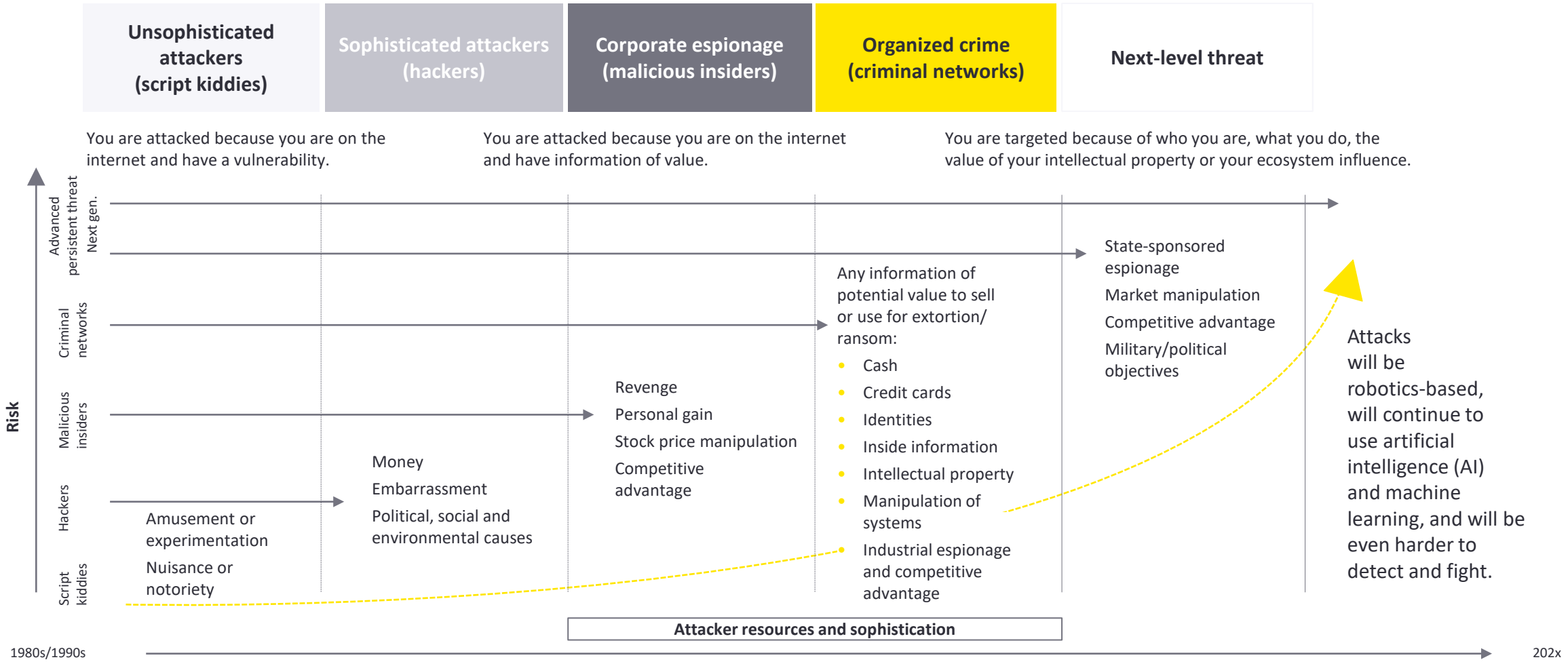
Cyber incidents and the role of Internal Audit

Disclaimer

- The views expressed by the presenters are not those of Ernst & Young LLP or other members of the global EY organization.
- These slides are for educational purposes only and are not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

The game has changed - the challenge of evolving security threats



What are board members saying about cyber risk governance that Internal Audit leaders should know?

