach (IBM, June 2020). If your logs are only kept 6 months (or less), there will be no evidence to understand what happened in the event of a data breach. The current approach of keeping logs 1-6 months should be reconsidered.

You're practicing for 'game day'.

Over half (60%) have prepared for an incident with the executive group – a very positive result! Championship teams are the ones that not only have a solid playbook, but who train hard on a regular basis – keep up the effort and you'll come out ahead on 'game day' (when the incident is real).

Make sure you've checked your cloud configuration.

Two thirds didn't know whether their cloud configuration had ever been independently checked.

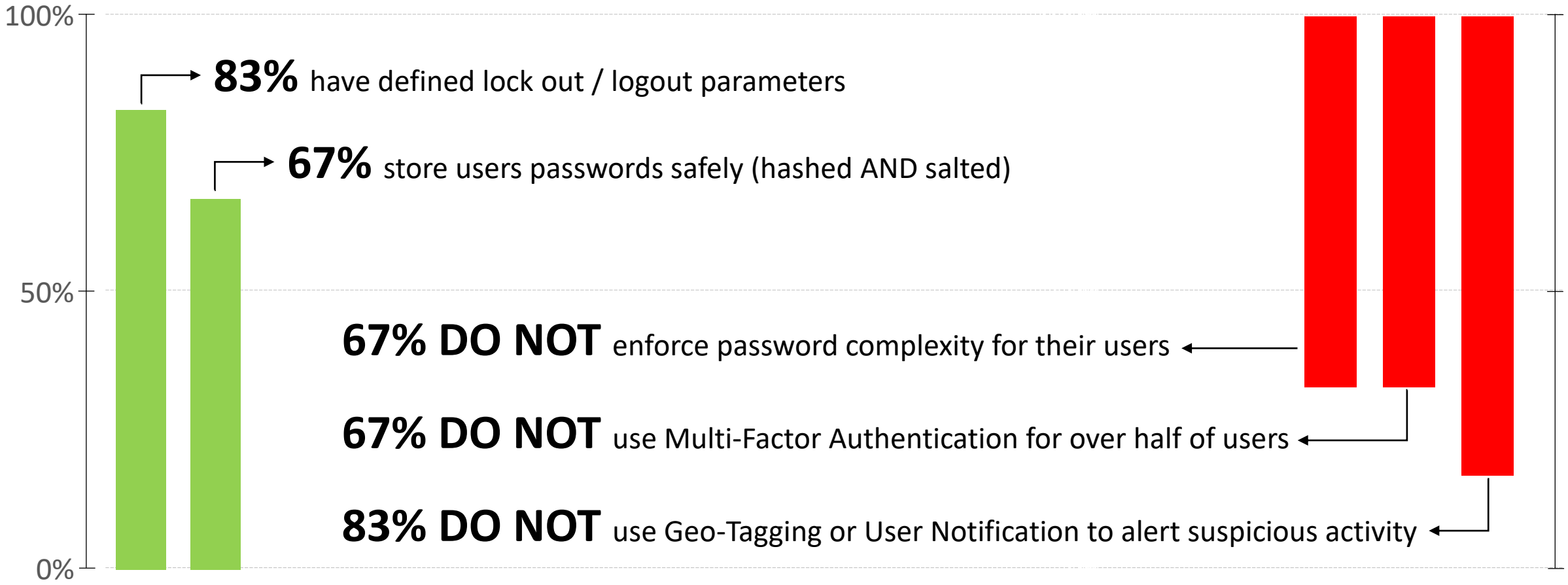
Our experience has shown that while many organisations have adopted the Cloud (AWS, Azure), few have kept pace with the idiosyncrasies of secure configuration. These things aren't always picked up in a "PenTest" and given the frequent data breach news relating to Open S3 Buckets, it's worth considering. At a minimum, the Centre for Internet Security (CIS) has some well defined benchmarks that can be used to get you there.

Hackers don't appreciate what's "IN scope" or "OUT of scope".

The majority either don't, or don't know if their ATO DSP Operational Framework and/or SSAM systems are physically separated or effectively segmented from other office systems. We get the fact that it can be difficult to 'certify' something against the entire organisation. From our experience, a large number of ISO:27001 (and similar) certifications have a limited scopes of certification.

