secureframe

Cybersecurity Tabletop Exercises

+ Scenario Templates

Contents

1. Ransomware attack

Scenario

It's a typical Monday morning, and employees are settling into their work routines. Suddenly, multiple users report that they can't open their files. Instead of documents, they see a message on their screens: *"Your files have been encrypted. Pay 10 Bitcoin within 72 hours, or they will be permanently deleted."*

The IT helpdesk is flooded with calls, and as the security team investigates, they quickly realize the situation is worse than expected. System administrators confirm that several file servers, endpoints, and even the customer database are locked down. Attempts to restore from backups fail as it's discovered those files are encrypted too.

The company's operations grind to a halt. Customer support cannot access order records, finance is unable to process transactions, and critical business systems are offline. Meanwhile, executives debate the next steps. Should they negotiate with the attackers? Do they contact law enforcement? What if sensitive customer data has been stolen? As the team scrambles for answers, the attackers send another message: *"We have your customer data. Pay now, or we will release it."*

Discussion prompts

Initial response & notification

- How does your team first become aware of the ransomware attack?
- Who is responsible for initiating the incident response plan?
- What immediate containment steps should be taken to prevent further spread?
- How is leadership informed, and what communication channels are used?
- Should customers, vendors, or regulators be notified immediately?

Assessment & impact analysis

- Which systems and data have been affected by the ransomware?
- Is there evidence of data exfiltration, or is this a purely encryption-based attack?
- What is the potential financial, operational, and regulatory impact?
- How does your organization determine whether backups are intact and usable?

Incident response & mitigation

- Should infected systems be immediately disconnected from the network?
- What tools and resources are available for identifying and containing the attack?
- What steps should be taken to prevent reinfection and determine the attack vector?
- How should law enforcement and cybersecurity insurance providers be involved?

Ransom payment decision

- What factors should influence whether to pay or not pay the ransom?
- If payment is considered, what legal, ethical, and regulatory concerns must be addressed?
- What alternatives exist to recover systems without paying the ransom?
- How should executives, legal teams, and law enforcement be involved in the decision?

Disaster recovery & business continuity

- What backup solutions are in place, and how quickly can data be restored?
- If backups are compromised, what are the alternative recovery options?
- How does your organization ensure business continuity while systems are being restored?
- What critical business functions need immediate restoration?

Incident communication & stakeholder management

- How should the company communicate with executives, employees, customers, and vendors?
- What messaging is prepared for external stakeholders, including customers, media, and regulators?
- Should a press release or public statement be issued, and if so, how should it be framed?

Post-recovery & lessons learned

- How do you verify that all systems are restored properly and securely?
- What long-term security improvements should be made to prevent future ransomware attacks?
- How should employee training and security awareness be adjusted based on lessons learned?
- What policy, process, and technical gaps were exposed, and how can they be addressed?

Suggested injects

- The attacker provides a "sample" of stolen data to prove they have access to sensitive information.
- IT discovers that backups are also encrypted and may not be usable.
- The ransomware note threatens to leak customer data if the ransom isn't paid within 48 hours.
- A journalist reaches out, asking for a statement on reports of a cyberattack on the company.

2. Business email compromise & wire fraud

Scenario

On a busy Friday afternoon, the CFO of your company receives an urgent email from the CEO. The message is brief and direct: **"***We need to wire $250,000 to Global Suppliers ASAP. It's for a critical partnership deal, so it needs to be processed immediately.*" The email appears legitimate, since it comes from the CEO's actual email address, includes a professional signature, and even references an ongoing vendor negotiation. Without hesitation, the finance team processes the transaction.

Hours later, the CFO mentions the payment to the CEO. A confused look spreads across the CEO's face, and she realizes her email account has been compromised. A sophisticated phishing attack had allowed an attacker to gain access and send fraudulent emails on her behalf. The money is gone, transferred to an offshore account that may be impossible to recover.

As the team scrambles to contain the breach, IT discovers that other executives' email accounts were also targeted. Employees start receiving more suspicious emails, and the finance team wonders: Have there been more unauthorized transfers? How long has this been happening? And who else might be compromised?

Discussion prompts

Incident identification & initial response

- How does the finance team detect the fraudulent request?
- Who is responsible for investigating and escalating the issue?
- What immediate containment steps should be taken to prevent further financial loss?
- Should law enforcement or financial institutions be contacted?

Containment & mitigation

- What steps should be taken to secure affected email accounts?
- How can your team determine if other accounts were compromised?

- Can the funds be recovered through the bank or fraud prevention teams?

Investigation & root cause analysis

- How did the attacker gain access to the email account?
- What weaknesses allowed this attack to succeed?
- What security monitoring should have detected this attack sooner?

