Education
Advisory
Board

IT Forum

IT Breach Preparation and Response Toolkit

Resources for Effective Planning and Mitigation

IT Forum

Practice Manager

Laura Whitaker

Research Analyst

Ben McGuire

LEGAL CAVEAT

The Advisory Board Company has made efforts to verify the accuracy of the information it provides to members. This report relies on data obtained from many sources, however, and The Advisory Board Company cannot guarantee the accuracy of the information provided or any analysis based thereon. In addition, The Advisory Board Company is not in the business of giving legal, medical, accounting, or other professional advice, and its reports should not be construed as professional advice. In particular, members should not rely on any legal commentary in this report as a basis for action, or assume that any tactics described herein would be permitted by applicable law or appropriate for a given member's situation. Members are advised to consult with appropriate professionals concerning legal, medical, tax, or accounting issues, before implementing any of these tactics. Neither The Advisory Board Company nor its officers, directors, trustees, employees and agents shall be liable for any claims, liabilities, or expenses relating to (a) any errors or omissions in this report, whether caused by The Advisory Board Company or any of its employees or agents, or sources or other third parties, (b) any recommendation or graded ranking by The Advisory Board Company, or (c) failure of member and its employees and agents to abide by the terms set forth herein.

The Advisory Board is a registered trademark of The Advisory Board Company in the United States and other countries. Members are not permitted to use this trademark, or any other Advisory Board trademark, product name, service name, trade name, and logo, without the prior written consent of The Advisory Board Company. All other trademarks, product names, service names, trade names, and logos used within these pages are the property of their respective holders. Use of other company trademarks, product names, service names, trade names and logos or images of the same does not necessarily constitute (a) an endorsement by such company of The Advisory Board Company and its products and services, or (b) an endorsement of the company or its products or services by The Advisory Board Company. The Advisory Board Company is not affiliated with any such company.

IMPORTANT: Please read the following.

The Advisory Board Company has prepared this report for the exclusive use of its members. Each member acknowledges and agrees that this report and the information contained herein (collectively, the "Report") are confidential and proprietary to The Advisory Board Company. By accepting delivery of this Report, each member agrees to abide by the terms as stated herein, including the following:

1. The Advisory Board Company owns all right, title and interest in and to this Report. Except as stated herein, no right, license, permission or interest of any kind in this Report is intended to be given, transferred to or acquired by a member. Each member is authorized to use this Report only to the extent expressly authorized herein.
2. Each member shall not sell, license, or republish this Report. Each member shall not disseminate or permit the use of, and shall take reasonable precautions to prevent such dissemination or use of, this Report by (a) any of its employees and agents (except as stated below), or (b) any third party.
3. Each member may make this Report available solely to those of its employees and agents who (a) are registered for the workshop or membership program of which this Report is a part, (b) require access to this Report in order to learn from the information described herein, and (c) agree not to disclose this Report to other employees or agents or any third party. Each member shall use, and shall ensure that its employees and agents use, this Report for its internal use only. Each member may make a limited number of copies, solely as adequate for use by its employees and agents in accordance with the terms herein.
4. Each member shall not remove from this Report any confidential markings, copyright notices, and other similar indicia herein.
5. Each member is responsible for any breach of its obligations as stated herein by any of its employees or agents.
6. If a member is unwilling to abide by any of the foregoing obligations, then such member shall promptly return this Report and all copies thereof to The Advisory Board Company.

Table of Contents

Organizing for an Inevitable Threat

Minimizing the Costs of Persistent Security Challenges

The Data Security Environment

- The interconnected digital world brings incredible opportunities for learning and discovery, while creating new risks and challenges to safety and security. As stewards of private information, intellectual property, and valuable research assets, higher education information technology leaders are at the center of a global war for data.
- Whether by accidental loss of a protected device, petty theft, major criminal activity, or international espionage, breaches in data security are not a question of if but of when. While Chief Information Officers may not directly control department policies, effective preparation and processes may reduce the likelihood, duration, and cost of data breaches.

New Threats and Challenges

- Escalating risks include advanced criminal networks and foreign attacks on research – the Privacy Rights Clearinghouse identified 200 hacking and malware attacks on higher education institutions between 2005 and 2013.[1]
- More data is at risk due to mobile device proliferation, new demands for wireless access to protected data, and external collaboration with many private vendors. Increasing access to an ever growing source of information increases both the attraction and opportunity for attacks.
- While risks multiply, IT leaders may struggle to exert significant influence on security policy across institutional siloes. When projects and data move across institutional boundaries, information security is only as strong as the weakest participant.

The Costs of Inaction

- Ineffective procedures for a security breach can put sensitive information at risk and damage the reputation of the CIO and IT function, if not the whole institution. With breach mitigation estimated to cost over $100 per compromised record, costs can escalate quickly.[2]
- Minor incident response might cost an institution in the low thousands, but a recent data breach at Maricopa Community College District in Arizona is estimated to cost the system at least $17 million; data security breaches can impact the life of every campus constituency.[3]
- While the IT team might identify and repair a security threat quickly, the escalating costs of investigation and verification can take months away from the most valuable technology staff, necessitate expensive vendor consultation, and result in lasting damage to the institution’s reputation.

[1] Chronology of Data Breaches, Privacy Rights Clearinghouse, https://www.privacyrights.org/data-breach.

[2] 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute and Symantec.https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf.

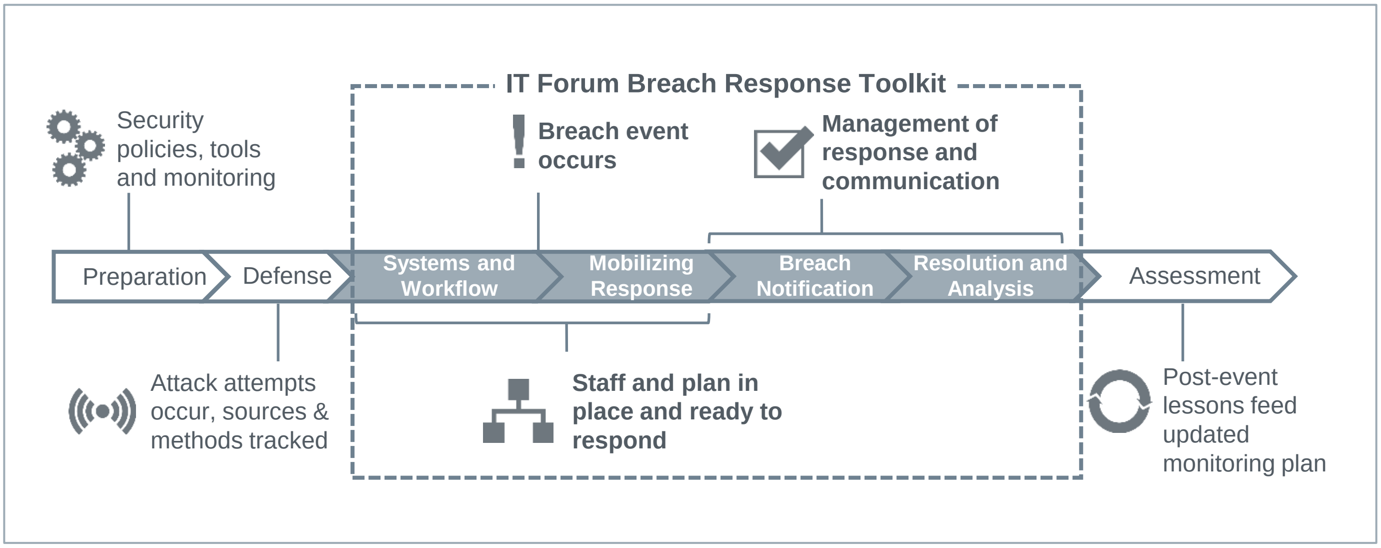
[3] Maricopa Community Colleges considers tuition, tax hikes after security incident, Arizona Newszap, http://arizona.newszap.com/eastvalley/130328-114/maricopa-community-colleges-considers-tuition-tax-hikes-after-security-incident

Tools for Effective Preparation and Response

The Purpose of This Toolkit

This toolkit provides guidance on preparation and planning steps that will help members lay the groundwork for effective breach response. As depicted in the graphic below, these resources address only a segment of the data security framework. Use the advice and templates here to:

- Expedite breach response
- Reduce cost of both breach and response
- Minimize risk to the institution if a breach occurs
- Protect the reputation of the institution


IT Forum Breach Response Toolkit
Security policies, tools and monitoring
Breach event occurs
Management of response and communication
Preparation
Defense
Systems and Workflow
Mobilizing Response
Breach Notification
Resolution and Analysis
Assessment
Attack attempts occur, sources & methods tracked
Staff and plan in place and ready to respond
Post-event lessons feed updated monitoring plan

Laying the Groundwork for Response

The last thing a technology leader needs to do during a data emergency is quibble over wording or worry about the chain of command. An effective plan provides clear, unequivocal definitions of a data breach, and staff members responsible for identification and response.

These frames for critical definitions and decision ownership are illustrative, combined from the existing plans of several institutions; the most effective policies will reflect campus-specific culture and policies.

Artifact A: **The University of Iowa's** Incident Response Team's Workflow (p. 14) provides a visualization of incident triage.

Developing a Consistent Workflow to Triage Incidents

Does the Breach Affect a Critical System?

- *Hierarchy of Priorities:*
  - Human Life and Safety
  - Sensitive and Regulated Information*
  - Critical Networks and Systems
  - Business Continuity
  - Internal Customer Service

Who Owns Decisions During the Breach?

- *Security Officer*
  - Detect and Report Incident
- *Chief and Deputy Information Officer*
  - Approve Incident Category
  - Manage Internal Communication
- *Incident Response Leader*
  - Build Incident Response Team

Maintain a pool of potential incident response leaders that will be ready to lead breach operations when necessary; leaders will most likely come from the central IT office, but knowledge and operational ability trump department.

Response leaders need to be empowered to make spending and notification decisions, and will range in seniority appropriate to their incident.

Asking leaders to collect response metrics (e.g., mean time to fix problem) will help technology leaders measure the effectiveness of procedures against different breach types, and improve future response.

Incident Leader Coordinates, Measures Response

Responsibilities of the Incident Response Leader

Manage Internal Communication

- Define incident priority level and notify CIO if necessary
- Update key staff (e.g., CIO, General Counsel) on breach during investigation

Staff Response Team

- Recruit technical staff members with experience in compromised data
- As necessary, involve escalating group of key participants

Ensure Data Collection

- With technical team members, collect forensic evidence and KPI's
- Compile report on data breach and response for future security preparation

!

Incident Response is a 'Drop Everything' Priority

Make sure that response leaders have the authority to clear all other team responsibilities during response.

* At many institutions, this will include licensed research and other high-value targets.

Organizing Staff and Resources

When a breach occurs, quick action can staunch losses and expedite the mitigation process. Make sure that response leaders know and are authorized to carry out the actions that will mobilize response, limit damage, and collect necessary data on the breach.

Artifacts B-C: **Indiana University** templates for breach reporting and response (p. 15-16).

Know the Necessary Immediate Steps

Mobilize Response

- *Limit Damage:*
  - Limit and secure access to compromised systems
  - If necessary, shut down affected machines and networks until forensic support arrives
- *Alert Team:*
  - Activate response leaders, who will be responsible for pulling in support personnel
  - Alert external response component groups (e.g., forensic data specialists)

Collect Information

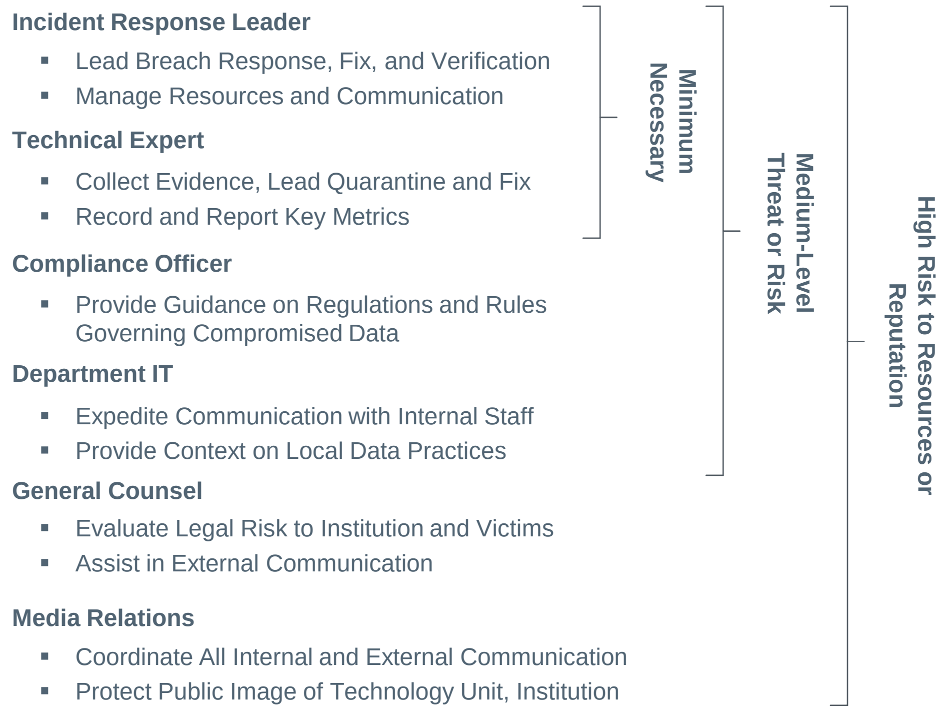
- *Document Key Facts:*
  - Record date and time of breach incident, breach discovery, and when response efforts began
  - Record who discovered the breach, reporting chain, and who on campus has been notified
- *Begin Assessment and Analysis*
  - Estimate impact to institution and possible victims
  - Prioritize response and notification components

A large team can slow response at a critical juncture, but too few participants can generate legal and reputational risk. Criteria that define initial steps and critical systems should build in recommendations for participation in the incident response team (e.g., type of impacted data, media relations, legal vulnerability).