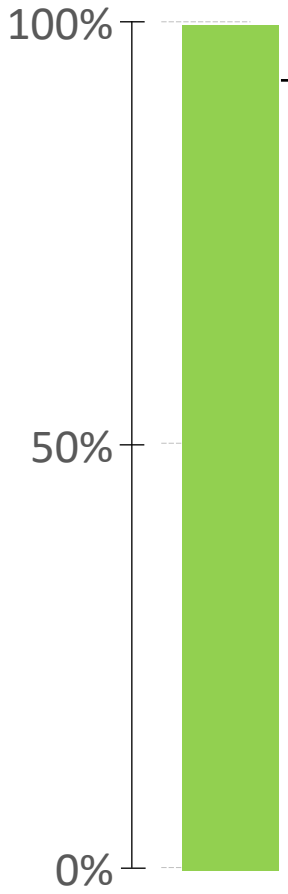
Just don't be lulled into thinking that because it's 'out of scope' that there are not significant risks by not properly segmenting (physically or logically) the environment from the other aspects of your organisation. If you've got valuables to protect, it's not a good idea to leave them sitting out in the open.

Survey Results – User Access



Members protect their systems against external threats, but don't particularly help their users protect themselves.

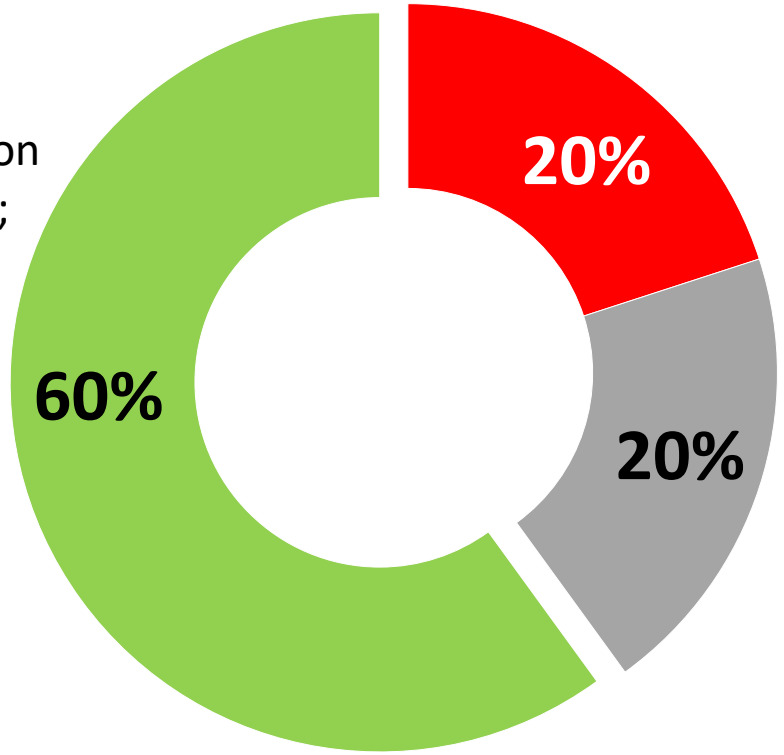
Survey Results – Developer Access



100% provide developer access specific to individuals

And **60%** have:

- Multi-Factor Authentication or allowed-listing in place;
- Password complexity checking;
- Account log/lockout; and
- Geotagging to alert suspicious activity…

