Information Technology Security Policy – Security Incident Response Procedure

To be read in conjunction with IT Security Policy

Introduction

Incident Response Procedures

1. Incident Response Procedures for Vulnerabilities
2. Incident Response Procedures for Compromised IT Resources
3. Incident Response Procedures for Copyright Infringement
4. Incident Response Procedures for Violations of the Acceptable Use
5. Incident Response Procedures for Suspicious Activity

Supporting Incident Response Standards, Procedures, and Guidelines

6. Critical IT Resources Standard
7. Critical IT Resource Registration Procedures
8. Service Interruption Notification Procedures
9. Incident Tracking Standard
10. Incident Severity Classification Guidelines

Appendix

11. Summary of Response Procedures for Incidents Involving Law Enforcement
12. Summary of Incident Response for Legal Issues
13. Summary of Internal and Public Communication Notification Procedures

References

14. Forensic

Introduction

An IT security incident, for the purpose of all Key Conference Solutions Information Technology (IT) Regulations, is defined as an event that impacts or has the potential to impact the confidentiality, availability, or integrity of company IT resources. Standards, procedures, and guidelines regarding IT security incident response are included in this document. Specific procedures vary depending on the type of incident, but all procedures include the following steps:

1. Discovery
2. Documentation
3. Notification
4. Acknowledgment
5. Containment
6. Investigation
7. Resolution
8. Closure

In order to coordinate response to and resolution of IT security incidents, the company has established an incident response team (IRT) The Incident Response Team (IRT) is led by the IT Security Manager or their designee. The IRT is responsible as follows:

- Has primary authority in response decisions for IT security incidents
- Coordinates incidents from discovery through resolution and closure
- Assesses threats to IT resources
- Determines vulnerabilities of IT resources
- Processes IT security complaints or incidents reported by others
- Alerts employees of active threats

The following list describes responsibility for each step in the typical incident response process:

1. IRT maintains systems to discover security incidents involving IT resources
2. IRT documents IT security incidents in a tracking system
3. IRT sends notifications to employees identifying the type of incident
4. Employees must acknowledge the notification
5. Employees must contain the incident as soon as possible
6. Employees report back to IRT to update the tracking system with details of the investigation
7. IRT, using details from the investigation, determines incident severity
8. IRT must update the tracking system when the incident is resolved
9. IRT reviews incidents in the tracking system and closes tickets as appropriate

IRT can be contacted with any questions regarding incident response. Employees must respond to and resolve all incidents reported to them by IRT. They must report to IRT all incidents that have the potential to impact other employees.

II. Incident Response Procedures

II.A. Incident Response Procedures for Vulnerabilities

Examples: patch or upgrade needed, weak password, unrestricted access

II.A.1. **Discovery**. The Incident Response Team assesses threats to company IT resources. When a threat is discovered, it is documented and Employees are alerted. When possible, company IT resources are assessed for vulnerability to the newly discovered threat and appropriate contacts are notified.

II.A.2. **Documentation**. IRT tracks discovered vulnerabilities in a tracking system.

II.A.3. **Notification**. When a vulnerability is discovered by the Incident Response Team, appropriate contacts are notified via email. The recipient list of IRT notifications may be augmented as needed to include employees with appropriate knowledge and skills.

II.A.4. **Acknowledgment**: Not all vulnerability notifications require acknowledgment; follow the instructions included with the notification. For accurate tracking of vulnerabilities and to avoid erroneous notifications, false positives should be reported to the IT Security Manager.

II.A.5. **Containment**. IT resources with vulnerabilities should be contained until the vulnerability is resolved.

II.A.6. **Investigation**. Network and server managers must investigate vulnerabilities identified in notifications..

II.A.7. **Resolution**. Network and server managers must resolve vulnerabilities identified in notifications. Common resolutions to correct a vulnerability include upgrading and patching. Alternatives include physical, network, host, user and/or other access restrictions. Other resolutions may also apply.

II.A.8. **Closure**. IRT reviews the tracking system and closes tickets when appropriate. IRT has primary authority in response decisions for IT security incidents and coordinates incidents from discovery through resolution and closure. IRT can be contacted with any questions regarding incident response.