1. **Elevate the tone:** Establish cybersecurity as a key consideration in all board matters
2. **Stay diligent:** Address new issues and threats stemming from remote work and expansion of digital transformation
3. **Determine value at risk:** Reconcile value at risk in dollar terms against the board's risk tolerance, including the efficacy of cyber insurance coverage
4. **Leverage new analytical tools:** Such tools inform the board of cyber risks ranging from high-likelihood, low-impact events to low-likelihood, high-impact events (i.e., a "black swan" event)
5. **Embed security from the start:** Embrace a "trust-by-design" philosophy when designing new technology, products and business arrangements
6. **Establish relationships with law enforcement early:** Have a strong relationship with law enforcement (e.g., FBI, DHS) and other governmental agencies in advance of crisis events
7. **Independently assess your program:** Obtain a rigorous third-party assessment of your cybersecurity risk management program (CRMP)
8. **Evaluate third-party risk:** Understand management's processes to identify, assess and oversee the risk associated with service providers and third parties involved in your supply chain
9. **Test response and recovery:** Enhance enterprise resilience by conducting rigorous simulations and arranging protocols with third-party specialists before a crisis
10. **Understand escalation protocols:** Have a defined communication plan for when the board should be notified, including incidents involving ransomware
11. **Monitor evolving practices and the regulatory and public policy landscape:** Stay attuned to evolving oversight practices, disclosures, reporting structures and metrics

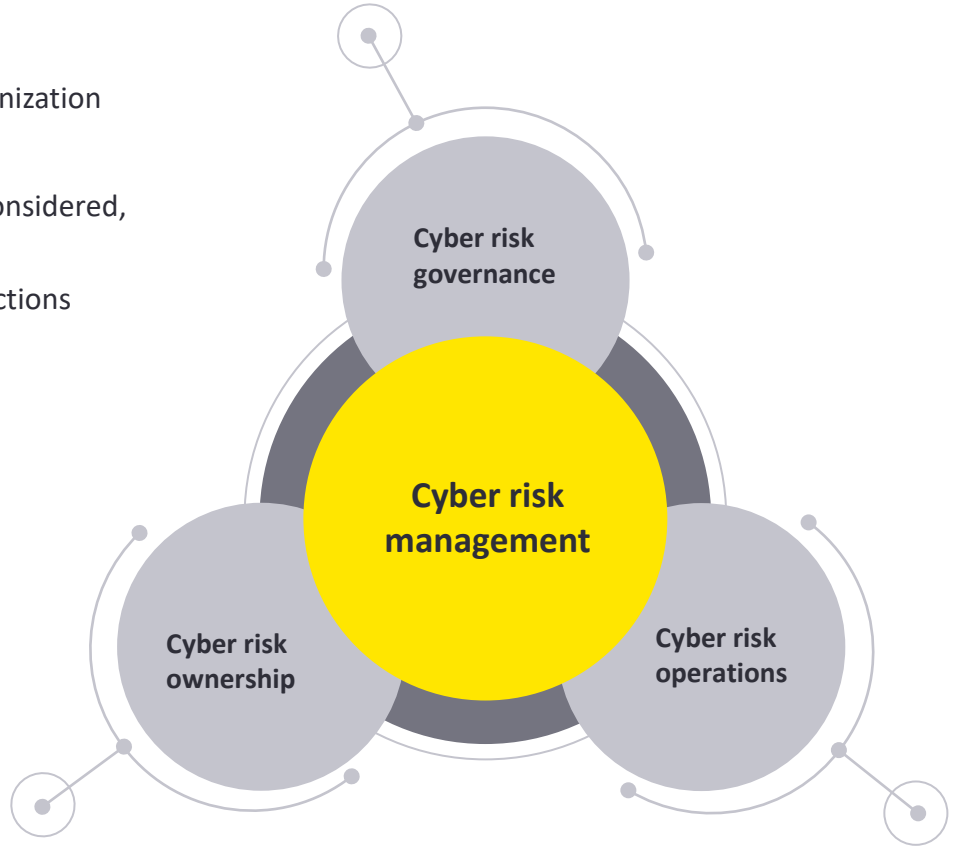
A view of cyber risk management and governance – where is Internal Audit?