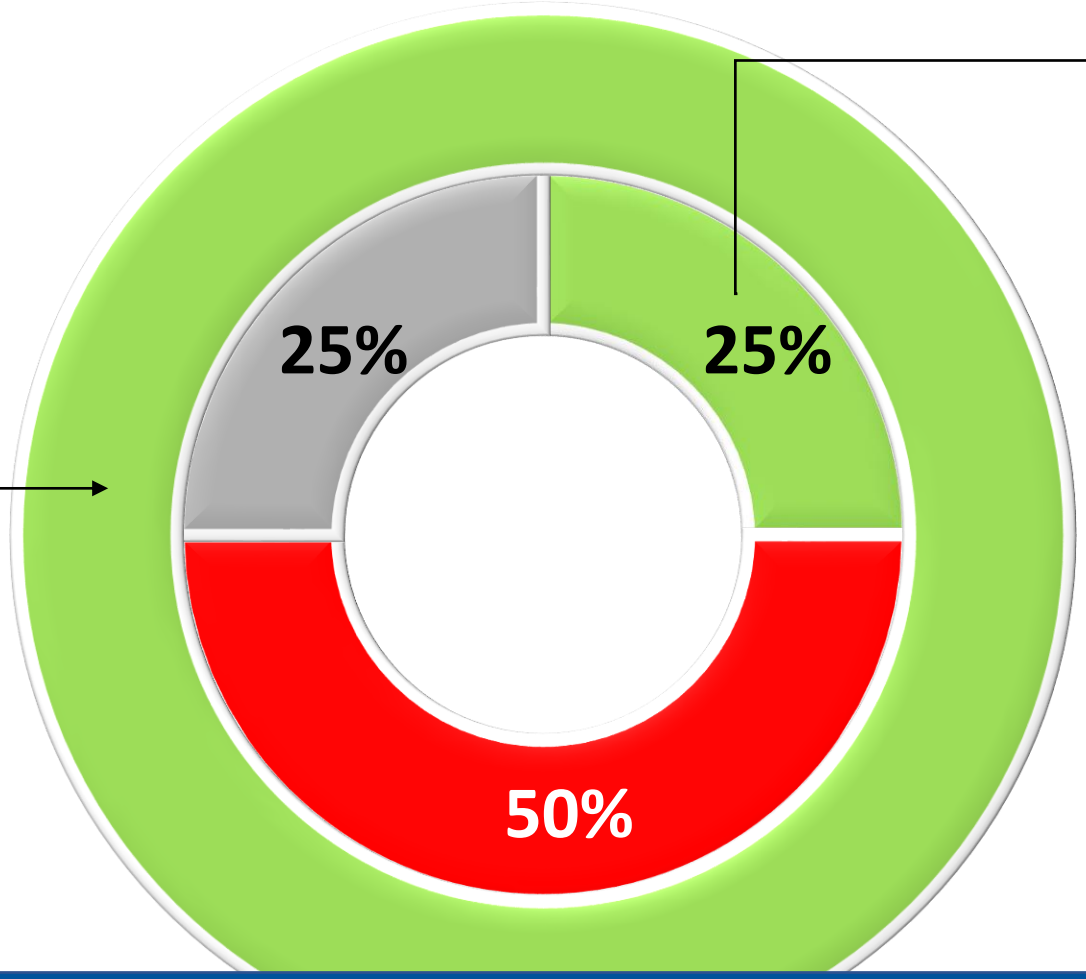


… yet **40%** either do not, or do not know

Members do a good job securing access for developers.

Survey Results – Training & Awareness

100%
provide all employees recurring awareness to reduce the risk of phishing and scams



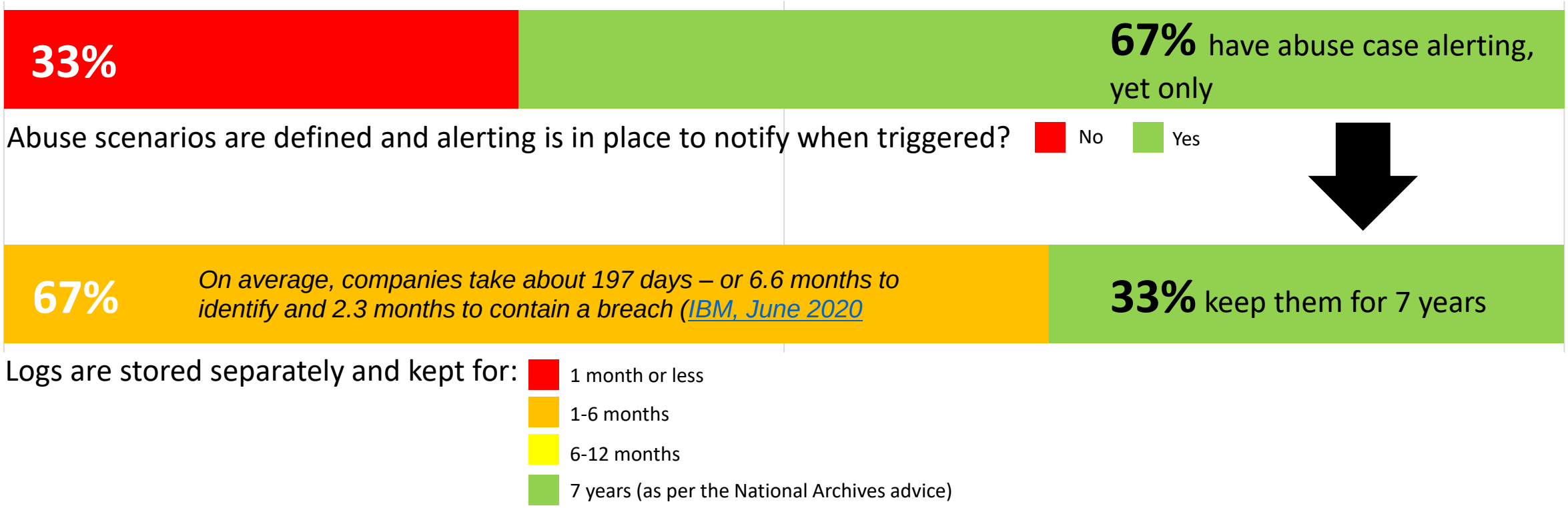
25%
provide developers 1 hour per month of code-specific secure development training