II.B. Incident Response Procedures for Compromised IT Resources

Examples: attack/exploit, backdoor or trojan, denial of service, malware, unauthorized access

II.B.1. **Discovery**. IRT receives and processes discovery notifications from other sources. IRT manages systems to discover compromised IT resources on the company network. Employees must deploy systems to detect compromised IT resources as needed. Employees must notify IRT of compromises that have the potential to impact other units. If one employee becomes aware of a compromised IT resource in another area, the manager of the network or resource containing the compromised resource should be notified, and the IRT should be copied.

II.B.2. **Documentation**. The IRT documents incidents of compromised IT resources in a tracking system. Employees should track compromises in their own tracking system. The employee retains a detailed log, including accurate times, maintained during the incident. The employee ensures preparation of a summary of the incident for:

- How the incident was detected
- Dates
  - Inferred date of compromise
  - Date the compromise was detected
  - Date the incident was contained
  - Date the incident was finally resolved
- Names
  - Person responsible for the IT Resource
  - Person compromising the resource, if known
- Investigation and scope
  - Cause of the compromise
  - Impact of the incident
  - Incident severity
  - Nature of the resolution
  - Proposed improvements

Where appropriate, the IRT should also prepare an incident summary for the users, using the incident as an object lesson to reinforce safe practices.

II.B.3. **Notification**. The recipient list of IRT notifications may be augmented as needed to include staff with appropriate knowledge and skills. Appropriate contacts are notified and recorded in the tracking system. The IT Security Manager will direct notification to all employees, law enforcement and other parties as appropriate.

II.B.4. **Acknowledgment**. IRT notifications should be acknowledged immediately.

II.B.5. **Containment**. IT resources engaged in active attacks against other IT resources must be contained immediately. Unless further investigation requires unrestricted access, all other compromises must be contained as soon as possible, but no later than the same business day in which the notification is received. Service might be interrupted to hosts involved in compromises that are not contained on the same business day. For special consideration regarding service disruption, critical servers can be registered according to procedures detailed earlier in this document. Containment can be achieved by immediately disconnecting the resource from the network, revoking user access, or other means as appropriate. The IT Security Manager may coordinate with the IRT to restrict access to compromised hosts that can't be immediately disconnected or must remain connected in a restricted environment for the purpose investigation or providing service. IRT has the authority to coordinate with Network Services to block compromised services and/or hosts that present a definitive danger to the rest of the network. Notification will follow the procedures outlined in the Service Interruption Notification section above.

II.B.6. **Investigation**. Investigation includes analysis, identification, prioritisation, and evidence collection and retention.

1. Analysis. Compromised hosts must be assessed.
2. Identification. Identify source as appropriate, including user, host or other resource.
3. Evidence Collection and Retention.
    1. If forensic evidence is needed for law enforcement (see Response Procedures for Incidents Involving Law Enforcement), an image of the compromised host must be retained. Email and any other relevant evidence must also be retained.
    2. If the method of compromise is unique or cannot be determined, evidence should be retained to aid in analysis of the incident.

If the incident involves law enforcement, secure evidence without reviewing additional content. Network hardware, software or data may be considered evidence. Care must be taken to preserve evidence. A public records request, subpoena, warrant or other official request must be issued before data is released to law enforcement. Evidence from incidents that involve an immediate threat to persons or property may be provided to law enforcement in advance of a public records request, subpoena or warrant. IRT must be informed of incident investigation details.

II.B.7. **Resolution**. Compromises must be resolved as soon as possible, preferably the day of the notification. Compromised hosts must be reformatted, rebuilt and have vulnerabilities resolved before reconnecting them to the network. However, at the discretion of the IT Security Manager compromised hosts may be cleaned and patched expeditiously. Incidents must be resolved to the satisfaction of the IRT before

compromised hosts are reconnected to the network or filters are lifted. In some cases, the IRT may request privileged access to ensure the host is safe to resume network connectivity, or may require that it be evaluated for vulnerabilities before being placed back in service. IRT must be informed of incident resolution details. Employees responsible for the IT resource that have been compromised must distribute to impacted users a summary of the compromise including:

- Impact on the user's work
- Remediation or preventative measures the users should take

In particular, if passwords have been compromised, they must be reset and changed by the users, once the system has been secured.

II.B.8. **Closure**. IRT reviews the tracking system and closes tickets when appropriate. IRT has primary authority in response decisions for IT security incidents and coordinates incidents from discovery through resolution and closure. IRT can be contacted with any questions regarding incident response.