Incident response leaders should prioritize capabilities above formal titles, and maintain a working knowledge of cross-departmental information technology functions.

Artifact D: See sample guidelines for a more comprehensive possible listing of incident roles (p. 17-21).

Escalate the Response Team With the Incident


Minimum Necessary
Medium-Level Threat or Risk
High Risk to Resources or Reputation

Incident Response Leader
- Lead Breach Response, Fix, and Verification
- Manage Resources and Communication

Technical Expert
- Collect Evidence, Lead Quarantine and Fix
- Record and Report Key Metrics

Compliance Officer
- Provide Guidance on Regulations and Rules Governing Compromised Data

Department IT
- Expedite Communication with Internal Staff
- Provide Context on Local Data Practices

General Counsel
- Evaluate Legal Risk to Institution and Victims
- Assist in External Communication

Media Relations
- Coordinate All Internal and External Communication
- Protect Public Image of Technology Unit, Institution

Source: Advisory Board interviews and analysis.

Notifying Authorities and Constituents

The appropriate level of outside notification during a data breach depends on many factors, not the least of which is the university's legal position. The same policies that define critical incidents and systems should provide guidance on which data breach service providers and community contacts should be a part of the post-incident process.

Artifact E-F: Review your procedures and contact preparation with Experian's Preparedness Plan Audit (p. 22) and Sample Breach Vendor Contact Cards (p. 23).

Prepare to Move Past the Rolodex

Data Breach Services

- Forensic Investigators
- Private Investigators
- Outside Legal Counsel
- Mailing Services
- Call Centers
- Public Relations Firms

Community Contacts

- Law Enforcement
- Local Media Outlets
- Vendors Connected with Compromised Data
- Professional Organizations Affected by Breach

Keep All Response Leaders Updated with Key Contacts

Review lists of breach service providers and community contacts at least quarterly, and make sure all response leaders have accurate information when launching into team recruitment and investigation.

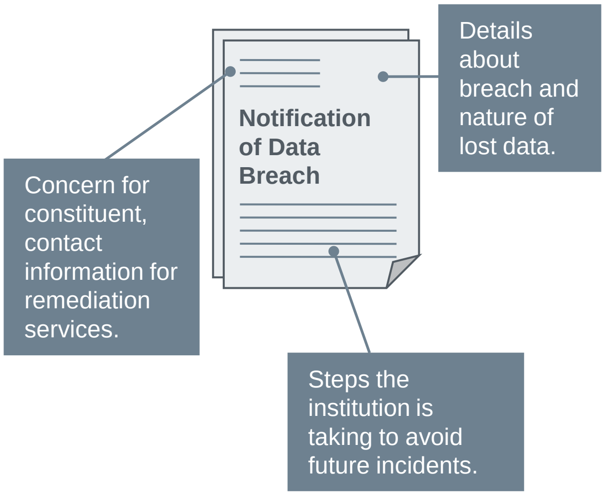
While IT professionals understand the persistent challenges of data breaches, others involved may not react appropriately to incidents. Be prepared for a range of attitudes, from fear and anger to ambivalence.

Seek support from legal counsel and compliance units to pre-draft press release and victim notification language. This can expedite administrative tasks during a breach and ensure rapid response.

Artifacts H-I: This press release from the **University of Indiana** (p. 25) and sample notification letter from the **University of California at Irvine** (p. 26-28) provide representative templates.

Strike the Right Tone

Sample Notification Letter



Notification of Data Breach

Details about breach and nature of lost data.

Concern for constituent, contact information for remediation services.

Steps the institution is taking to avoid future incidents.

Remember that a breach can damage relationships with students, staff, and vendors. Ensure that every detail of external communication expresses sincere apologies and conveys determination to do better – down to the quality of paper used in outreach.

Artifact G: See more tips for Breach Communication on page 24.

Source: Advisory Board interviews and analysis.

Analysis and Process Improvement

A data breach can hurt constituents, incur significant costs, and damage the reputation of the IT function as well as the larger institution.

However, devoting the most skilled and valuable staff to forensic analysis and verification of breach processes can sap IT's ability to move past an incident and improve future risk management. Consider how more effective preparatory steps and response processes can improve time-based metrics.

Artifact J: The Ponemon Institute's 2014 survey on cyber security issues provides a lens into industry practices (p. 29).

The Key Performance Indicators of Effective Response

Standard Model

- Did we detect the breach and understand the problem?
- Did we assign an appropriate incident response team?
- Did we fix the problem?
- Did we notify the appropriate authorities and affected parties?
- Is service restored?

Progressive Model*

- Measure Mean Time to:
  - ✓Identify: How long between breach and detection?
  - ✓Know: How long between detection and understanding of root causes?
  - ✓Fix: How long to resolve the situation and restore service?
  - ✓Verify: How long to confirm resolution with affected parties?

If You Had One Security Breach Analysis Tool…

Private industry respondents report* that storage of audit trails using a packet capture system or SIEM (security incident and event manager) tool is the most effective way to detect and analyze security breaches.

Conduct a risk assessment of the entire organization and use it as a basis for a remediation plan. Often, assessments and remediation plans are reviewed and monitored by external auditors to ensure management attention and participation. An institution's Board of Trustees may also want to be briefed on these regularly.

Breach plan language, process documents, and discussions should focus on the connections between incident response and effective risk management rather than treat breaches as isolated incidents.

Build New Threat Indicators into Future Planning

Outside Attacks and Threat Indicators

- What was the source of the attack?
- What are the key characteristics of the attacking individual or group?
- What was the vulnerability exploited (e.g., social engineering, poor security architecture)?
- How can future response processes and communications for similar incidents be improved?

Inside Theft and Accidental Exposure

- What was the source of the theft or loss?
- What vulnerabilities were exploited or exposed by the incident?
- Has the responsible employee or department caused problems before?
- Can improved awareness and trainings for local staff prevent future similar incidents?

"Cyber Security Incident Response: Are we as prepared as we think?" Ponemon Institute LLC, January 2014. http://www.lancope.com/files/documents/Industry-Reports/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf/.

Self-Diagnostic for Breach Response Preparation

□ Standard Practice ▒ Strong Practice ■ Advanced Practice

Plan

		Yes	No
□	▪ *I have a breach plan in place.*	□	□
□	▪ *My breach plan is approved by the General Counsel and compliance staff.*	□	□
▒	▪ *My breach plan is reviewed and updated on a regular basis.*	□	□
▒	▪ *My breach plan defines response based on all critical data systems and information types.*	□	□
▒	▪ *My breach plan recommends staffing and support based on breach and data types.*	□	□
■	▪ *My breach plan defines which technology, security, and legal staff are responsible for early incident triage.*	□	□

Process

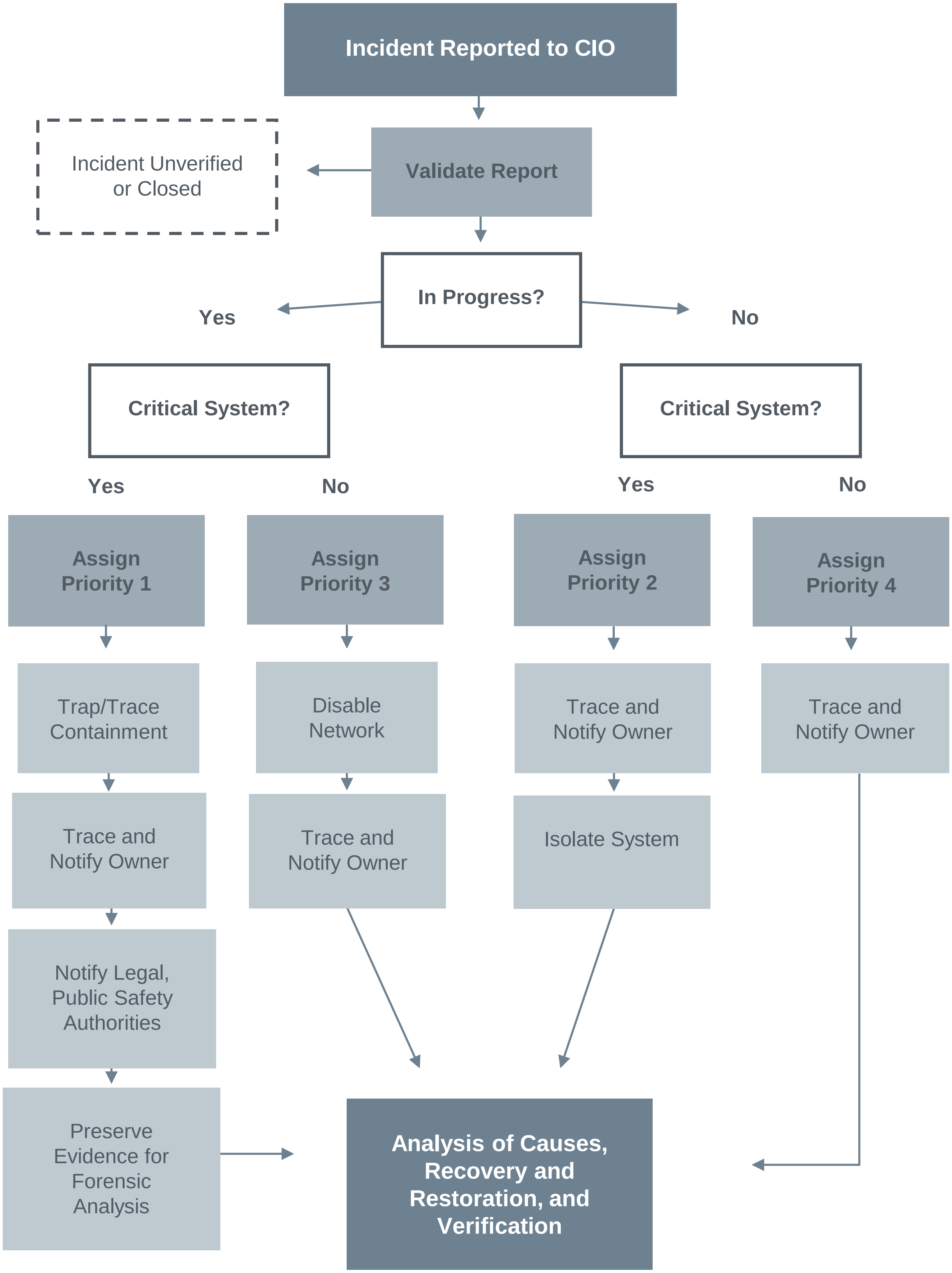
□	▪ *I have a pool of incident leaders ready to coordinate and lead response when necessary.*	□	□
▒	▪ *Incident leaders understand the minimum staffing and resources necessary to meet forensic investigation needs, and when to escalate staffing to meet a more critical incident.*	□	□
■	▪ *Technical staff are capable of collecting key performance indicators (e.g., mean time to identification) for response analysis.*	□	□

Preparation

□	▪ *I have drafted template release and notification documents approved by the General Counsel.*	□	□
□	▪ *I have a list of local breach services vendors and community contacts on hand and with all breach response leaders.*	□	□
▒	▪ *I verify and update all contact lists at least once quarterly.*	□	□
■	▪ *After each incident, staff feed new threat indicators into security training, awareness, and response procedures.*	□	□