Communication & legal considerations

- How should the company inform leadership, employees, and regulators?
- Should affected customers or vendors be notified?
- What legal and compliance obligations apply?

Prevention & security enhancements

- Should multi-factor authentication (MFA) be enforced on all email accounts?
- What policies should be updated to prevent future BEC attacks?
- How can finance and executive teams be trained to recognize similar fraud attempts?

Suggested injects

- The finance team realizes this was not the only fraudulent wire transfer—two additional transactions have already been approved.
- IT discovers that multiple executive email accounts were accessed, suggesting a broader compromise.
- A vendor contacts the company, claiming they received an unusual payment request from your finance department.
- Your organization's bank flags suspicious activity, freezing some transactions.
- A phishing email similar to the original scam is sent to another department, raising concerns that other employees may fall victim.

3. Data center failure

Scenario

At 10:23 AM, a sudden power surge hits your company's primary data center. Within seconds, network engineers see red alerts flood the monitoring dashboards: all major production systems are offline. The automated failover to backup power should have kicked in, but it didn't. Instead, the hardware failure has left critical applications, customer databases, and internal operations in complete disarray.

Customer service channels light up with complaints. The website is inaccessible, transactions are failing, and employees can't even log into their email accounts. Worse still, when IT attempts to restore services, they discover that the most recent database backup is corrupted**.**

As leadership demands a timeline for recovery, the IT team works to identify the root cause. Was this an internal failure or a cyberattack? A major client is already threatening to take their business elsewhere, and regulators are asking questions. Every passing minute costs the company thousands of dollars, and the team must act fast before the damage becomes irreversible.

Discussion prompts

Initial response & awareness

- How does your team first detect the data center failure?
- Who is responsible for declaring a disaster and activating the disaster recovery plan?
- What immediate containment and assessment steps should be taken?

Business impact assessment

- Which systems and services are affected?
- How long is the expected downtime?
- What is the financial and operational impact?

Disaster recovery plan execution

- What backup and failover solutions are in place?
- If using cloud services, how does your team ensure data integrity?
- How quickly can business operations be restored?

Communication strategy & stakeholder management

- How should employees, executives, and customers be informed?
- What messaging should be prepared for public communication?

Post-recovery & improvements

- What worked well in the response?
- What gaps in disaster recovery planning were identified?
- What long-term improvements should be made to prevent future failures?

Suggested injects

- The backup generator also fails, extending downtime longer than expected.

- IT staff discover that the last backup is corrupt and cannot be restored.
- The company's cloud provider experiences an unrelated outage, further complicating recovery efforts.
- A key IT team member responsible for disaster recovery is unreachable due to a personal emergency.
- Customers begin posting complaints on social media about being unable to access services.

4. Third-party vendor breach

Scenario

Late on a Friday evening, the cybersecurity team at your company receives an alarming notification. One of their third-party vendors, which handles customer payment processing, has suffered a major security breach. Initial reports suggest that attackers exploited a vulnerability in the vendor's systems, potentially exposing thousands of customer records, including credit card details and personal information.

The vendor downplays the situation, assuring your team that no sensitive data was affected. But within hours, customers start reporting fraudulent transactions linked to accounts processed through the vendor. A journalist has already reached out for a comment.

Your team must decide how to respond. Do you cut ties with the vendor immediately? Should you inform customers now or wait for further details? Is there legal liability, and how will regulators react?

Discussion prompts

Breach discovery & initial response

- How does your team become aware of the breach?
- Who is responsible for initiating an internal investigation?
- What immediate containment steps should be taken?

Impact assessment & risk mitigation

- What systems and data were accessed by the vendor?
- Is customer or employee data exposed?
- Should access to the vendor be suspended?

Legal & regulatory considerations

- What are the reporting requirements for regulators and customers?

- Should affected parties be notified immediately or after investigation?
- Are there contractual obligations with the vendor that impact response efforts?

Communication strategy & public relations

- What messaging should be prepared for internal stakeholders?
- How should customers and the public be informed?
- How does the company manage PR to maintain trust?

Post-breach vendor management & security improvements

- What security gaps in vendor risk management were identified?
- Should vendor contracts include stronger security requirements?
- How can the company ensure better vendor risk assessment and monitoring?

Suggested injects

- The vendor initially claims that no sensitive data was exposed, but later reveals that customer records were accessed.
- A regulator contacts your organization asking if you were affected by the vendor's breach.
- The vendor refuses to provide detailed forensic reports about the attack, citing confidentiality concerns.
- One of your customers reports receiving phishing emails that reference their account details, suggesting stolen data is being used for fraud.
- An internal audit reveals that the vendor did not meet the security requirements outlined in their contract.

5. Insider threat

Scenario

A month after a senior engineer left his role at your company, an IT security audit reveals something troubling: large amounts of sensitive company data were downloaded to a personal USB drive just hours before his resignation.