II.C. Incident Response Procedures for Copyright Infringement

Examples: unlicensed movies, music, or software.

II.C.1. **Discovery**. Any formal copyright complaints received directly from a representative of the copyright holder should be referred to the IT Security Manager. Upon receipt of a complaint, the IT Security Manager will examine the notice of alleged copyright infringement.

1. Identification of the copyrighted work claimed to have been infringed.
2. Identification of the material that is claimed to be infringing and that is to be taken down or disabled, and information “reasonably sufficient” to enable the service provider to locate the materials.
3. Information “reasonably sufficient” to enable the service provider to contact the complainant.
4. A physical or electronic signature of a person authorised to act on behalf of the owner (i.e., the copyright owner or its licensee) of the right that is alleged to be infringed.
5. A statement that the complainant has “a good faith belief” that use of the material in the manner complained of is not authorised by the copyright owner, the owner’s agent, or the law.
6. A statement that the information in the notification is accurate and that, under penalty of perjury, the complainant is authorised to act on behalf of the copyright owner.

II.C.2. **Documentation**. IRT documents alleged copyright infringement complaints in a tracking system.

II.C.3. **Notification**. If the notice substantially complies with A, B, and C above, the IT Security Manager will forward the complaint to the appropriate employee. If the complaint complies with A, B, and C, but does not substantially comply with D, E, and F, more information may be requested from the complainant. Only if the notice does not adequately comply with A, B, and C above or if the complainant does not respond to request for more information can the IT Security Manager disregard the notice.

II.C.4. **Acknowledgment**. Notifications must be acknowledged immediately.

II.C.5. **Containment**. The procedures listed below must be followed upon receipt of a notice of copyright violation:

1. The IT Security Manager will ensure that public access to the material targeted by the complaint is disabled as quickly as reasonably possible..
2. The IT Security Manager will ensure that the person believed to be responsible for the alleged infringing distribution of copyrighted material is notified of the complaint,

and of the action taken to remove access to the material. The person must be given an opportunity to contest the removal of the material if they believe the complainant has misidentified it or if the material is lawful. If required, the IT Security Manager is responsible for a final decision.

3. If the material in question is not legally possessed by the person believed responsible for making it publicly accessible, the IT Security Manager will ensure that the material is removed from the system on which it was found.
4. The IT Security Manager will ensure that the complainant is notified when the material is no longer publicly accessible, and (if appropriate) that the person responsible for distributing the material is contesting its removal.

II.C.6. **Investigation**. If the person responsible for the alleged infringing distribution of copyrighted material believes the material was misidentified or the distribution was lawful, they should send a counter-notification to the IT Security Manager. The counter-notification must contain the following:

1. A physical or electronic signature of the person responsible for the alleged infringing distribution.
2. Identification of the material (or the location of the material) to which public access has been disabled. The identification should match the original identification provided by the complainant.
3. A statement under penalty of perjury that the alleged infringer has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material.
4. The alleged infringer's name, address and telephone number, and a statement that the alleged infringer consents to the appropriate jurisdiction in which the alleged infringer is located and that the alleged infringer will accept service of process from the complainant.

II.C.7. **Resolution**. The IT Security Manager should work with the alleged infringer to obtain any missing components of the counter-notification. When the counter-notification is complete, the IT Security Manager will forward it to the complainant, along with a notification that the removed material may be restored in ten business days unless legal action is commenced against the alleged infringer. If the complainant fails to notify the IT Security Manager that it has initiated legal proceedings within ten business days after receiving a counter-notification, the IT Security Manager will notify the employee that the material may be returned to public distribution.

II.C.8. **Closure**. IRT reviews copyright infringement incidents in the tracking system and closes tickets as appropriate. IRT has primary authority in response decisions for copyright infringement incidents and coordinates incidents from discovery through resolution and closure. IRT can be contacted with any questions regarding incident response.

II.D. Incident Response Procedures for Violations of the Acceptable Use of Computing Resources policy (AUP)

Examples: excessive or disruptive use, complaint, spam, inappropriate content, suspicious activity.

II.D.1. **Discovery**. Employees that identify violations of the company Acceptable Use of Computing Resources policy should take action as reasonably necessary to protect the companies and IT resources, and notify the violator of the action.

II.D.2. **Documentation**. IRT documents AUP violations in a tracking system.