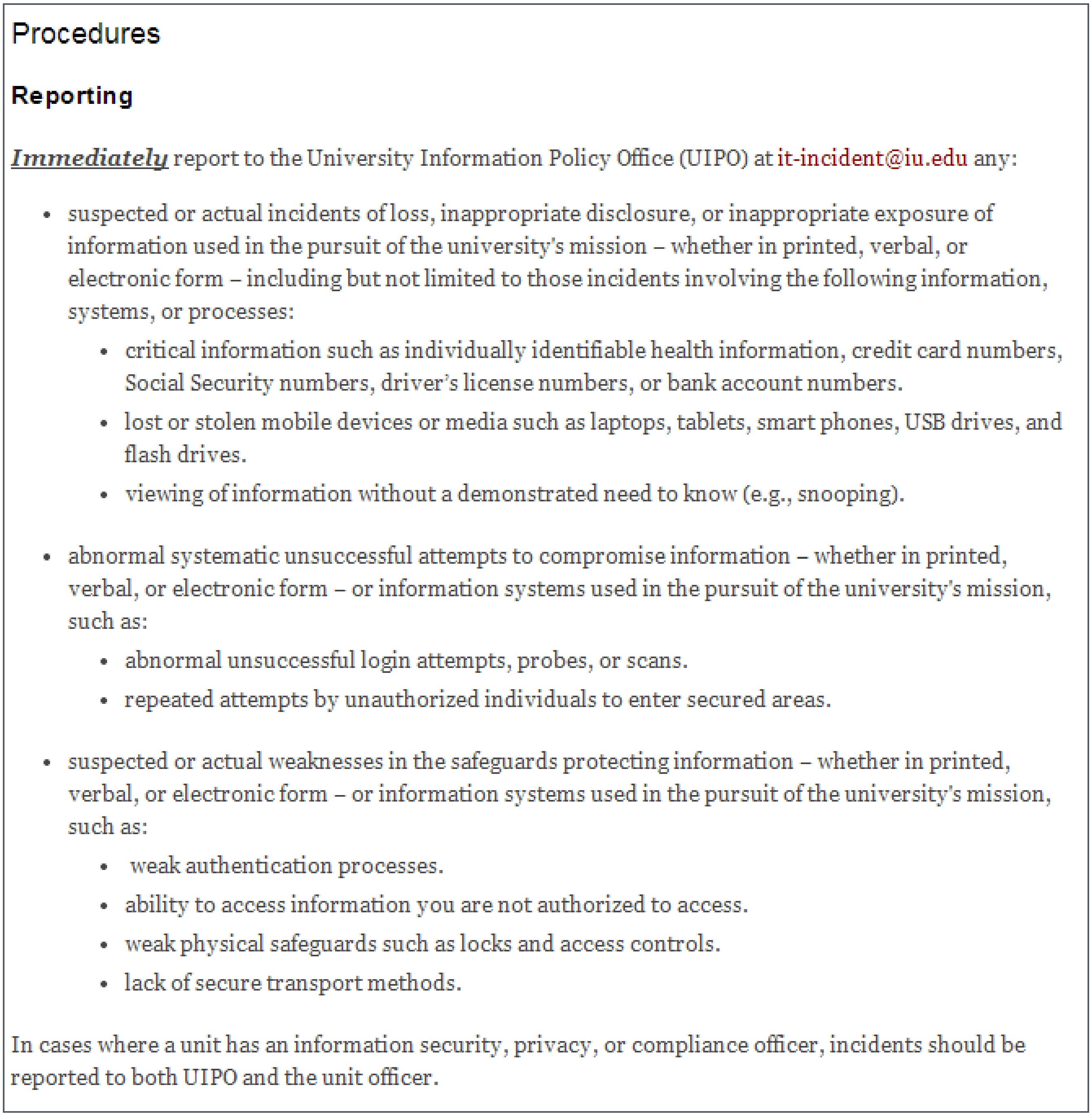
Appendix: **Artifacts** for Your Breach Toolkit

Artifact A: University of Iowa I-CSIRT Breach Response Workflow



Adapted from Iowa Computer Security Incident Response Team (I-CSIRT) Flow 5/6/2010, http://itsecurity.uiowa.edu/resources/documents/i-csirt-flowchart.pdf.

Artifact B: Indiana University Breach Reporting Guidelines



Procedures

Reporting

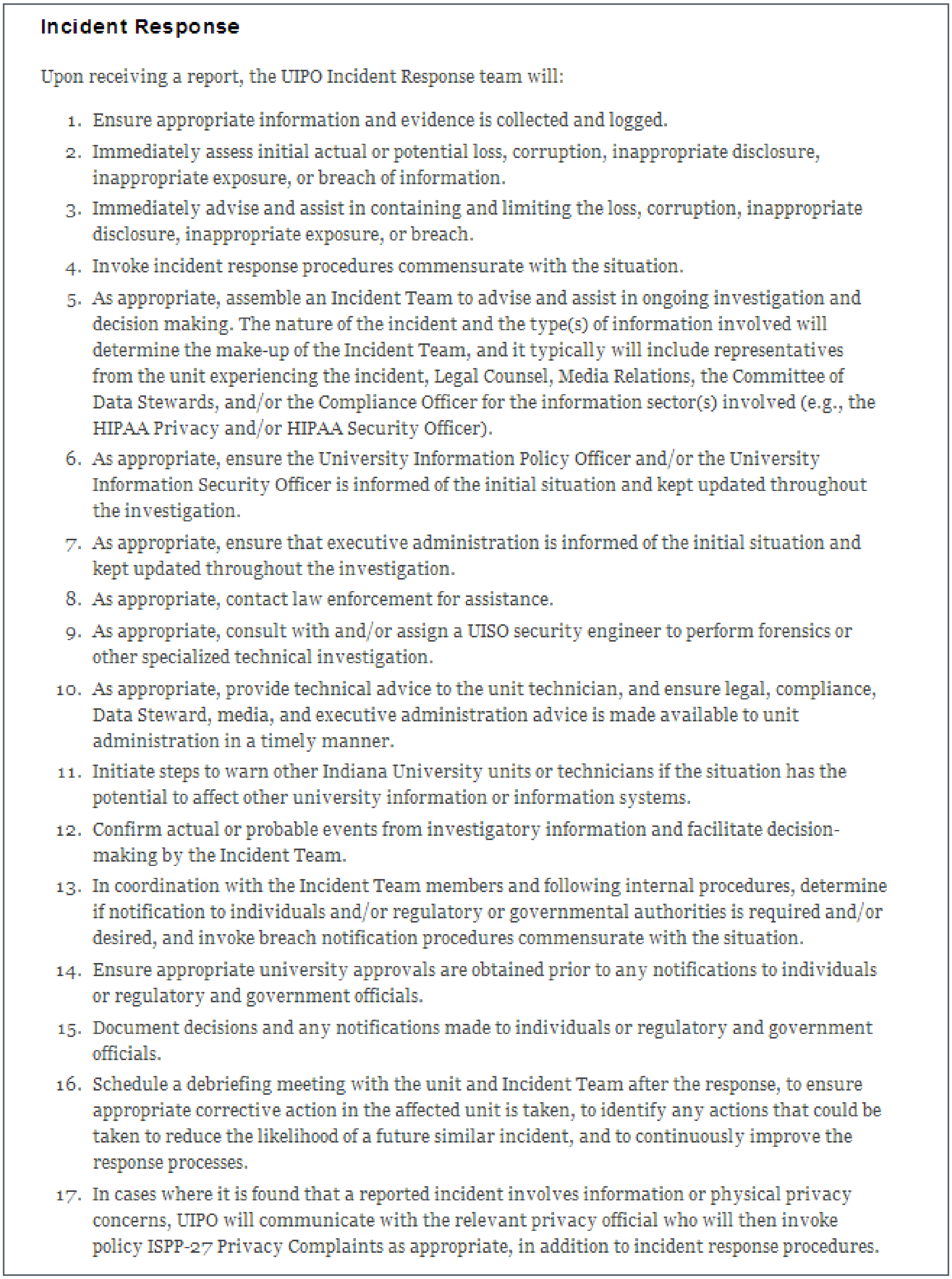
Immediately report to the University Information Policy Office (UIPO) at it-incident@iu.edu any:

- suspected or actual incidents of loss, inappropriate disclosure, or inappropriate exposure of information used in the pursuit of the university's mission – whether in printed, verbal, or electronic form – including but not limited to those incidents involving the following information, systems, or processes:
    - critical information such as individually identifiable health information, credit card numbers, Social Security numbers, driver's license numbers, or bank account numbers.
    - lost or stolen mobile devices or media such as laptops, tablets, smart phones, USB drives, and flash drives.
    - viewing of information without a demonstrated need to know (e.g., snooping).
- abnormal systematic unsuccessful attempts to compromise information – whether in printed, verbal, or electronic form – or information systems used in the pursuit of the university's mission, such as:
    - abnormal unsuccessful login attempts, probes, or scans.
    - repeated attempts by unauthorized individuals to enter secured areas.
- suspected or actual weaknesses in the safeguards protecting information – whether in printed, verbal, or electronic form – or information systems used in the pursuit of the university's mission, such as:
    - weak authentication processes.
    - ability to access information you are not authorized to access.
    - weak physical safeguards such as locks and access controls.
    - lack of secure transport methods.

In cases where a unit has an information security, privacy, or compliance officer, incidents should be reported to both UIPO and the unit officer.

Information and Information System Incident Reporting, Management, and Breach Notification, http://policies.iu.edu/policies/categories/information-it/ispp/ISPP-26.shtml.

Artifact C: Indiana University Breach Response Guidelines



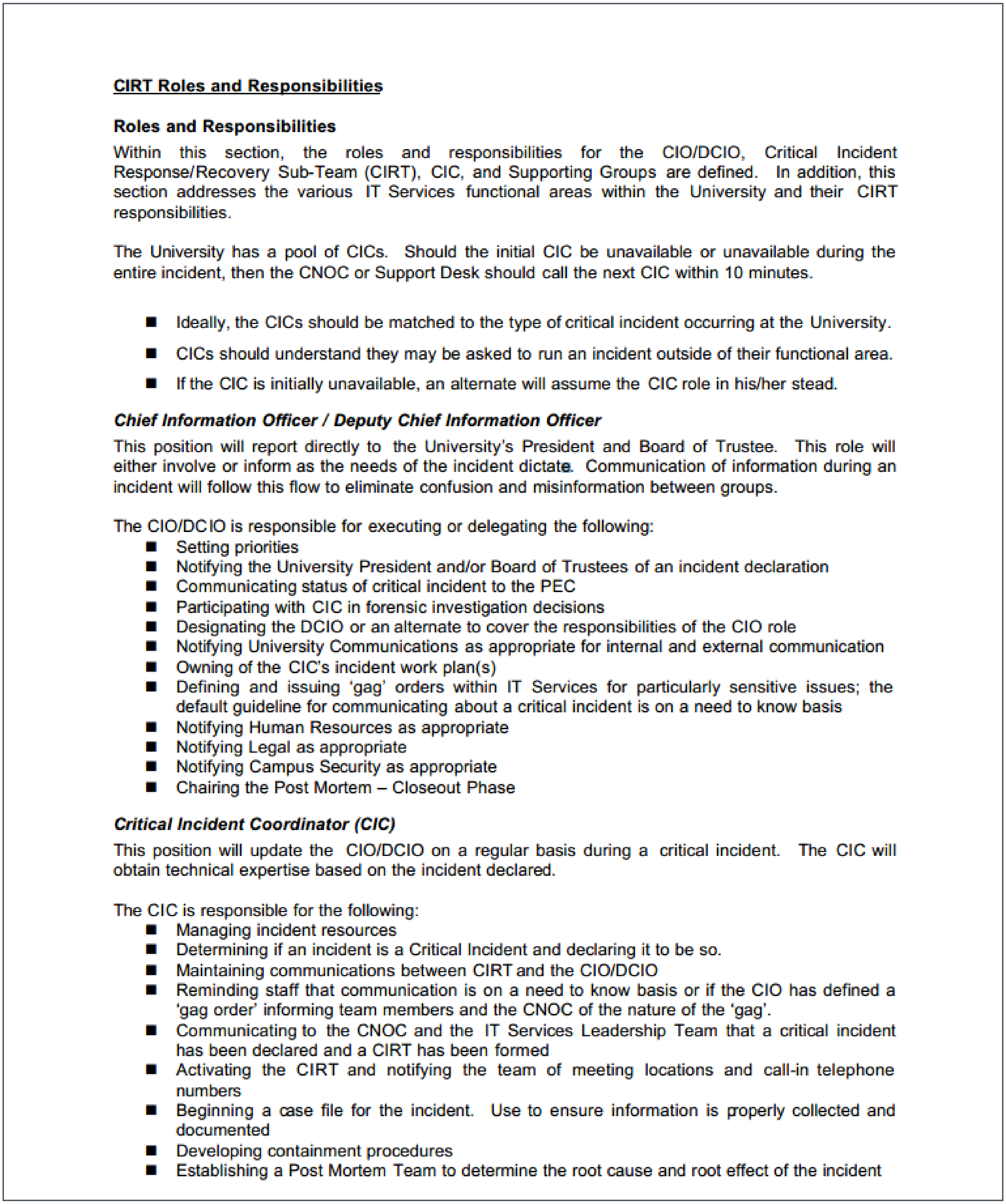
Incident Response

Upon receiving a report, the UIPO Incident Response team will:

1. Ensure appropriate information and evidence is collected and logged.
2. Immediately assess initial actual or potential loss, corruption, inappropriate disclosure, inappropriate exposure, or breach of information.
3. Immediately advise and assist in containing and limiting the loss, corruption, inappropriate disclosure, inappropriate exposure, or breach.
4. Invoke incident response procedures commensurate with the situation.
5. As appropriate, assemble an Incident Team to advise and assist in ongoing investigation and decision making. The nature of the incident and the type(s) of information involved will determine the make-up of the Incident Team, and it typically will include representatives from the unit experiencing the incident, Legal Counsel, Media Relations, the Committee of Data Stewards, and/or the Compliance Officer for the information sector(s) involved (e.g., the HIPAA Privacy and/or HIPAA Security Officer).
6. As appropriate, ensure the University Information Policy Officer and/or the University Information Security Officer is informed of the initial situation and kept updated throughout the investigation.
7. As appropriate, ensure that executive administration is informed of the initial situation and kept updated throughout the investigation.
8. As appropriate, contact law enforcement for assistance.
9. As appropriate, consult with and/or assign a UISO security engineer to perform forensics or other specialized technical investigation.
10. As appropriate, provide technical advice to the unit technician, and ensure legal, compliance, Data Steward, media, and executive administration advice is made available to unit administration in a timely manner.
11. Initiate steps to warn other Indiana University units or technicians if the situation has the potential to affect other university information or information systems.
12. Confirm actual or probable events from investigatory information and facilitate decision-making by the Incident Team.
13. In coordination with the Incident Team members and following internal procedures, determine if notification to individuals and/or regulatory or governmental authorities is required and/or desired, and invoke breach notification procedures commensurate with the situation.
14. Ensure appropriate university approvals are obtained prior to any notifications to individuals or regulatory and government officials.
15. Document decisions and any notifications made to individuals or regulatory and government officials.
16. Schedule a debriefing meeting with the unit and Incident Team after the response, to ensure appropriate corrective action in the affected unit is taken, to identify any actions that could be taken to reduce the likelihood of a future similar incident, and to continuously improve the response processes.
17. In cases where it is found that a reported incident involves information or physical privacy concerns, UIPO will communicate with the relevant privacy official who will then invoke policy ISPP-27 Privacy Complaints as appropriate, in addition to incident response procedures.