No Developer Training

Unknown Developer Training

Overall awareness training is high, but developer-specific training is low.

Survey Results – Logging & Monitoring

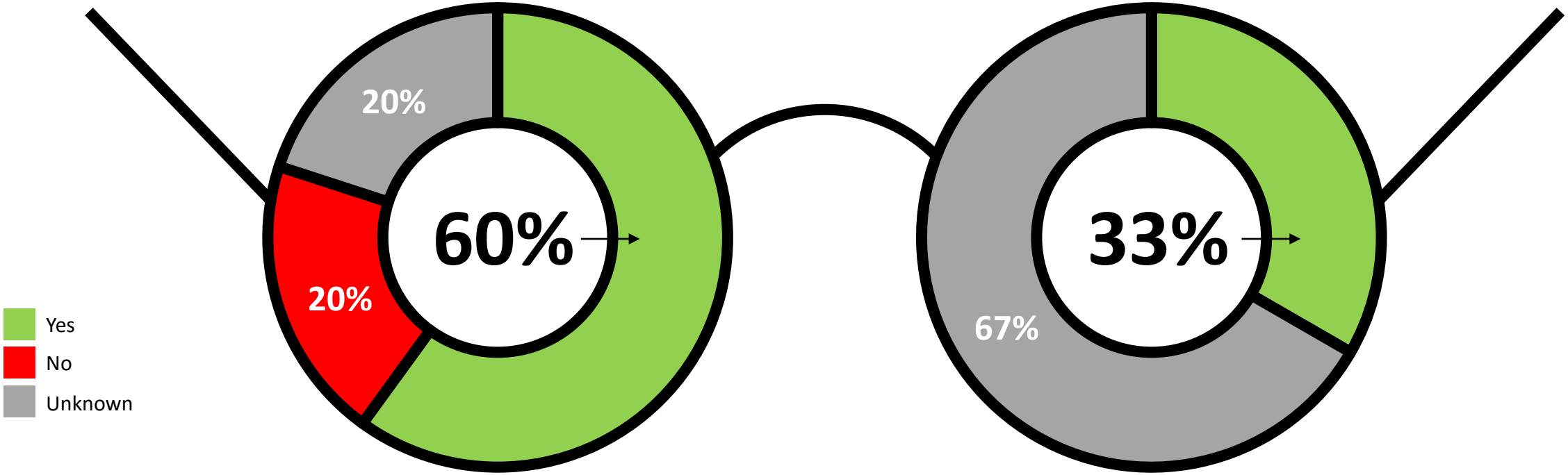


Members monitor their systems, but few keep the evidence for very long.

Survey Results – Cloud Configuration

You have a defined incident response plan and it is exercised with the executive group at least yearly?

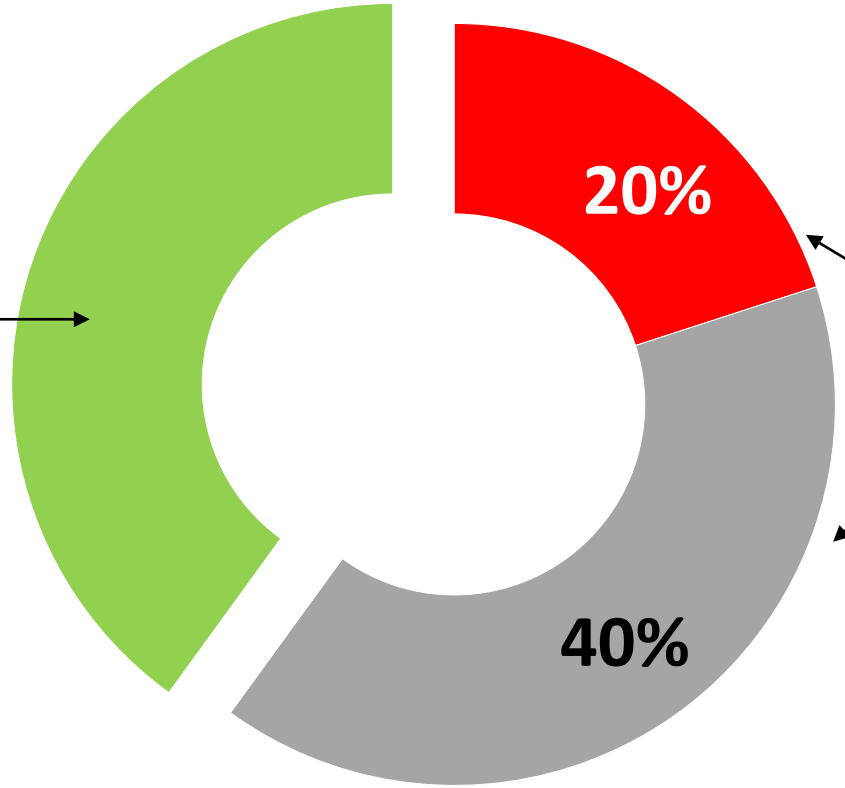
You independently assess the security configuration settings of your AWS/AZURE cloud instance at least yearly?