II.D. 3. **Notification**. Employee must respond to the original notification, including content of the original notification, to acknowledge receipt, containment and commencement of the investigation. If any incident involves unauthorized disclosure or acquisition of private data, UF and Level2 Unit ISMs must notify the IT Security Manager. The IT Security Manager will direct notification to law enforcement and other parties as appropriate. Law enforcement should be notified immediately of incidents involving threat to persons or property. IT Security Manager must notify the company Directors of any incident likely to draw public interest.

II.D.4. **Acknowledgment**. IRT notifications should be acknowledged immediately.

II.D.5. **Containment**. AUP violations must be contained immediately. Unless further investigation requires unrestricted access, all other violators must be contained as soon as possible, but no later than the same business day in which the notification is received. Service might be interrupted to violators that are not contained on the same business day. Containment can be achieved by immediately disconnecting the user from the network, revoking user access, or other means as appropriate.

II.D. 6. **Investigation**. If the incident involves law enforcement, secure evidence without reviewing additional content. Network hardware, software or data may be considered evidence. Care must be taken to preserve evidence. A public records request, subpoena, warrant or other official request must be issued before data is released to law enforcement. Evidence from incidents that involve an immediate threat to persons or property may be provided to law enforcement in advance of a public records request, subpoena or warrant. IRT must be informed of incident investigation details.

II.D. 7. **Resolution**. IRT must be informed of incident resolution details.

II.D.8. **Closure**. IRT reviews the tracking system and closes tickets as appropriate. IRT has primary authority in response decisions for IT security incidents and coordinates

incidents from discovery through resolution and closure. IRT can be contacted with any questions regarding incident response.

II.E. Incident Response Procedures for Suspicious Activity

Examples: sweeps, scans, unusual connections, excessive bandwidth consumption

II.E.1. **Discovery**. IRT receives and processes discovery notifications from other sources. IRT manages systems to discover suspicious activity on the company network. Employees are responsible to deploy systems to detect suspicious activity within their unit as needed, as directed by the IT Security Manager. Employees must notify IRT of suspicious activity that has the potential to impact other resources or employees. If one employee becomes aware of a suspicious activity by another employee, the IT Security Manager should be notified.

II.E.2. **Documentation**. IRT documents suspicious activity in a tracking system.

II.E. 3. **Notification**. When suspicious activity is discovered by the Incident Response Team, appropriate contacts are notified The IRT notifications may be augmented as needed to include staff with appropriate knowledge and skills. Employees must respond to the original notification, including content of the original notification, to acknowledge receipt, containment and commencement of the investigation. If any incident involves unauthorised disclosure or acquisition of private data, the IT Security Manager must be notified. Law enforcement should be notified immediately of incidents involving threat to persons or property. The IT Security Manager should be consulted regarding other incidents before contacting law enforcement.

II.E.4. **Acknowledgment**. IRT notifications should be acknowledged immediately.

II.E.5. **Containment**. Suspicious activity should be contained as appropriate until the investigation is complete or the incident is resolved. Containment can be achieved by immediately disconnecting the resource from the network, revoking user access, or other means as appropriate. Employees may coordinate with the IRT to restrict access to compromised hosts that can't be immediately disconnected or must remain connected in a restricted environment for the purpose investigation or providing service. IRT has the authority to coordinate with Network Services to block compromised services and/or hosts that present a definitive danger to the rest of the network.

II.E. 6. **Investigation**. Investigation includes analysis and identification.

1. Analysis. Suspicious activity must be assessed.
2. Identification. Identify source as appropriate, including user, host or other resource.

IRT must be informed of investigation details.

II.E.7. **Resolution**. Suspicious activity must be resolved as soon as possible, preferably the day of the notification. IRT must be informed of resolution details.

II.E.8. **Closure**. IRT reviews the tracking system and closes tickets as appropriate.

III. Additional Incident Response Standards, Procedures, and Guidelines

III.A. Critical IT Resources Standard

A critical IT resource is vital to the function of the company. It might store sensitive data, confidential data, or data protected by law. Critical IT resources may need special consideration with respect to risk assessment, service interruption, and notification.

III.B. Critical IT Resource Registration Procedures

Employees can submit a written request to register critical IT resources with the IT Security Manager. All submissions for classification as a critical IT resource will be reviewed by the IT Security Manager and considered for approval by the IRT.