Board of directors:

- Sets guidance and provides oversight for the organization
- Approves the organization's risk appetite
- Confirms whether risks are being appropriately considered, evaluated and managed
- Oversees performance and monitors corrective actions

Management:

- Assesses the business requirements
- Defines the organization's risk appetite
- Identifies and evaluates cyber risks impacting the business

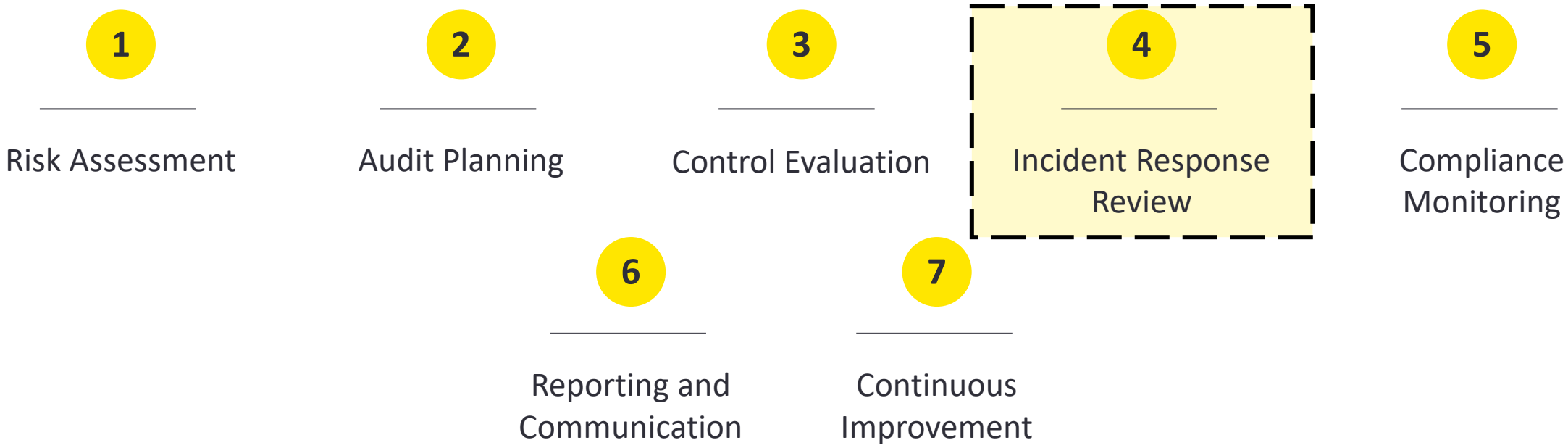


Information technology:

- Establishes and operates cyber risk management framework
- Delivers IT services to meet business requirements

The role of Internal Audit in cyber risk management is critical to ensuring effective oversight and providing independent assurance

Internal Audit serves as an **independent** and **objective assurance function** that provides insights, recommendations, and ongoing monitoring to help **enhance cyber risk management** framework, **strengthen cybersecurity controls**, and **improve overall resilience** to cyber threats.