Information and Information System Incident Reporting, Management, and Breach Notification, http://policies.iu.edu/policies/categories/information-it/ispp/ISPP-26.shtml.

Artifact D: Sample Roles for Breach Response



CIRT Roles and Responsibilities

Roles and Responsibilities

Within this section, the roles and responsibilities for the CIO/DCIO, Critical Incident Response/Recovery Sub-Team (CIRT), CIC, and Supporting Groups are defined. In addition, this section addresses the various IT Services functional areas within the University and their CIRT responsibilities.

The University has a pool of CICs. Should the initial CIC be unavailable or unavailable during the entire incident, then the CNOC or Support Desk should call the next CIC within 10 minutes.

- Ideally, the CICs should be matched to the type of critical incident occurring at the University.
- CICs should understand they may be asked to run an incident outside of their functional area.
- If the CIC is initially unavailable, an alternate will assume the CIC role in his/her stead.

Chief Information Officer / Deputy Chief Information Officer

This position will report directly to the University's President and Board of Trustee. This role will either involve or inform as the needs of the incident dictate. Communication of information during an incident will follow this flow to eliminate confusion and misinformation between groups.

The CIO/DCIO is responsible for executing or delegating the following:

- Setting priorities
- Notifying the University President and/or Board of Trustees of an incident declaration
- Communicating status of critical incident to the PEC
- Participating with CIC in forensic investigation decisions
- Designating the DCIO or an alternate to cover the responsibilities of the CIO role
- Notifying University Communications as appropriate for internal and external communication
- Owning of the CIC's incident work plan(s)
- Defining and issuing 'gag' orders within IT Services for particularly sensitive issues; the default guideline for communicating about a critical incident is on a need to know basis
- Notifying Human Resources as appropriate
- Notifying Legal as appropriate
- Notifying Campus Security as appropriate
- Chairing the Post Mortem – Closeout Phase

Critical Incident Coordinator (CIC)

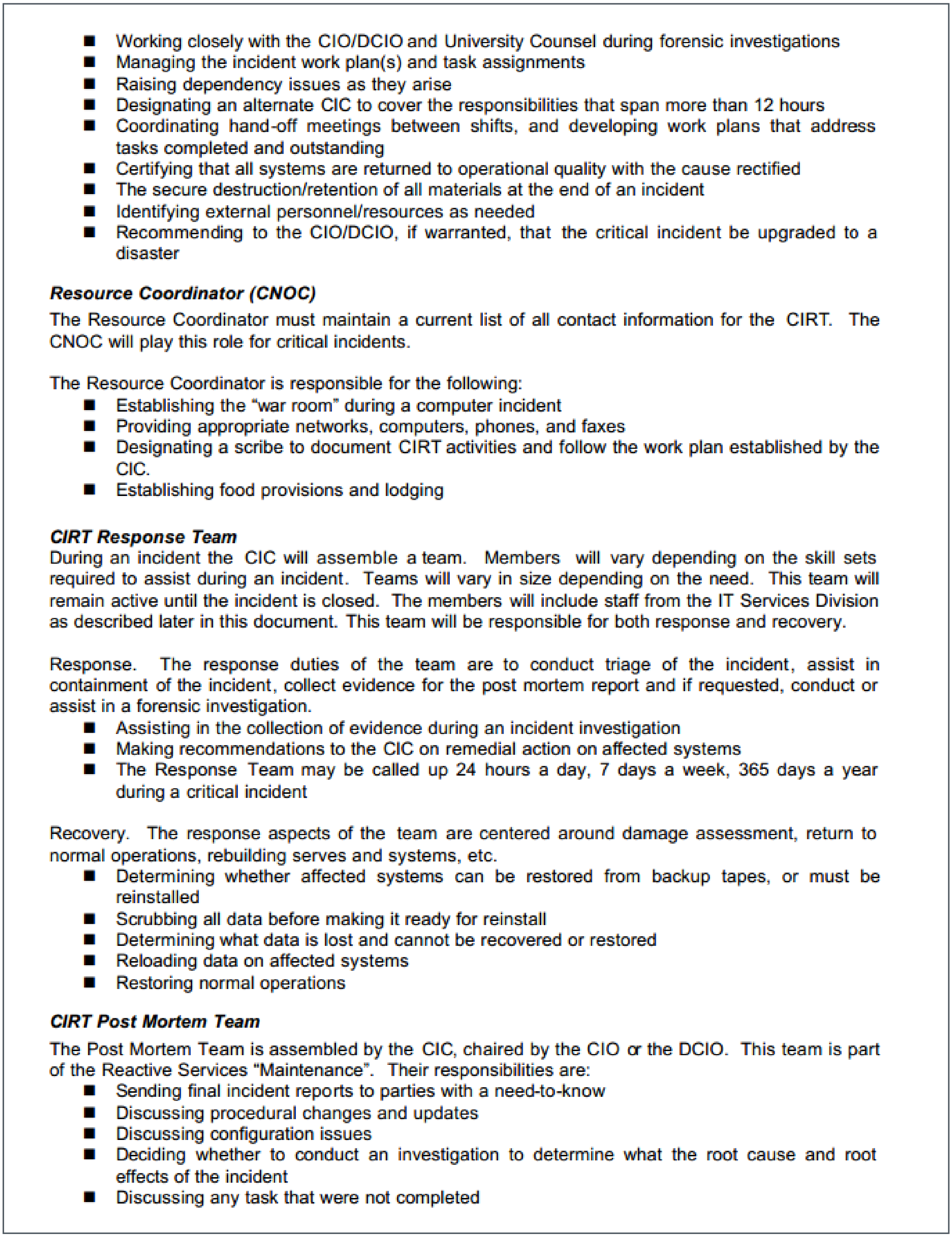
This position will update the CIO/DCIO on a regular basis during a critical incident. The CIC will obtain technical expertise based on the incident declared.

The CIC is responsible for the following:

- Managing incident resources
- Determining if an incident is a Critical Incident and declaring it to be so.
- Maintaining communications between CIRT and the CIO/DCIO
- Reminding staff that communication is on a need to know basis or if the CIO has defined a 'gag order' informing team members and the CNOC of the nature of the 'gag'.
- Communicating to the CNOC and the IT Services Leadership Team that a critical incident has been declared and a CIRT has been formed
- Activating the CIRT and notifying the team of meeting locations and call-in telephone numbers
- Beginning a case file for the incident. Use to ensure information is properly collected and documented
- Developing containment procedures
- Establishing a Post Mortem Team to determine the root cause and root effect of the incident

University Critical Incident Response Plan, https://net.educause.edu/Elements/Attachments/security/9320/MUOhio_CIR_Plan.pdf.

Artifact D: Sample Roles for Breach Response (Cont.)



- Working closely with the CIO/DCIO and University Counsel during forensic investigations
- Managing the incident work plan(s) and task assignments
- Raising dependency issues as they arise
- Designating an alternate CIC to cover the responsibilities that span more than 12 hours
- Coordinating hand-off meetings between shifts, and developing work plans that address tasks completed and outstanding
- Certifying that all systems are returned to operational quality with the cause rectified
- The secure destruction/retention of all materials at the end of an incident
- Identifying external personnel/resources as needed
- Recommending to the CIO/DCIO, if warranted, that the critical incident be upgraded to a disaster

Resource Coordinator (CNOC)

The Resource Coordinator must maintain a current list of all contact information for the CIRT. The CNOC will play this role for critical incidents.

The Resource Coordinator is responsible for the following:

- Establishing the "war room" during a computer incident
- Providing appropriate networks, computers, phones, and faxes
- Designating a scribe to document CIRT activities and follow the work plan established by the CIC.
- Establishing food provisions and lodging

CIRT Response Team

During an incident the CIC will assemble a team. Members will vary depending on the skill sets required to assist during an incident. Teams will vary in size depending on the need. This team will remain active until the incident is closed. The members will include staff from the IT Services Division as described later in this document. This team will be responsible for both response and recovery.

Response. The response duties of the team are to conduct triage of the incident, assist in containment of the incident, collect evidence for the post mortem report and if requested, conduct or assist in a forensic investigation.

- Assisting in the collection of evidence during an incident investigation
- Making recommendations to the CIC on remedial action on affected systems
- The Response Team may be called up 24 hours a day, 7 days a week, 365 days a year during a critical incident

Recovery. The response aspects of the team are centered around damage assessment, return to normal operations, rebuilding serves and systems, etc.

- Determining whether affected systems can be restored from backup tapes, or must be reinstalled
- Scrubbing all data before making it ready for reinstall
- Determining what data is lost and cannot be recovered or restored
- Reloading data on affected systems
- Restoring normal operations

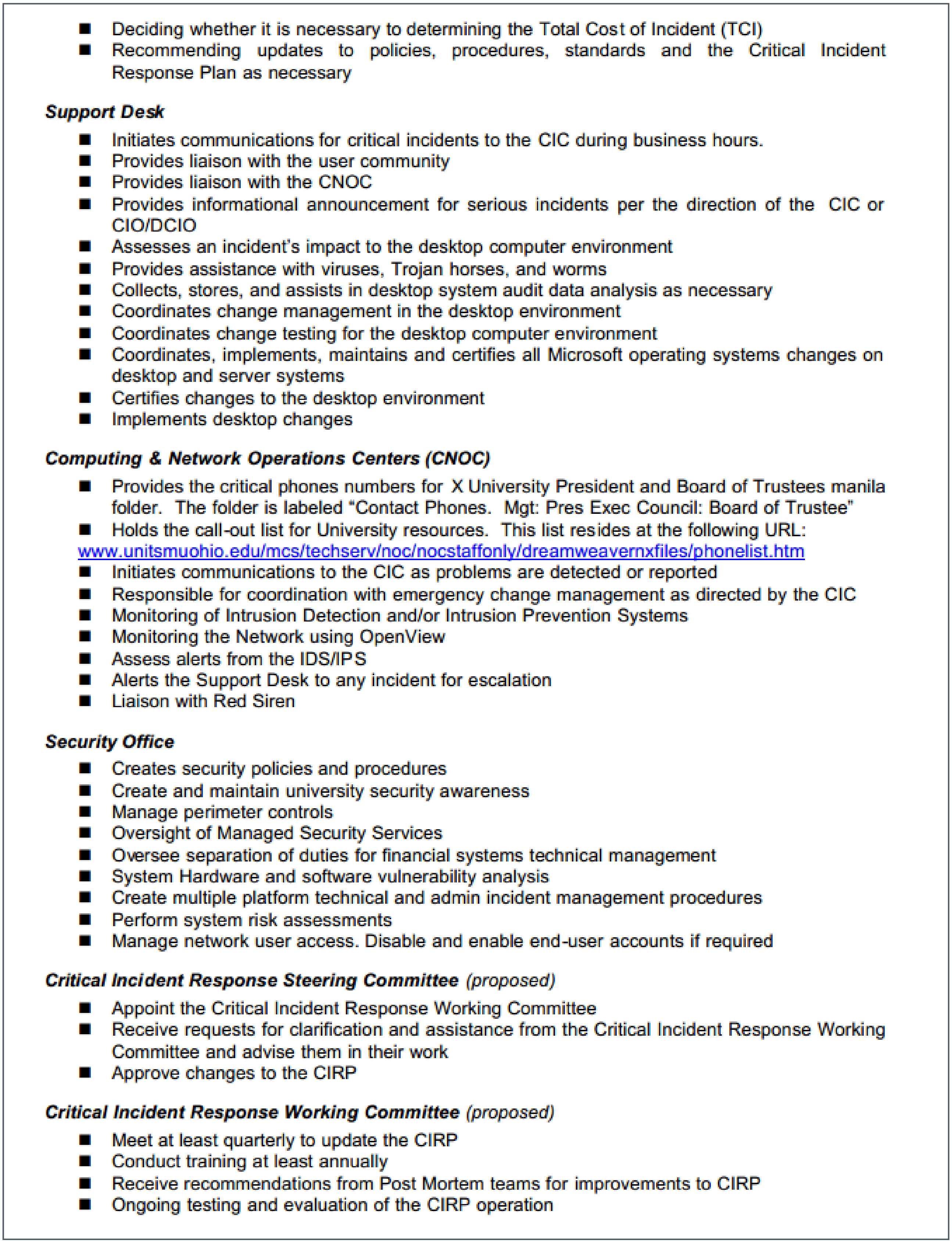
CIRT Post Mortem Team

The Post Mortem Team is assembled by the CIC, chaired by the CIO or the DCIO. This team is part of the Reactive Services "Maintenance". Their responsibilities are:

- Sending final incident reports to parties with a need-to-know
- Discussing procedural changes and updates
- Discussing configuration issues
- Deciding whether to conduct an investigation to determine what the root cause and root effects of the incident
- Discussing any task that were not completed

University Critical Incident Response Plan, https://net.educause.edu/Elements/Attachments/security/9320/MUOhio_CIR_Plan.pdf.