III.C. Service Interruption Notification Procedures

Employees will be notified prior to or concurrent with a service interruption applied as the result of a security incident.

III.D. Incident Tracking Standard

All security incidents involving IT resources must be tracked. The company incident tracking system is intended to monitor progress toward incident resolution and to store data that can be used for incident trend analysis. To ensure accountability and assessment, the IT Security Manager will provide incident trend analysis to the company Directors as requested. The IT Security Manager maintains an IT security incident tracking system for incidents that it processes. Employees should implement a tracking system for incidents in their unit as required. Security incident tickets contain the following information, but are subject to change:

1. Contacts: A list of all contacts notified about the incident.
2. Employee name:.
3. Diary: Incident details must be recorded each time the ticket is updated.
4. Filter: Relevant information about filters associated with an incident are tracked.
5. Incident status
    - New: Opened, but not assigned to individual on IRT.
    - Assigned: Responsibility assigned to individual on IRT.
    - Contained: Threat is contained usually via some form of access restriction, but incident is not fully resolved.
    - Dormant: Contacts did not respond to the IRT notification and no further activity was observed for one month. The status of tickets with associated filters can not be changed to Dormant.
    - Resolved: All appropriate actions have been completed.
    - Closed: IRT concurs that the incident is resolved.

- False Positive: Erroneous ticket.

6. Incident severity classification (see Incident Classification Guidelines below)
    - Class 3: Any of the following.
        - Critical Data
        - Involves serious legal issues
        - Service disruption impacting institution
        - Active threat
        - Widespread
        - Public interest
    - Class 2: Not Class 3 and any of the following.
        - Sensitive Data
        - Involves less serious legal issues or potential for legal issues
        - Service disruption impacting unit or potential for disruption impacting institution
        - Potential for threat
        - Somewhat widespread
        - Potential for public interest
    - Class 1: Not Class 3 or Class 2.
        - Unrestricted Data
        - No legal issues
        - No potential for service disruption impacting institution
        - No threat
        - Not widespread
        - No public interest
7. Incident type
    - Vulnerability
    - Compromise/Attack
    - Copyright violation
    - AUP violation
    - Suspicious activity
    - Other
8. Operating systems of host
    - Windows
    - Macintosh
    - Unix
    - Unknown/Other

III.E. Incident Severity Classification Guidelines

Incident severity classifications are described below. Severity classifications are used for incident trend reporting. If there is any doubt about the classification of an incident, the higher severity classification should be used. Incident classifications may be changed at the discretion of the IT Security Manager. The following criteria are evaluated to determine incident classification.

1. Data classification
2. Legal issues
3. Magnitude of service disruption
4. Threat potential
5. Expanse
6. Public interest

To determine the severity classification for the incident tracking systems, employees are asked to affirm the following assertions regarding each incident.

- There is a reasonable expectation that critical data was acquired by an unauthorised person as a result of this incident.
- There is a reasonable expectation that sensitive data was acquired by an unauthorised person as a result of this incident.
- There is reasonable expectation that confidential or security-related information was acquired by an unauthorised person.
- Data protected by privacy legislation is involved.
- Disclosure of company intellectual property is involved.
- This incident involves legal violation(s).
- This incident impacts company mission critical services.
- There is strong potential this incident might impact company mission critical services.
- There is active public interest in this incident.
- There is strong potential for active public interest in this incident.
- Hosts involved in this incident are actively attacking other hosts.
- There is strong potential for attack from hosts involved in this incident.
- This incident is widespread.
- This incident is somewhat widespread.

Class 3: Highest Severity

If the answer is ‘yes’ to any of the following questions regarding an incident, then it is a Class 3 incident.

1. Data security. Is there a reasonable expectation that critical data was acquired by an unauthorised person as a result of this incident?
    1. Are data protected by privacy rules or legislation involved? For example:
        1. Non-directory employee data
        2. Bank account, credit card, or other private financial information
        3. Drivers license number
        4. Any medical records or protected health information
    2. Is intellectual property involved? For example:
        1. Company trade secrets
    3. Are other data security issues involved? For example:
        1. Passwords, risk assessments, or other security-related data.
        2. Data restricted by legal contracts, memorandums of understanding, or other agreements.
        3. Data, if available to unauthorised users, will cause harm to an individual, a group or the institution.
2. Legal issues. Does this incident involve any legal violation?
    1. Threat to persons or property
    2. Theft greater than $10,000
    3. Child pornography
    4. Copyright violations
        1. Warez server
        2. Unauthorised P2P server of music, movies, or other content protected by copyright
3. Magnitude of service disruption. Does this incident impact company mission critical services?
4. Threat. Are hosts involved in this incident actively attacking other hosts?
5. Expanse. Is this incident widespread?
6. Public interest. Is there active public interest in this incident?