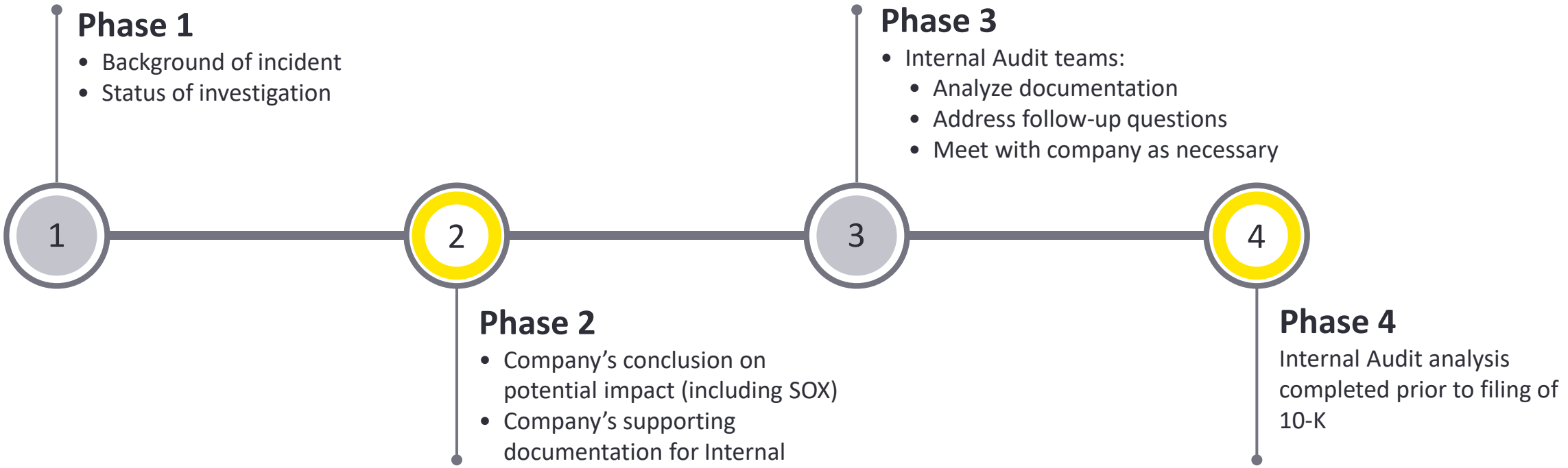


Understanding Internal Audit's role in incident response review

During an active incident, it is critical to understand and evaluate impact, including:

- Where did the adversary go in the environment?
- What did the adversary do in the environment?
- **What could the adversary do in the environment?** Internal Audit can help and has a deep understanding of:
  - Financial processes and data flows
  - Risks and controls
  - Connection between IT systems and the impact on financial controls
  - Significance of control deficienices

Phases of Internal Audit analysis of a cyber incident



Key elements of cyber breach response plans

1 Cybersecurity risk management

How will the organization make sure it detects the attack in a timely manner, isolates and assesses the damage done (i.e., responds), and shores up its defenses to prevent similar breaches in the future?

2 Business continuity planning and resiliency

How will the organization continue to operate as normal while recovering from the attack? Is it possible to operate as normal?

3 Compliance

What are the organization's duties for reporting the breach to the appropriate authorities, including law enforcement agencies if necessary, and how will these be discharged?

4 Public relations and communications

How will the organization communicate with all potential stakeholders, including employees, customers, suppliers and investors, both directly and via the media where there is public interest in the breach?

5 Legal

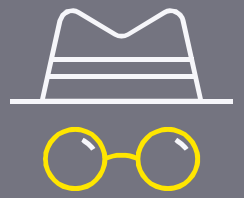
Has the organization assessed its vulnerability to potential litigation from a cyber incident? How will it record and maintain evidence for use in legal proceedings or use by law enforcement agencies?

6 Insurance

Has the efficacy of the company's cyber insurance been independently assessed?

How does Internal Audit understand sufficiency of investigation?

Sufficiency of investigation



Investigative methodology

- What were the indicators of compromise?
- What evidence was analyzed, and what were the results?
- What containment and eradication procedures were taken?

Presence of malware

- Was there endpoint detection and response (EDR) in place?
- What was the coverage of the EDR application?
- Did the EDR application provide any alerts?

Scope of compromise

- What accounts were compromised?
- What applications, hosts or databases were compromised?
- What data was accessed and/or manipulated?