Artifact D: Sample Roles for Breach Response (Cont.)



- Deciding whether it is necessary to determining the Total Cost of Incident (TCI)
- Recommending updates to policies, procedures, standards and the Critical Incident Response Plan as necessary

Support Desk

- Initiates communications for critical incidents to the CIC during business hours.
- Provides liaison with the user community
- Provides liaison with the CNOC
- Provides informational announcement for serious incidents per the direction of the CIC or CIO/DCIO
- Assesses an incident's impact to the desktop computer environment
- Provides assistance with viruses, Trojan horses, and worms
- Collects, stores, and assists in desktop system audit data analysis as necessary
- Coordinates change management in the desktop environment
- Coordinates change testing for the desktop computer environment
- Coordinates, implements, maintains and certifies all Microsoft operating systems changes on desktop and server systems
- Certifies changes to the desktop environment
- Implements desktop changes

Computing & Network Operations Centers (CNOC)

- Provides the critical phones numbers for X University President and Board of Trustees manila folder. The folder is labeled "Contact Phones. Mgt: Pres Exec Council: Board of Trustee"
- Holds the call-out list for University resources. This list resides at the following URL:

www.unitsmuohio.edu/mcs/techserv/noc/nocstaffonly/dreamweavernxfiles/phonelist.htm

- Initiates communications to the CIC as problems are detected or reported
- Responsible for coordination with emergency change management as directed by the CIC
- Monitoring of Intrusion Detection and/or Intrusion Prevention Systems
- Monitoring the Network using OpenView
- Assess alerts from the IDS/IPS
- Alerts the Support Desk to any incident for escalation
- Liaison with Red Siren

Security Office

- Creates security policies and procedures
- Create and maintain university security awareness
- Manage perimeter controls
- Oversight of Managed Security Services
- Oversee separation of duties for financial systems technical management
- System Hardware and software vulnerability analysis
- Create multiple platform technical and admin incident management procedures
- Perform system risk assessments
- Manage network user access. Disable and enable end-user accounts if required

Critical Incident Response Steering Committee *(proposed)*

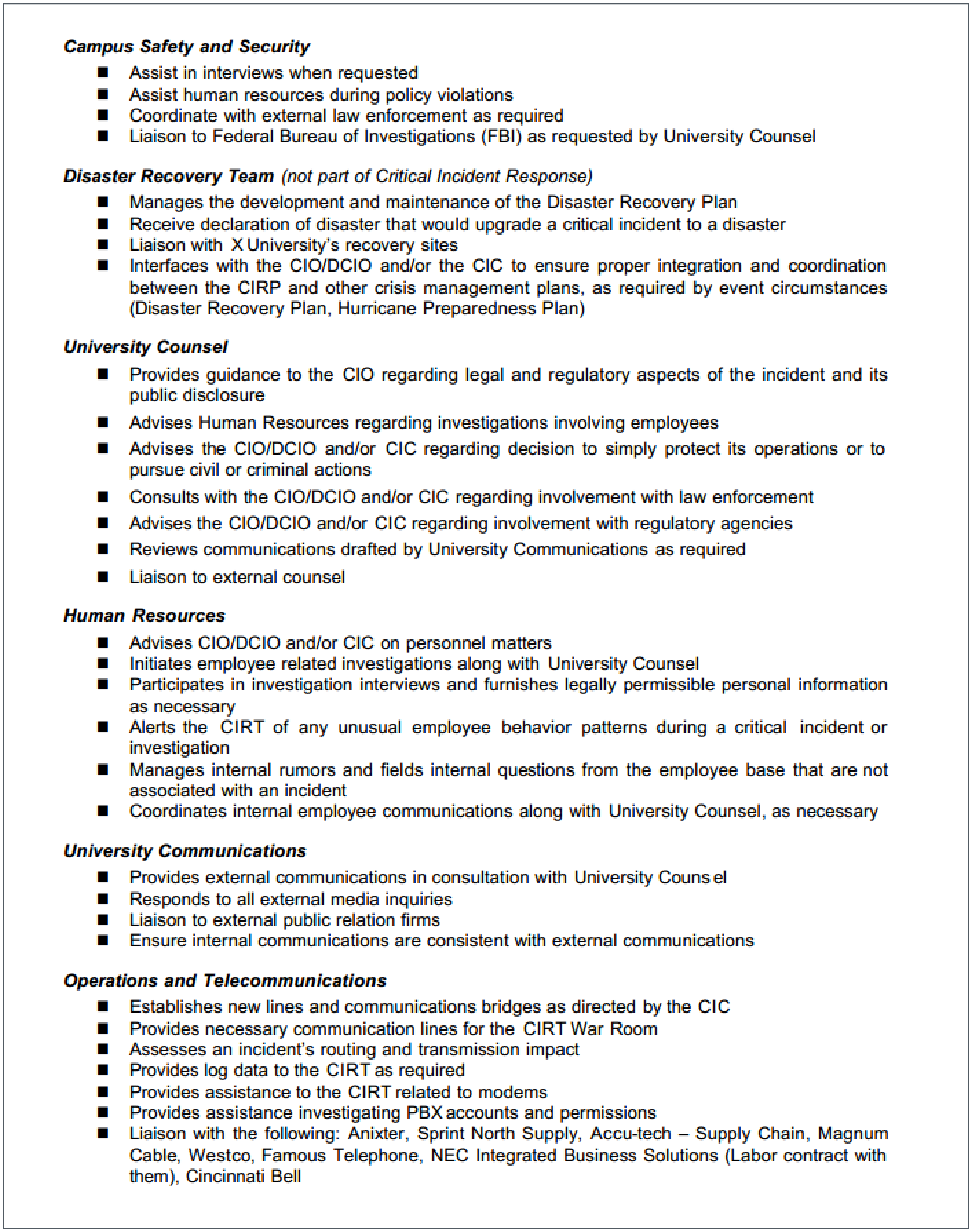
- Appoint the Critical Incident Response Working Committee
- Receive requests for clarification and assistance from the Critical Incident Response Working Committee and advise them in their work
- Approve changes to the CIRP

Critical Incident Response Working Committee *(proposed)*

- Meet at least quarterly to update the CIRP
- Conduct training at least annually
- Receive recommendations from Post Mortem teams for improvements to CIRP
- Ongoing testing and evaluation of the CIRP operation

University Critical Incident Response Plan, https://net.educause.edu/Elements/Attachments/security/9320/MUOhio_CIR_Plan.pdf.

Artifact D: Sample Roles for Breach Response (Cont.)



Campus Safety and Security

- Assist in interviews when requested
- Assist human resources during policy violations
- Coordinate with external law enforcement as required
- Liaison to Federal Bureau of Investigations (FBI) as requested by University Counsel

Disaster Recovery Team *(not part of Critical Incident Response)*

- Manages the development and maintenance of the Disaster Recovery Plan
- Receive declaration of disaster that would upgrade a critical incident to a disaster
- Liaison with X University's recovery sites
- Interfaces with the CIO/DCIO and/or the CIC to ensure proper integration and coordination between the CIRP and other crisis management plans, as required by event circumstances (Disaster Recovery Plan, Hurricane Preparedness Plan)

University Counsel

- Provides guidance to the CIO regarding legal and regulatory aspects of the incident and its public disclosure
- Advises Human Resources regarding investigations involving employees
- Advises the CIO/DCIO and/or CIC regarding decision to simply protect its operations or to pursue civil or criminal actions
- Consults with the CIO/DCIO and/or CIC regarding involvement with law enforcement
- Advises the CIO/DCIO and/or CIC regarding involvement with regulatory agencies
- Reviews communications drafted by University Communications as required
- Liaison to external counsel

Human Resources

- Advises CIO/DCIO and/or CIC on personnel matters
- Initiates employee related investigations along with University Counsel
- Participates in investigation interviews and furnishes legally permissible personal information as necessary
- Alerts the CIRT of any unusual employee behavior patterns during a critical incident or investigation
- Manages internal rumors and fields internal questions from the employee base that are not associated with an incident
- Coordinates internal employee communications along with University Counsel, as necessary

University Communications

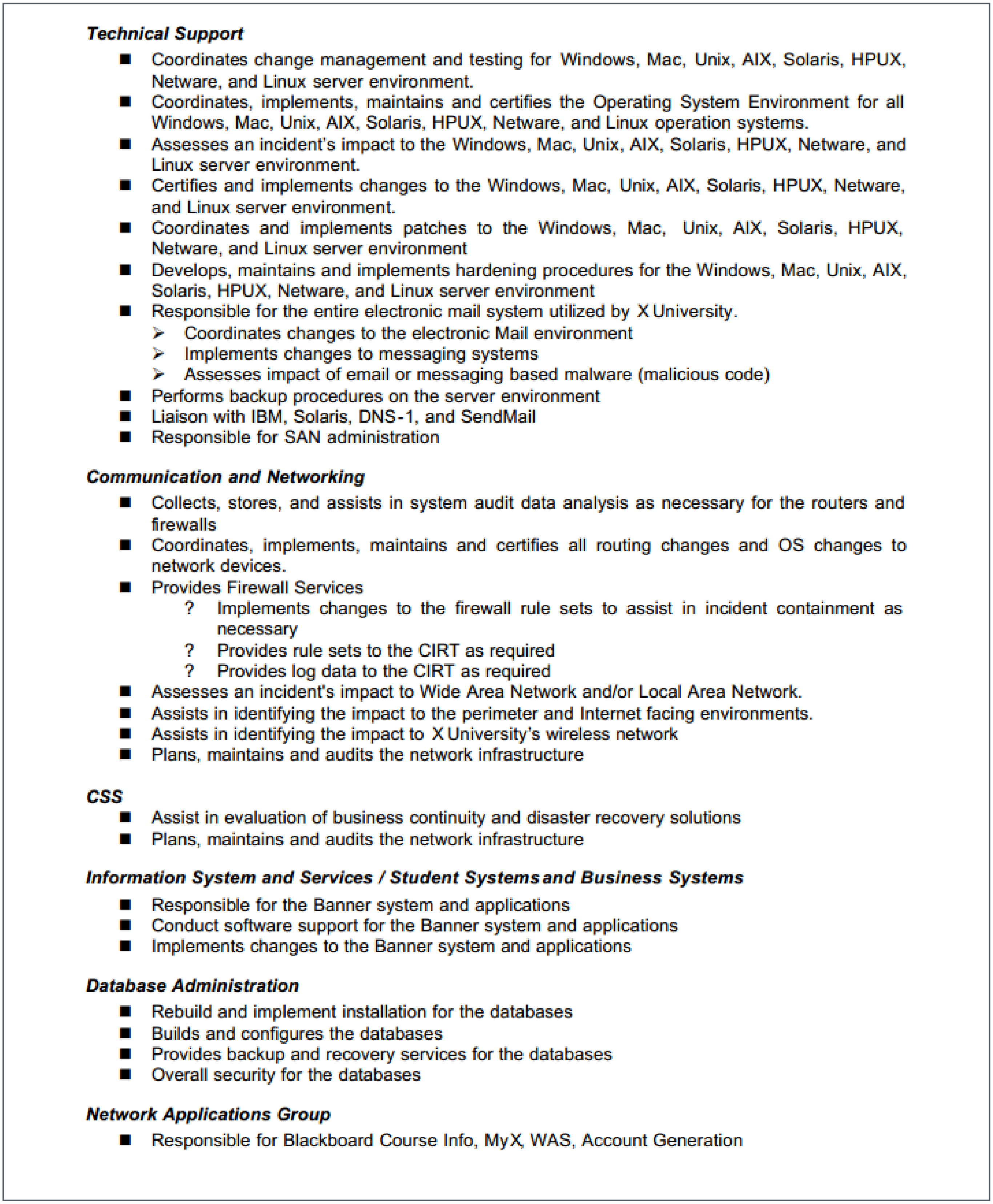
- Provides external communications in consultation with University Counsel
- Responds to all external media inquiries
- Liaison to external public relation firms
- Ensure internal communications are consistent with external communications

Operations and Telecommunications

- Establishes new lines and communications bridges as directed by the CIC
- Provides necessary communication lines for the CIRT War Room
- Assesses an incident's routing and transmission impact
- Provides log data to the CIRT as required
- Provides assistance to the CIRT related to modems
- Provides assistance investigating PBX accounts and permissions
- Liaison with the following: Anixter, Sprint North Supply, Accu-tech – Supply Chain, Magnum Cable, Westco, Famous Telephone, NEC Integrated Business Solutions (Labor contract with them), Cincinnati Bell

University Critical Incident Response Plan, https://net.educause.edu/Elements/Attachments/security/9320/MUOhio_CIR_Plan.pdf.

Artifact D: Sample Roles for Breach Response (Cont.)