You're practicing for 'game day', but check your cloud configuration.

Survey Results – Separation

While **40%** have physically separated or effectively segmented environments for their ATO DSP / SSAM environments…



… the majority (**60%**) either do not, or do not know.

The system(s) 'in scope' for the ATO DSP Operational Framework and SSAM (or ISO:27001, etc.) are physically separated and/or effectively segmented from all other office systems (email, share drives, other products)?

Hackers don't appreciate what's "IN scope" or "OUT of scope".

Survey Results – Specific Questions

For those organisations with **USERS** logging onto a system:

1. Users can not use simple passwords – password complexity checking is enforced? (Y/N/Unknown/Not Applicable)
2. Stored user passwords are hashed and salted (Y/N/Unknown/Not Applicable)?
3. Account logout / lockout parameters are defined and working (Y/N/Unknown/Not Applicable).
4. Geotagging and user notification is being used to alert users to suspicious activity (Y/N/Unknown/Not Applicable)
5. MFA is turned on and more than 50% of users have it turned on (Y/N/Unknown/Not Applicable)

For those organisations with **DEVELOPERS** working on the system:

6. Developer access is specific to an individual (no generic accounts) (Y/N/Unknown)?
7. MFA or whitelisting is in place for all developer access (Y/N/Unknown)?
8. Password complexity checking is employed for all developers (Y/N/Unknown)?
9. Developer account logout / lockout parameters are defined and working (Y/N/Unknown)?
10. Geotagging and notification (eg via email) is being used to alert suspicious activity (Y/N/Unknown)?

11. For those who use public cloud offerings to host your software (AWS, Azure), you independently assess the security specific configuration settings of your cloud instance at least yearly (Y/N/Unknown/Not Applicable)?

12. Your organisation has a recurring awareness program to reduce the risk of phishing / scams for all company employees (Y/N/Unknown/Not Applicable)

13. Each developer takes a minimum of 12 hours (1hrs/month) of code-unique (eg, java, .net) secure development training for common programming issues (OWASP 10) each year.(Y/N/Unknown/Not Applicable)

14. Abuse scenarios across different software / hardware components of your solution are defined, and alerting is in place to notify when triggered?(Y/N/Unknown/Not Applicable)

15. Logs are stored separately and kept for:

   a. 1 month (or less)
   b. between 1-6 months
   c. between 7-12 months
   d. 7 years

16. Your organisation has a defined incident response plan in case of a loss of a system or data breach --- and is exercised with the executive group at least yearly (Y/N/Unknown/Not Applicable)?

17. The system(s) 'in scope' for the ATO DSP Operational Framework and SSAM (or ISO:27001, etc.) are physically separated and/or effectively segmented from all other office systems (email, share drives, other products)? (Y/N/Unknown/Not Applicable)?

Please note for Encryption: While this is an area often handled poorly, the issues of encryption 'at rest' (Key Management), and 'in-transit' are covered well in the ATO DSP Operational Framework and the ABSIA Security Standard for Add-on Marketplaces (SSAM)


In the Digital Age,
A security breach is inevitable.
Becoming a headline doesn't need to be.
YourData
YourBusiness
YourReputation
Protect Them.
Specialist consulting
in information security
www.trustedimpact.com / info@trustedimpact.com
TrustedImpact
PROTECTING DIGITAL