Insights & trends from recent investigations

The 10 most recent investigations show that

- **50% of attacks resulted in monetary losses to the malicious actor:**
  - Two fraudulent transactions, both were the result of business email compromise attacks
  - Three ransom payments made to threat actor (five ransomware incidents; only three incidents resulted in payment)
- **60% of attacks resulted in data exposure and/or exfiltration:**
  - Six data exfiltration attacks, including confidential company information and company credentials
- **50% of attacks resulted in notification to customers and/or regulatory disclosure**

Of the 10 most recent investigations received

- **3 of the incidents were the result of a supply chain/third-party compromise (i.e., applications, vendors, subsidiaries, clients, customers)**
- **3 of the incidents were the result of an unpatched vulnerability or backdoor exploit**
- **4 of the incidents were the result of social engineering (Phishing, Smishing, Vishing, Business Email Compromise etc.)**

Investigation Insights – Key threat actor techniques

Key threat actor techniques

1. ***Help Desk (HD) Social Engineering*** — Outsourced / offshore help desk resetting user credentials and multi-factor authentication (MFA) after threat actor phone calls (without HD following proper vetting procedures).
2. ***SIM Swapping*** — Threat actors going into retail phone stores (or online) and leaving with phone provisioned with name and number of company executives, leading to account/MFA compromise.
3. ***Cloud Nesting*** — Gaining credentials of IT team member (or service accounts) with elevated privileges to spin up new unauthorized domain joined cloud instance(s). Use it as an EDR-less proxy to move laterally, deploy malware, gather exfiltrated data, keep backdoor connection into the environment.
4. ***Security Tool Hijacking*** — Gaining credentials of infosec team members (or service accounts) that manage EDR and use it to deliver legitimate tools for remote access persistence.
5. ***Virtual Machine Destruction*** — Gaining credentials of IT team members (or service accounts) with administrative virtual machine's console access. Taking down large swaths of production systems and applications via shutdown and removal at the machine level.

Evaluating and concluding on sufficiency of investigation

#	Components supporting sufficiency of investigation	Suggested supporting documentation/evidence
1	Incident **background** and overview of **investigative methodology**	▪ Written investigative reports, incident memos (third-party and/or internal)
2	**Indicators of compromise** (IOCs) were **extracted** from adversary activity (such as IP addresses, malicious URLs, hashes of malicious files, etc.) and **recursively searched across the environment** until no further malicious activity could be identified	▪ List of indicators of compromise ▪ Screenshots/screen-share showing IOCs, such as IP addresses, were searched in environment and results are consistent with Company representations
3	**Data/logs** pertaining to the incident **exist** and were able to be **searched**	▪ Summary of logs analyzed (Azure AD, SIEM, etc.) with date range of the data available for each log
4	**Timeline of key adversary activity**, such as: ▪ First known activity ▪ Last known activity ▪ Compromise of new users or assets ▪ Exfiltration of data ▪ Other key activity	▪ Full timeline of attacker activity (sometimes known as an incident management sheet), or a sample of transactions/log entries related to evidence of first and last known attacker activity and other notable activity for this incident (such as the compromise of additional accounts)
5	What was the **scope of compromise**? ▪ **Users** ▪ **Assets** - applications, hosts, databases, etc. ▪ **Data** - financial data, PII, PHI, proprietary information, passwords, etc.	▪ List of compromised user accounts ▪ List of compromised assets (hosts, applications and/or database)