Technical Support

- Coordinates change management and testing for Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment.
- Coordinates, implements, maintains and certifies the Operating System Environment for all Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux operation systems.
- Assesses an incident's impact to the Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment.
- Certifies and implements changes to the Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment.
- Coordinates and implements patches to the Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment
- Develops, maintains and implements hardening procedures for the Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment
- Responsible for the entire electronic mail system utilized by X University.
  - Coordinates changes to the electronic Mail environment
  - Implements changes to messaging systems
  - Assesses impact of email or messaging based malware (malicious code)
- Performs backup procedures on the server environment
- Liaison with IBM, Solaris, DNS-1, and SendMail
- Responsible for SAN administration

Communication and Networking

- Collects, stores, and assists in system audit data analysis as necessary for the routers and firewalls
- Coordinates, implements, maintains and certifies all routing changes and OS changes to network devices.
- Provides Firewall Services
  - ? Implements changes to the firewall rule sets to assist in incident containment as necessary
  - ? Provides rule sets to the CIRT as required
  - ? Provides log data to the CIRT as required
- Assesses an incident's impact to Wide Area Network and/or Local Area Network.
- Assists in identifying the impact to the perimeter and Internet facing environments.
- Assists in identifying the impact to X University's wireless network
- Plans, maintains and audits the network infrastructure

CSS

- Assist in evaluation of business continuity and disaster recovery solutions
- Plans, maintains and audits the network infrastructure

Information System and Services / Student Systems and Business Systems

- Responsible for the Banner system and applications
- Conduct software support for the Banner system and applications
- Implements changes to the Banner system and applications

Database Administration

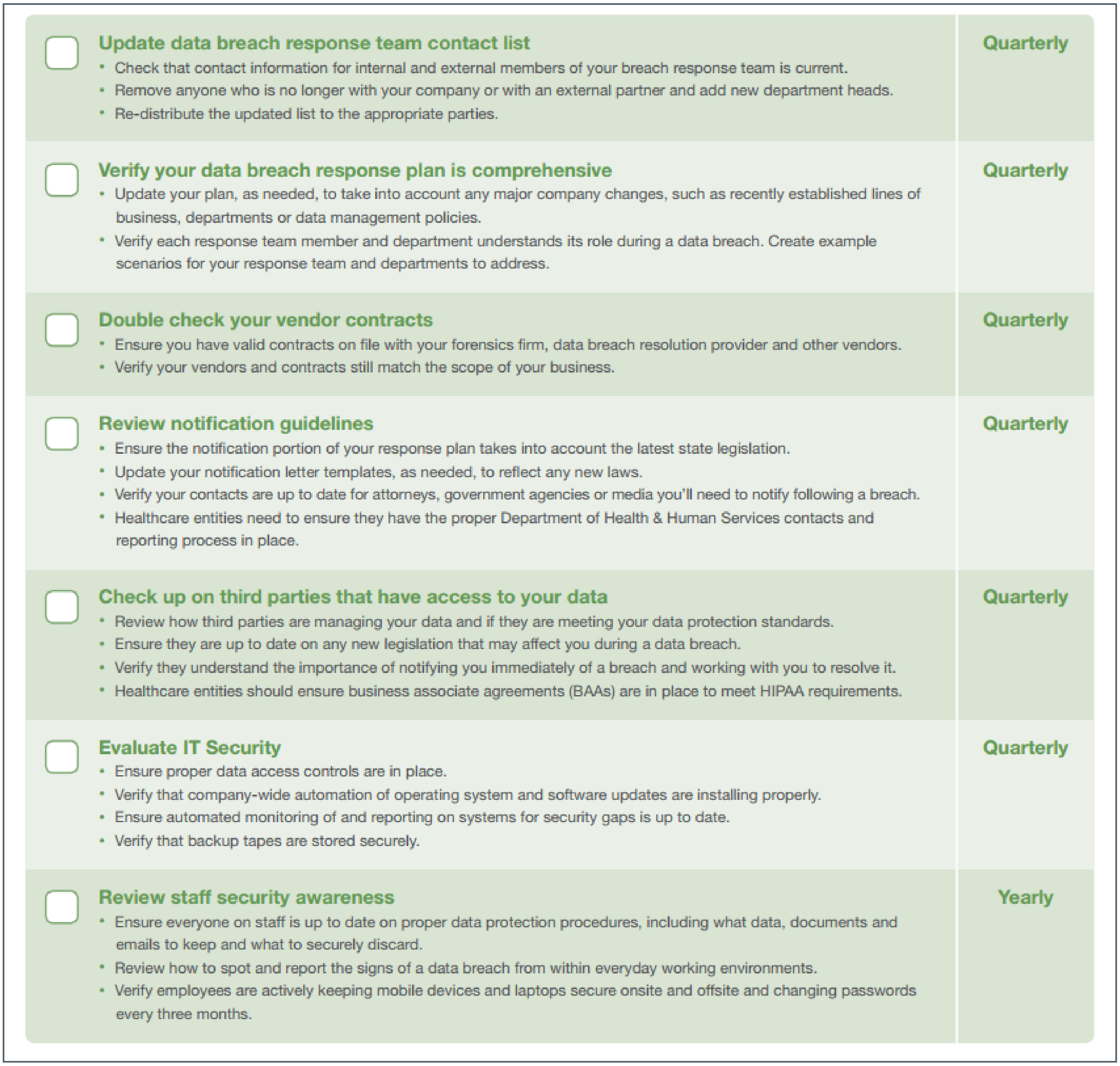
- Rebuild and implement installation for the databases
- Builds and configures the databases
- Provides backup and recovery services for the databases
- Overall security for the databases

Network Applications Group

- Responsible for Blackboard Course Info, MyX, WAS, Account Generation

University Critical Incident Response Plan, https://net.educause.edu/Elements/Attachments/security/9320/MUOhio_CIR_Plan.pdf.

Artifact E: Experian Preparedness Plan Audit Checklist



□ **Update data breach response team contact list**

- Check that contact information for internal and external members of your breach response team is current.
- Remove anyone who is no longer with your company or with an external partner and add new department heads.
- Re-distribute the updated list to the appropriate parties.

Quarterly

□ **Verify your data breach response plan is comprehensive**

- Update your plan, as needed, to take into account any major company changes, such as recently established lines of business, departments or data management policies.
- Verify each response team member and department understands its role during a data breach. Create example scenarios for your response team and departments to address.

Quarterly

□ **Double check your vendor contracts**

- Ensure you have valid contracts on file with your forensics firm, data breach resolution provider and other vendors.
- Verify your vendors and contracts still match the scope of your business.

Quarterly

□ **Review notification guidelines**

- Ensure the notification portion of your response plan takes into account the latest state legislation.
- Update your notification letter templates, as needed, to reflect any new laws.
- Verify your contacts are up to date for attorneys, government agencies or media you'll need to notify following a breach.
- Healthcare entities need to ensure they have the proper Department of Health & Human Services contacts and reporting process in place.

Quarterly

□ **Check up on third parties that have access to your data**

- Review how third parties are managing your data and if they are meeting your data protection standards.
- Ensure they are up to date on any new legislation that may affect you during a data breach.
- Verify they understand the importance of notifying you immediately of a breach and working with you to resolve it.
- Healthcare entities should ensure business associate agreements (BAAs) are in place to meet HIPAA requirements.

Quarterly

□ **Evaluate IT Security**

- Ensure proper data access controls are in place.
- Verify that company-wide automation of operating system and software updates are installing properly.
- Ensure automated monitoring of and reporting on systems for security gaps is up to date.
- Verify that backup tapes are stored securely.

Quarterly

□ **Review staff security awareness**

- Ensure everyone on staff is up to date on proper data protection procedures, including what data, documents and emails to keep and what to securely discard.
- Review how to spot and report the signs of a data breach from within everyday working environments.
- Verify employees are actively keeping mobile devices and laptops secure onsite and offsite and changing passwords every three months.

Yearly

Data Breach Response Guide: 2013-2014 Edition, http://www.experian.com/assets/data-breach/brochures/response-guide.pdf.

Artifact F: Sample Breach Vendor Contact Cards

Breach Vendor A

- *Type of Services Offered..* ____________________
- *Company Website……....* ____________________
- *Name of Contact…………..* ____________________
- *Office Phone……………….* (____)______-________
- *Mobile Phone……………...* (____)______-________
- *Email Address……………..* ____________________
- *Date of last Vetting……….* ____________________
- *Estimated Pricing…………* ____________________

Breach Vendor B

- *Type of Services Offered..* ____________________
- *Company Website……....* ____________________
- *Name of Contact…………..* ____________________
- *Office Phone……………….* (____)______-________
- *Mobile Phone……………...* (____)______-________
- *Email Address……………..* ____________________
- *Date of last Vetting……….* ____________________
- *Estimated Pricing…………* ____________________

Breach Vendor C

- *Type of Services Offered..* ____________________
- *Company Website……....* ____________________
- *Name of Contact…………..* ____________________
- *Office Phone……………….* (____)______-________
- *Mobile Phone……………...* (____)______-________
- *Email Address……………..* ____________________
- *Date of last Vetting……….* ____________________
- *Estimated Pricing…………* ____________________

Artifact G: Tips for Data Breach Communication

Composite of Institutional Breach Plans and Private Industry Recommendations

Press Release

- *Key Components*
  - Who is affected?
  - What type of data has been compromised?
  - What evidence is available (i.e., what are the facts)?
  - What actions have been taken by the university to fix the breach and rectify the security issue?
  - What are next steps for relevant university units?
  - Where is more information available?

✓

Remember to

- Only report what is verifiable, and describe facts as what is 'known so far'- surprises will damage the IT function's credibility during incidents
- Vet all external press releases with general counsel
- Designate one source of university communications about the breach (e.g., an Assistant Vice President of Communications)

Notification Letter

- *Key Components*
  - Apology and statement of responsibility
  - What are the facts?
  - What is the type of data and possible risk to individuals?
  - What services or remediation will be made available for victims, and how will they be accessed?
  - Who can be contacted for more information?

✓

Remember to

- Only report what is verifiable, and describe facts as what is 'known so far'
- Express regret and determination to avoid future breaches
- Ensure the quality and sincerity of all communication with victims- down to the quality of paper you use to send notifications

Internal Messaging

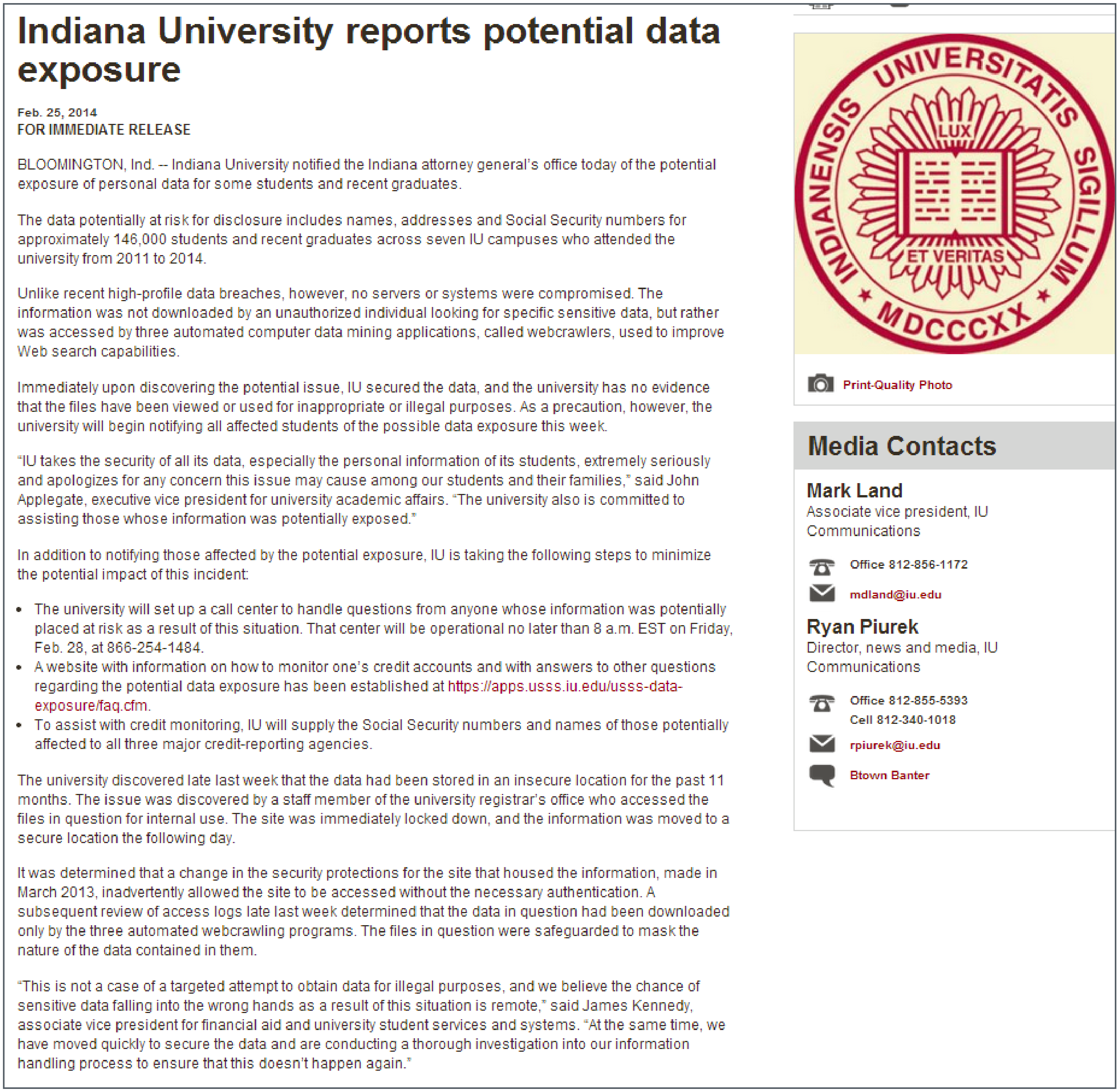
- *Key Components*
  - Do not cast blame without full knowledge of facts and resolution
  - Do not understate potential losses or risks
  - Coordinate message with responsible department
  - Prepare for range of reactions

✓

Remember to

- Include security threat discussions with regular executive communication
- Be ready for ambivalence, anger, confusion, and disbelief from university staff and leadership

Artifact H: Indiana University Data Exposure Press Release



Indiana University reports potential data exposure

Feb. 25, 2014
FOR IMMEDIATE RELEASE

BLOOMINGTON, Ind. -- Indiana University notified the Indiana attorney general's office today of the potential exposure of personal data for some students and recent graduates.