Class 2: Medium Severity

If the answer is ‘no’ to all of the Class 3 questions above, but ‘yes’ to any of the following questions, then it is a Class 2 incident.

1. Data Security. Is there a reasonable expectation that Sensitive data was acquired by an unauthorised person as a result of this incident? For example:
    1. Infrastructure diagrams such as building and network
    2. Strategy documents
    3. Financial information
    4. Purchasing information
    5. Policies, standards, and procedures
    6. Business recovery plans
    7. System configurations
    8. Emergency response plans
    9. Emergency equipment inventories
2. Legal issues. Does this incident involve a legal violation? For example:
    1. Theft less than $10,000
    2. Harassment
3. Magnitude of service disruption. Is it likely that this incident will impact company mission critical services?
4. Threat. Is an attack likely to occur from hosts involved in this incident?
5. Expanse. Is this incident somewhat widespread?
6. Public interest. Is there likely to be public interest in this incident?

Class 1: Lowest Severity

If the answer is ‘no’ to all of the Class 2 and Class 3 questions above, then it is a Class 1 incident.

IV. Appendix

IV.A. Summary of Response Procedures for Incidents Involving Law Enforcement

Examples: obscenity, stalking, threat to persons or property, child pornography, unauthorised access.

IV.A.1. **Evidence retention**. Secure evidence without reviewing additional content. Network hardware, software or data may be considered evidence. Care must be taken to preserve evidence.

IV.A.2. **Evidence release**. A public records request, subpoena, warrant or other official request must be issued before data is released to law enforcement. Contact IT Security Manager to review public records requests, subpoenas, and warrants before responding. Evidence from incidents that involve an immediate threat to persons or property may be provided to law enforcement in advance of a public records request, subpoena or warrant, but IT Security Manager should be contacted if time allows.

IV.A.3. **Notifications**. If any incident involves unauthorised disclosure or acquisition of private data, the IT Security Manager must inform the company Directors. The IT Security Manager will direct notification law enforcement and other parties as appropriate. Law enforcement should be notified of incidents involving an immediate threat to persons or property. The IT Security Manager should be consulted regarding other incidents before contacting law enforcement.

IV.B. Summary of Incident Response for Legal Issues

Examples: defamation, civil fraud, harassment, disclosure of intellectual property or company trade secrets.

IV.B.1. **Evidence retention**. Secure evidence without reviewing additional content. Contact the IT Security Manager.

IV.B.2. **Notifications**. If any incident involves unauthorised disclosure or acquisition of private data, the IT Security Manager must be notified. The IT Security Manager will direct notification to the company Directors, law enforcement and other parties as appropriate.

IV.C. Summary of Internal and Public Communication Notification Procedures

Upon receipt of notifications from IRT, employees must respond as directed in the notification. All employees must notify IRT immediately upon discovery of security incidents that impact resources. If any incident involves unauthorised disclosure or acquisition of private data, the IT Security Manager must notify the company Directors. When evidence of a possible crime is discovered, employees should report it to the IT

Security Manager. The IT Security Manager must consult company Directors before responding to public records requests, subpoenas, warrants or other requests for assistance from law enforcement unless there is an immediate threat to persons or property. The IT Security Manager should consult company Directors if there is any doubt about whether an incident should be reported to law enforcement. Law enforcement should be notified of incidents involving:

- Threats to persons or property
- Damages in excess of $10,000
- Child pornography

Other incidents should be reported to law enforcement according to the judgment of the IT Security Manager. Individual employees might have public relations contacts that must be notified before responding to any inquiry from the press; for more information, consult the IT Security Manager, before responding to any inquiry from the press.The IT Security Manager must consult the company Directors regarding any incident that draws public attention or is expected to draw public attention. Employees should coordinate with the IT Security Manager to create a public communication plan for any incident likely to attract public interest.