Evaluating and concluding on sufficiency of investigation – cont'd

#	Components supporting sufficiency of investigation	Suggested supporting documentation/evidence
6	**Presence of malware**: Have reasonable efforts been made to assess for the presence of malware in the environment? ▪ **Capabilities must exist** to allow for a reasonable assessment to be made: endpoint detection and response (EDR) preferred, may consider antivirus/malware scanning or host-forensics as alternatives ▪ Several "conclusions" by company are possible: ▪ **No malware identified** during the course of the incident ▪ **Malware was identified** during the course of the incident but was determined to be **unrelated** ▪ **Malware was identified** during the course of the incident and is **related** ▪ Appropriate steps taken to **understand** the nature/capabilities of the malware (such as reverse engineering) and **assess for its presence** in the environment	▪ Supporting documentation to exhibit Company has assessed for the presence of malware, such as: ▪ Endpoint detection and response (EDR) or antivirus/malware scanning ▪ Statement on coverage percentage and status ▪ Screenshot of alerts (or lack thereof) generated during incident ▪ If any generated and determined to be unrelated, provide explanation of how this was determined ▪ If any generated and determined to be related to the incident, provide explanation of how its capabilities were analyzed and how it was remediated ▪ Host forensic analysis methodology/workplan and results
7	**Containment/remediation** methodology and timeline: ▪ Was the incident properly mitigated? ▪ Has the company demonstrated they are taking steps to prevent such an incident from occurring in the future?	▪ Written investigative reports, incident memos (third-party and/or internal) ▪ Lessons learned write-up with action plan, revised roadmap
8	**Competency** and **objectivity** of investigative team	▪ Investigator CVs, biographies ▪ Summary of relationship between company and investigating team

Evaluating impact – illustrative SOX considerations

1. Which SOX systems were impacted by the threat actor?

   What is the specific ICFR risk for each SOX system?

2. Which SOX systems did the compromised accounts provide access too?

   What SOX systems could have been accessed with the compromised account credentials?

3. Which SOX systems were offline and when were they restored?

   What is Management's recovery/restart process for SOX systems?

4. Were significant changes to the functionality of the systems made in connection with the incident?

   If so, was the standard change management process followed?

5. Was access elevated for new or existing users during the period systems were pre-emptively taken offline?

   Is so, was the standard access provisioning process followed?

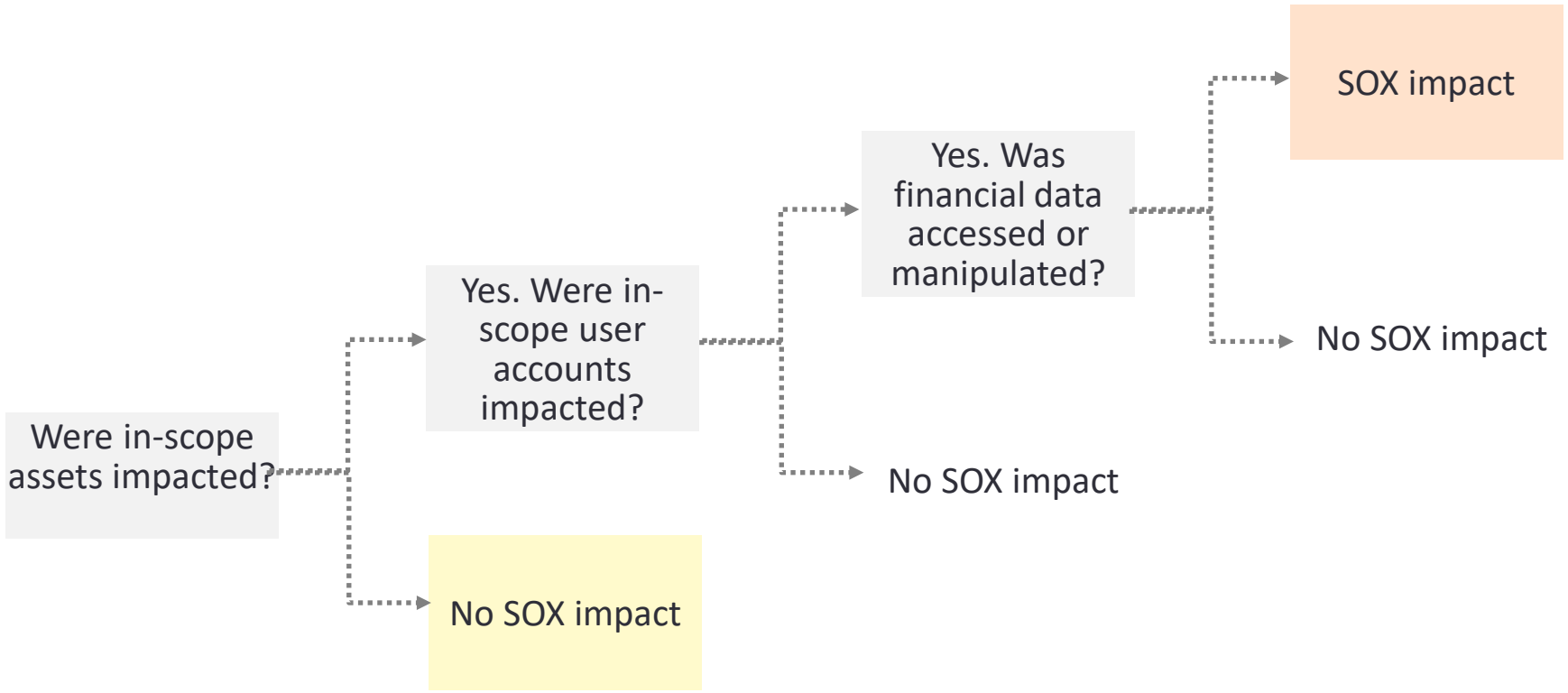
6. Were new key controls created for manual procedures performed while systems were offline?