The data potentially at risk for disclosure includes names, addresses and Social Security numbers for approximately 146,000 students and recent graduates across seven IU campuses who attended the university from 2011 to 2014.

Unlike recent high-profile data breaches, however, no servers or systems were compromised. The information was not downloaded by an unauthorized individual looking for specific sensitive data, but rather was accessed by three automated computer data mining applications, called webcrawlers, used to improve Web search capabilities.

Immediately upon discovering the potential issue, IU secured the data, and the university has no evidence that the files have been viewed or used for inappropriate or illegal purposes. As a precaution, however, the university will begin notifying all affected students of the possible data exposure this week.

"IU takes the security of all its data, especially the personal information of its students, extremely seriously and apologizes for any concern this issue may cause among our students and their families," said John Applegate, executive vice president for university academic affairs. "The university also is committed to assisting those whose information was potentially exposed."

In addition to notifying those affected by the potential exposure, IU is taking the following steps to minimize the potential impact of this incident:

- The university will set up a call center to handle questions from anyone whose information was potentially placed at risk as a result of this situation. That center will be operational no later than 8 a.m. EST on Friday, Feb. 28, at 866-254-1484.
- A website with information on how to monitor one's credit accounts and with answers to other questions regarding the potential data exposure has been established at https://apps.usss.iu.edu/usss-data-exposure/faq.cfm.
- To assist with credit monitoring, IU will supply the Social Security numbers and names of those potentially affected to all three major credit-reporting agencies.

The university discovered late last week that the data had been stored in an insecure location for the past 11 months. The issue was discovered by a staff member of the university registrar's office who accessed the files in question for internal use. The site was immediately locked down, and the information was moved to a secure location the following day.

It was determined that a change in the security protections for the site that housed the information, made in March 2013, inadvertently allowed the site to be accessed without the necessary authentication. A subsequent review of access logs late last week determined that the data in question had been downloaded only by the three automated webcrawling programs. The files in question were safeguarded to mask the nature of the data contained in them.

"This is not a case of a targeted attempt to obtain data for illegal purposes, and we believe the chance of sensitive data falling into the wrong hands as a result of this situation is remote," said James Kennedy, associate vice president for financial aid and university student services and systems. "At the same time, we have moved quickly to secure the data and are conducting a thorough investigation into our information handling process to ensure that this doesn't happen again."

📷 Print-Quality Photo

Media Contacts

Mark Land
Associate vice president, IU Communications

☎ Office 812-856-1172

✉ mdland@iu.edu

Ryan Piurek
Director, news and media, IU Communications

☎ Office 812-855-5393
Cell 812-340-1018

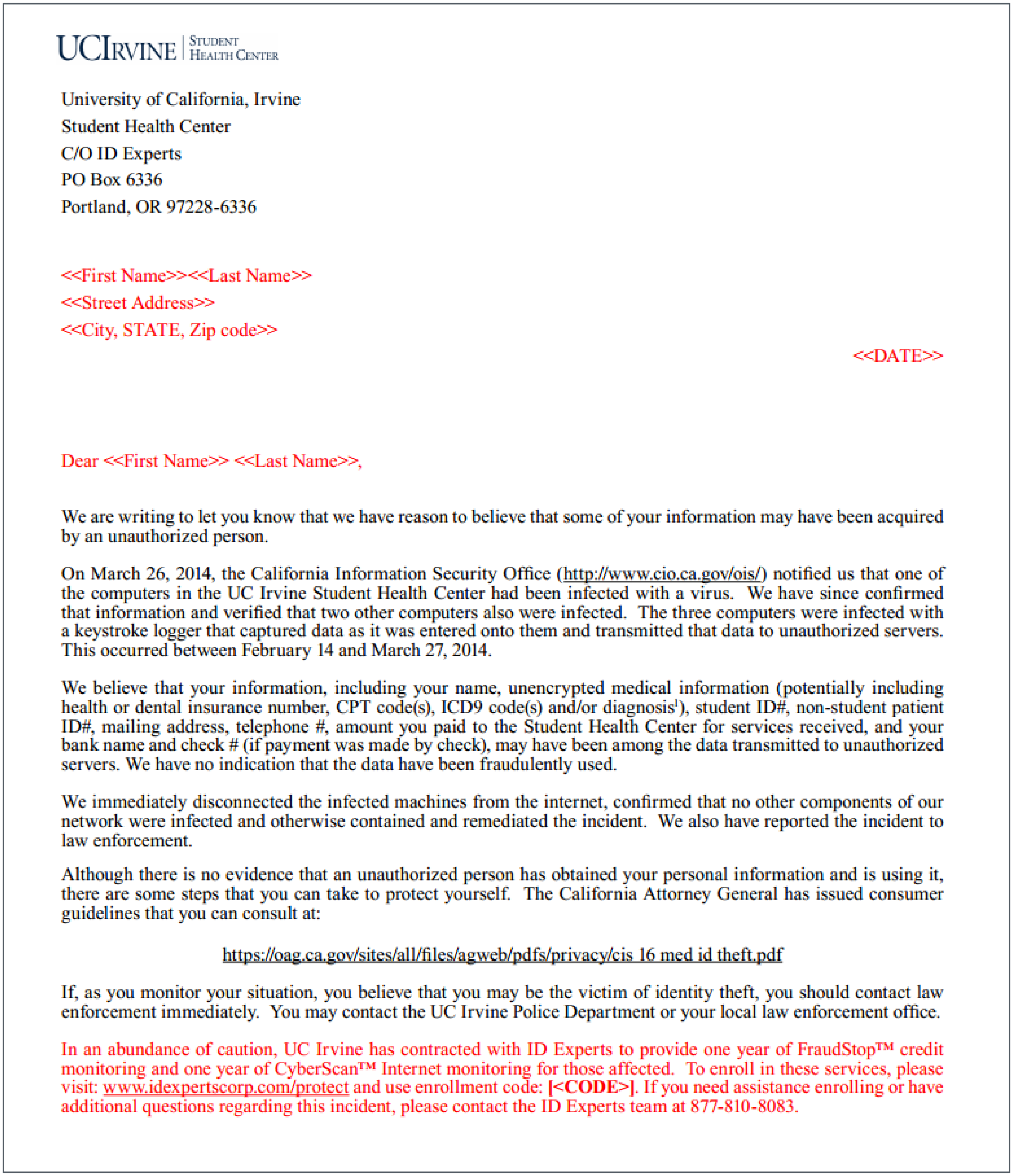
✉ rpiurek@iu.edu

Btown Banter

http://news.iu.edu/releases/iu/2014/02/data-exposure-disclosure.shtml.

Artifact I: Sample Notification Letter from the University of California, Irvine

Further samples of notifications available at the Office of the Attorney General's resource center (http://oag.ca.gov/ecrime/databreach/list)



UCIrvine | Student Health Center

University of California, Irvine
Student Health Center
C/O ID Experts
PO Box 6336
Portland, OR 97228-6336

<<First Name>><<Last Name>>
<<Street Address>>
<<City, STATE, Zip code>>

<<DATE>>

Dear <<First Name>> <<Last Name>>,

We are writing to let you know that we have reason to believe that some of your information may have been acquired by an unauthorized person.

On March 26, 2014, the California Information Security Office (http://www.cio.ca.gov/ois/) notified us that one of the computers in the UC Irvine Student Health Center had been infected with a virus. We have since confirmed that information and verified that two other computers also were infected. The three computers were infected with a keystroke logger that captured data as it was entered onto them and transmitted that data to unauthorized servers. This occurred between February 14 and March 27, 2014.

We believe that your information, including your name, unencrypted medical information (potentially including health or dental insurance number, CPT code(s), ICD9 code(s) and/or diagnosis[1]), student ID#, non-student patient ID#, mailing address, telephone #, amount you paid to the Student Health Center for services received, and your bank name and check # (if payment was made by check), may have been among the data transmitted to unauthorized servers. We have no indication that the data have been fraudulently used.

We immediately disconnected the infected machines from the internet, confirmed that no other components of our network were infected and otherwise contained and remediated the incident. We also have reported the incident to law enforcement.

Although there is no evidence that an unauthorized person has obtained your personal information and is using it, there are some steps that you can take to protect yourself. The California Attorney General has issued consumer guidelines that you can consult at:

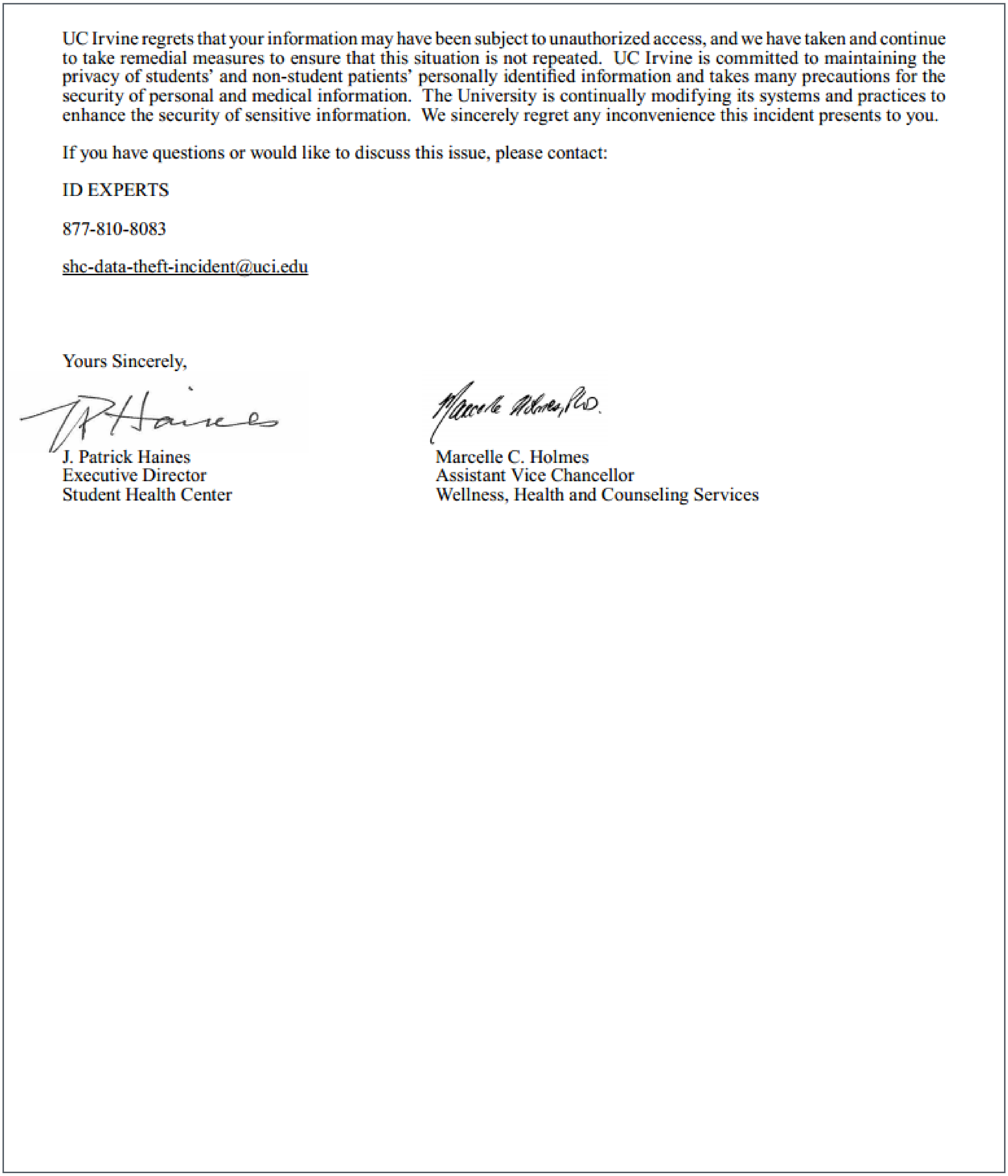
https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis_16_med_id_theft.pdf

If, as you monitor your situation, you believe that you may be the victim of identity theft, you should contact law enforcement immediately. You may contact the UC Irvine Police Department or your local law enforcement office.

In an abundance of caution, UC Irvine has contracted with ID Experts to provide one year of FraudStop™ credit monitoring and one year of CyberScan™ Internet monitoring for those affected. To enroll in these services, please visit: www.idexpertscorp.com/protect and use enrollment code: **[<CODE>]**. If you need assistance enrolling or have additional questions regarding this incident, please contact the ID Experts team at 877-810-8083.

Submitted Breach Notification Sample, http://oag.ca.gov/system/files/UCIrvine%20Notice%20Letter%20Sample_0.pdf.