At first, your security team wonders if it was accidental. But as they dig deeper, they discover that the former employee also accessed proprietary source code, customer lists, and confidential financial projections. Further investigation reveals he forwarded critical project files to his personal email account.

Then comes another surprise: this former senior engineer recently joined a direct competitor as Chief Product Officer. Was this corporate espionage? Did he sell company secrets? Will customers be impacted? The legal team scrambles to assess what actions can be taken. Meanwhile, your cybersecurity team worries that if one ex-employee took this much data, who else might be doing the same?

Discussion prompts

Detection & initial response

- How does the incident first come to your team's attention?
- What security monitoring tools or policies could have detected this activity sooner?
- What immediate actions should be taken to contain the threat?
- Who should be notified internally, and what teams need to be involved in the response?

Investigation & risk assessment

- What types of data were exfiltrated, and what is their sensitivity level?
- Has any customer or proprietary information been exposed?
- Could this incident result in regulatory or legal violations?
- What forensic steps should be taken to verify the extent of the breach?

Legal & compliance considerations

- What legal actions can or should be taken against the employee?
- Are there industry regulations or data protection laws that require disclosure of this incident?
- Should law enforcement be contacted, and if so, at what stage?
- How does your organization handle HR and legal implications of the incident?

Containment & remediation

- What steps should be taken to prevent further unauthorized data transfers?
- Should access to sensitive systems be immediately revoked for all departing employees?
- What security controls (e.g., Data Loss Prevention tools) need to be reviewed and improved?
- Should additional restrictions be placed on personal device usage and data transfers?

Communication & stakeholder management

- Should employees be informed about the incident to raise awareness?
- If customer data was involved, how and when should they be notified?
- How does your organization manage internal messaging to prevent unnecessary panic?
- What public relations steps should be considered in case of media exposure?

Post-Incident review & policy enhancements

- What weaknesses in your team's insider threat detection were identified?
- Should new policies or procedures be implemented for employee offboarding?
- How can security training be improved to better recognize insider threats?
- What long-term technical and policy improvements should be made to reduce insider risks?

Suggested injects

- IT discovers that the ex-employee also sent files to a personal email account before leaving.
- A competitor announces a new product suspiciously similar to proprietary information that was accessed.
- A whistleblower reports that the ex-employee may have been working with an external party before their resignation.
- Legal teams receive an inquiry from a regulator asking if the company has experienced any data security incidents.
- The incident response team finds that the employee's access was never fully revoked, and they are still logging in remotely.

6. Red vs Blue team simulated cyberattack

Scenario

It's a regular workday at your organization, a mid-sized technology company specializing in cloud-based software. Unbeknownst to the IT and security teams, a sophisticated attacker (the Red Team) has been planning their move for weeks. After conducting reconnaissance, they identify a vulnerable external-facing web application that lacks proper security patches.

At 8:00 AM, the attack begins. The Red Team exploits a known vulnerability in the application, gaining an initial foothold in the company's network. They move laterally, escalating privileges and exfiltrating sensitive internal documents. The Blue Team must now detect and respond to the breach in real-time, using security monitoring tools, log analysis, and incident response procedures to contain the attack before critical data is lost or systems are severely compromised.

Red team objectives:

1. Gain initial access via a web application vulnerability.
2. Escalate privileges to gain administrative control.
3. Move laterally within the network undetected.

4. Attempt to exfiltrate sensitive company data such as customer records and intellectual property.
5. Deploy persistence mechanisms to maintain access.
6. Test your team's response time and mitigation strategies.

Blue team objectives:

1. Detect unusual activity (e.g., unauthorized logins, privilege escalation).
2. Analyze logs to trace attacker movement.
3. Contain the breach by isolating affected systems.
4. Remove persistence mechanisms and block attacker access.
5. Restore compromised systems while ensuring business continuity.
6. Communicate and escalate appropriately to leadership and stakeholders.

Discussion prompts

- How long did it take for the Blue Team to detect the breach?
- What indicators of compromise were missed or overlooked?
- Were security tools configured properly to detect and mitigate the attack?
- How well did teams communicate and coordinate during the incident?
- What security gaps were identified, and what improvements should be made?

Suggested injects

- The Red Team sends a convincing phishing email to a high-level executive, attempting to capture credentials and gain additional access.
- The attack simulation includes a rogue employee unknowingly aiding the attackers by disabling security alerts.
- The Red Team deploys simulated ransomware on a test machine, forcing the Blue Team to decide whether to shut down portions of the network.
- Red Team exploits misconfigured cloud storage, gaining access to customer records stored off-premises.
- A fake journalist reaches out to the company, claiming to have insider knowledge of an ongoing breach. How does your organization respond publicly?