7. Was the incident related to an ICFR deficiency?
   - Relevant compensating controls
   - Management conclusion
   - Management remediation plan

8. Other procedures performed: password resets, user access reviews

*Evaluate what **could** the threat actor have done?*

Evaluating impact – illustrative SOX decision tree



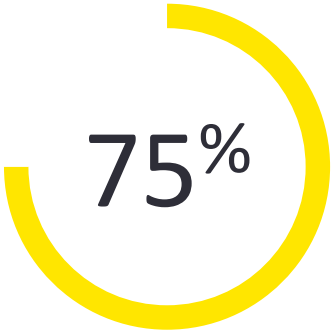
How can Internal Audit help leaders prepare?

Know that even the most robust cybersecurity program can never eliminate all risk.

Verify that cyber breach response plans span the whole organization.

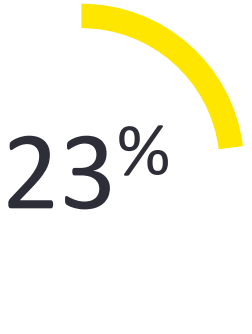
Identify most significant threats and vulnerabilities.

Run simulations and exercises for multiple scenarios to enhance preparedness.



of directors said their board had **not** participated in a breach or ransomware simulation exercise in the last 12 months

Source: Survey of board participants during the EY Better Questions for Boards webcast "How audit committees can strengthen cyber resiliency, crisis preparedness and corporate governance," October 2022.



of directors said their organization was very ready to respond to a ransomware attack

Source: Survey of directors during the EY Cybersecurity webcast "Ransomware," October 8, 2021.

SEC cyber disclosure

Compliance now; help enhance the program maturity over time

	Now	Next
	Comply with disclosure rules	**Enhance program maturity**
Risk management and strategy	• Cybersecurity risk assessment process and results • Risk materiality and disclosure evaluation process	• Additional cybersecurity capabilities to reduce risk • Risk assessment inputs expansion — threat intelligence, threat and vulnerability management • Data-driven risk quantification for automated and continuous assessment (leading edge)
Governance	• Management roles and responsibilities documentation • Board reporting and oversight • Materiality framework • Disclosure controls and procedures under Section 302 of the Sarbanes-Oxley Act	• Cybersecurity policies, standards and procedures formally documented • Prior-year disclosure analysis • Entity-level control considerations • Independent program verification
Incident disclosure	• Incident response process and workflow • Incident materiality evaluation and disclosure determination methodology	• Incident simulation and scenario exercises • Incident response program • Incident response governance committee

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

ABC JJMM-123
ED None

ey.com