Artifact I: Sample Notification Letter from the University of California, Irvine (Cont.)



UC Irvine regrets that your information may have been subject to unauthorized access, and we have taken and continue to take remedial measures to ensure that this situation is not repeated. UC Irvine is committed to maintaining the privacy of students' and non-student patients' personally identified information and takes many precautions for the security of personal and medical information. The University is continually modifying its systems and practices to enhance the security of sensitive information. We sincerely regret any inconvenience this incident presents to you.

If you have questions or would like to discuss this issue, please contact:

ID EXPERTS

877-810-8083

shc-data-theft-incident@uci.edu

Yours Sincerely,

PHaines

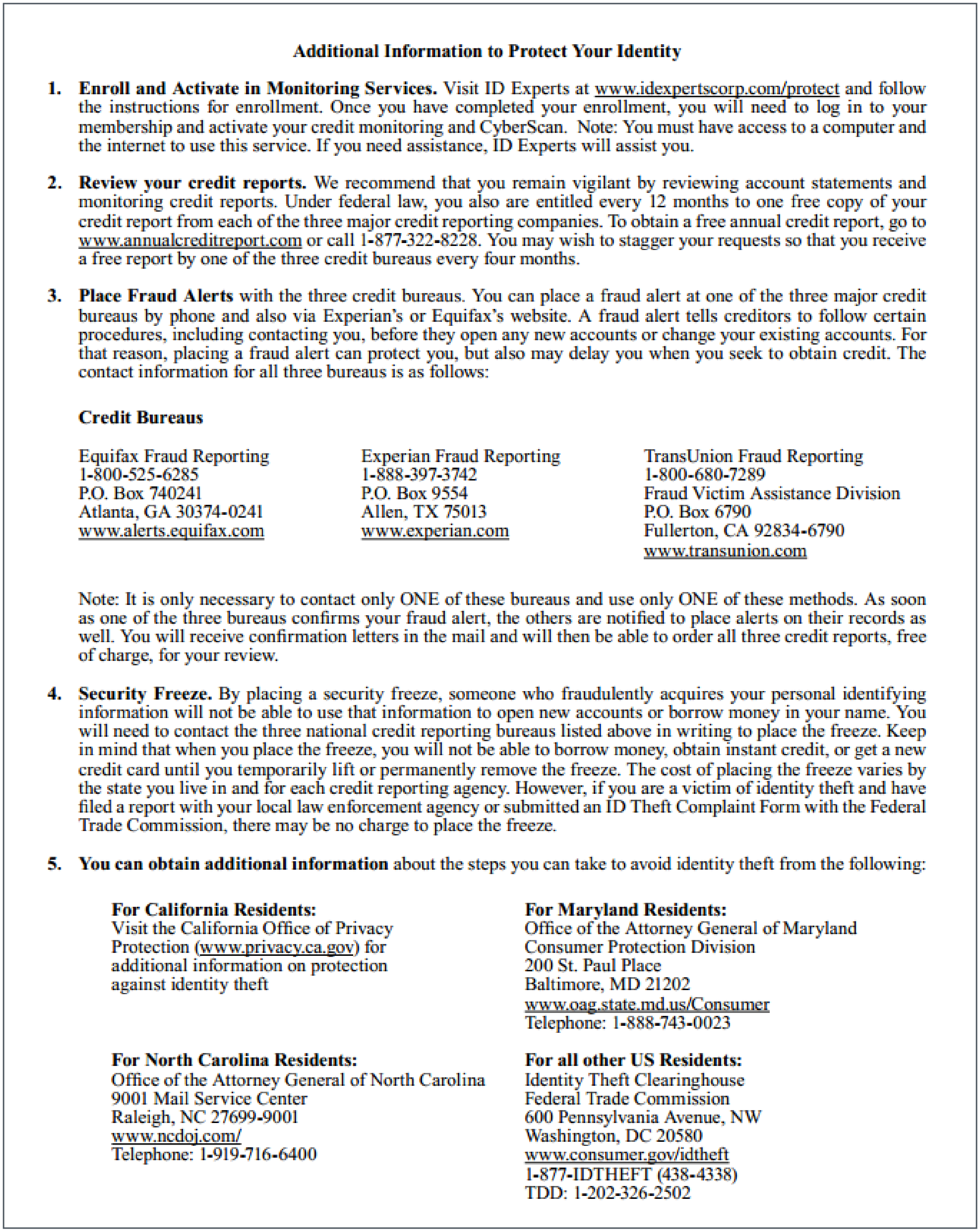
J. Patrick Haines
Executive Director
Student Health Center

Marcelle Holmes, PhD.

Marcelle C. Holmes
Assistant Vice Chancellor
Wellness, Health and Counseling Services

Submitted Breach Notification Sample, http://oag.ca.gov/system/files/UCIrvine%20Notice%20Letter%20Sample_0.pdf.

Artifact I: Sample Notification Letter from the University of California, Irvine (Cont.)



Additional Information to Protect Your Identity

1. **Enroll and Activate in Monitoring Services.** Visit ID Experts at www.idexpertscorp.com/protect and follow the instructions for enrollment. Once you have completed your enrollment, you will need to log in to your membership and activate your credit monitoring and CyberScan. Note: You must have access to a computer and the internet to use this service. If you need assistance, ID Experts will assist you.

2. **Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

3. **Place Fraud Alerts** with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

   Credit Bureaus

   Equifax Fraud Reporting
   1-800-525-6285
   P.O. Box 740241
   Atlanta, GA 30374-0241
   www.alerts.equifax.com

   Experian Fraud Reporting
   1-888-397-3742
   P.O. Box 9554
   Allen, TX 75013
   www.experian.com

   TransUnion Fraud Reporting
   1-800-680-7289
   Fraud Victim Assistance Division
   P.O. Box 6790
   Fullerton, CA 92834-6790
   www.transunion.com

   Note: It is only necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

4. **Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting agency. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

5. **You can obtain additional information** about the steps you can take to avoid identity theft from the following:

   For California Residents:
   Visit the California Office of Privacy
   Protection (www.privacy.ca.gov) for
   additional information on protection
   against identity theft

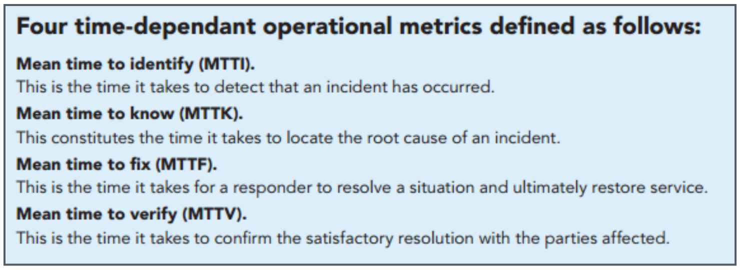
   For Maryland Residents:
   Office of the Attorney General of Maryland
   Consumer Protection Division
   200 St. Paul Place
   Baltimore, MD 21202
   www.oag.state.md.us/Consumer
   Telephone: 1-888-743-0023

   For North Carolina Residents:
   Office of the Attorney General of North Carolina
   9001 Mail Service Center
   Raleigh, NC 27699-9001
   www.ncdoj.com/
   Telephone: 1-919-716-6400

   For all other US Residents:
   Identity Theft Clearinghouse
   Federal Trade Commission
   600 Pennsylvania Avenue, NW
   Washington, DC 20580
   www.consumer.gov/idtheft
   1-877-IDTHEFT (438-4338)
   TDD: 1-202-326-2502

Submitted Breach Notification Sample, http://oag.ca.gov/system/files/UCIrvine%20Notice%20Letter%20Sample_0.pdf.

Artifact J: Ponemon Institute LLC Industrial Cyber Security Key Performance Indicators



Four time-dependant operational metrics defined as follows:

Mean time to identify (MTTI).
This is the time it takes to detect that an incident has occurred.

Mean time to know (MTTK).
This constitutes the time it takes to locate the root cause of an incident.

Mean time to fix (MTTF).
This is the time it takes for a responder to resolve a situation and ultimately restore service.

Mean time to verify (MTTV).
This is the time it takes to confirm the satisfactory resolution with the parties affected.

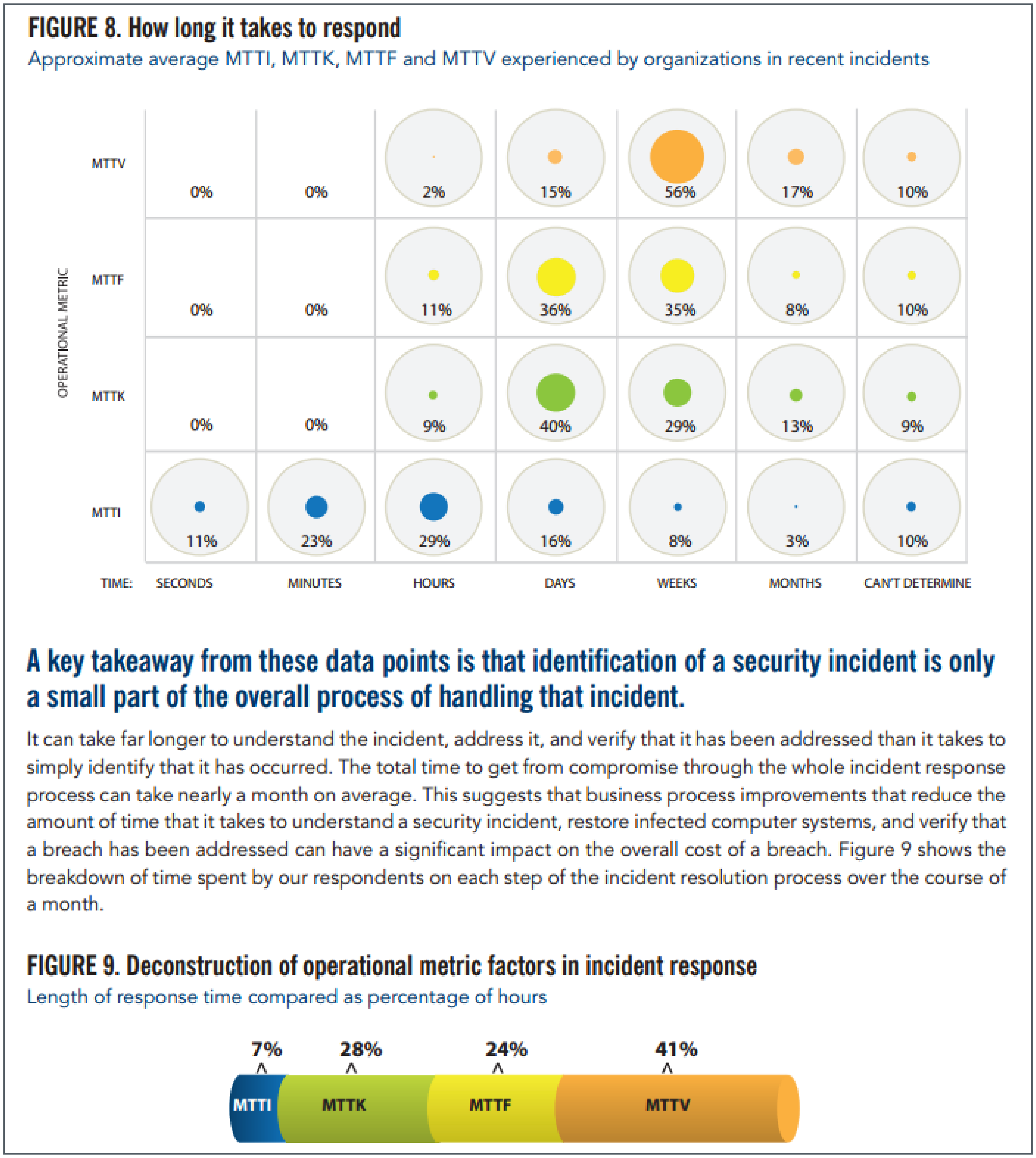


FIGURE 8. How long it takes to respond

Approximate average MTTI, MTTK, MTTF and MTTV experienced by organizations in recent incidents

OPERATIONAL METRIC	SECONDS	MINUTES	HOURS	DAYS	WEEKS	MONTHS	CAN'T DETERMINE
MTTV	0%	0%	2%	15%	56%	17%	10%
MTTF	0%	0%	11%	36%	35%	8%	10%
MTTK	0%	0%	9%	40%	29%	13%	9%
MTTI	11%	23%	29%	16%	8%	3%	10%

A key takeaway from these data points is that identification of a security incident is only a small part of the overall process of handling that incident.

It can take far longer to understand the incident, address it, and verify that it has been addressed than it takes to simply identify that it has occurred. The total time to get from compromise through the whole incident response process can take nearly a month on average. This suggests that business process improvements that reduce the amount of time that it takes to understand a security incident, restore infected computer systems, and verify that a breach has been addressed can have a significant impact on the overall cost of a breach. Figure 9 shows the breakdown of time spent by our respondents on each step of the incident resolution process over the course of a month.

FIGURE 9. Deconstruction of operational metric factors in incident response

Length of response time compared as percentage of hours

"Cyber Security Incident Response: Are we as prepared as we think?" Ponemon Institute LLC, January 2014. http://www.lancope.com/files/documents/Industry-Reports/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf/.

Education
Advisory
Board

eab.com

2445 M Street NW I Washington DC 20037
P 202.266.6400 I F 202.266.5700