Addendum to the Security Incident Response Plan

Computer Security Incidents Involving Payment Card Data or CDE Devices

Introduction

This addendum identifies the application of the OU-Norman Computer Security Incident Response Plan to information security events and incidents involving cardholder data or CDE devices, including detailing of information specific to such breaches and additional special requirements.

Applicability

The response details described in this addendum apply to information security events and incidents that involve cardholder data or systems of the cardholder data environment.

Special Considerations, Provisions, and Requirements

A table of the special considerations, provisions, and requirements specific to Payment Cardholder Data for all stages of incident management is provided below. The remainder of this addendum focuses on incident identification and response.

Incident Management—Payment Cardholder Data			
Stage	**Task**	**Special Notes and/or Additional Requirements**	**Respons.**
Preparation	**Preparation**	The following preparations have been made for the Cardholder Data Environment (CDE) and breaches involving cardholder data: • Establishment of preventative and detective controls, processes, and procedures per adopted standards. • Preparation of incident response controls, processes, and procedures of this Computer Security Incident Response Plan and adopted standards.	CSIRT & Non-CSIRT
Identification	**Detection, Discovery, and Identification**	The following identification and detection controls have been implemented specially for cardholder data: • Advance identification and classification of systems containing cardholder data in the designation and documentation of the CDE. • Special monitoring of systems (per adopted standards) within the CDE based on proactive system classification. • Events indicative of the occurrence of a security breach are reviewed according to industry-recognized indicators of compromise, including those of the Global Payment Brands of the payment card industry	CSIRT & Non-CSIRT
Response	**Triage**	Some components of triage have special considerations as indicated below.	See below
	Triage (on-site)	Payment card data considerations have been incorporated into training, procedures, and documentation for incident triage (both CSIRT and non-CSIRT)	CSIRT & Non-CSIRT
	Triage (lab)	(see above)	CSIRT
	Containment	No change; priorities remain as indicted on page 5 of the CSIRP.	CSIRT
	Initial Event Assessment	No change	CSIRT
	Event Escalation	Special escalation criteria are defined	CSIRT
	Reporting—Internal	Special initial reporting requirements are established by the Office of the Bursar. Communication to Bursar and Legal Counsel required within a 24-hour timeframe.	CSIRT
	Incident Investigation	No change	CSIRT
	At-Risk Scoping and Quantification	In the event of a breach of cardholder data, the business is responsible for the final identification and quantification of total and unique records at-risk or breached.	Non-CSIRT
	Reporting—External	The Office of the Bursar has specially designated responsibility for providing required event reporting to the payment processor and payment card brands.	Non-CSIRT
	Remediation	Root causes for a breach of a system within the CDE must be fully remediated and all control requirements of the PCI-DSS validated.	Non-CSIRT
	Restoration and Recovery	Restoration of systems within the CDE having experienced a breach must be fully recertified and accredited for PCI-DSS compliance.	Non-CSIRT
	Breach Victim Notification	The merchant/business unit involved as specially designated responsibility for providing required breach notification to victims of a breach.	Non-CSIRT
	Breach Victim Post-Ex	If pursued, breach victim redress is the responsibility of the business unit involved.	Non-CSIRT
	Incident Response Post-Ex	A final forensics report must always be made. Post-incident review elements may involve members of the Office of the Bursar and the PCI Steering Committee.	CSIRT

Special Roles and Responsibilities

Business Unit

In the event of a breach or suspected breach of information, the business unit will be responsible for

- providing, and all costs associated with providing, activities and actions for escalation, notification, and ex-post response, including but not limited to the following:
    - escalation (preparations to report breach of protected information to appropriate entities within time requirements).
    - notification (letters, outbound telephone calls, e-mail, public media, or general notice regarding the breach).
    - ex-post response (arrangements facilitating breach victim communication with the University or University representative regarding questions and recommendations for minimizing potential harm, as well as redress actions including credit report monitoring or cost recovery for reissuance of new accounts or payment cards),
- fines, judgments, and legal fees and expenses associated with the event,
- corrective actions to remediate causes for the breach and actions to bring affected systems, environments, and entities into compliance,
- reimbursement of costs incurred by other University departments and areas as a result of the incident, including costs of investigation, fines, judgment, and legal fees and expenses.

First Responders, IT and Non-IT

Security event first responders , whether IT Tier 1 and Tier 2 support personnel, staff from other IT support functions, or business unit staff, are responsible for following the incident discovery, reporting, and initial response procedures for initial response and triage established and communicated by the Office of Information Security (provided at the end of this addendum).

IT System Administrators

IT system administrators are responsible for following the incident discovery, reporting, and initial response procedures for initial response and triage established and communicated by the Office of Information Security (provided at the end of this addendum).

Office of the Bursar

The Office of the Bursar will oversee incidents involving payment cardholder data, and is responsible for providing notice and report to payment card processor, global payment brands, and acquiring banks, as appropriate, according to their respective reporting requirements. The Office of the Bursar sets the internal notification responsibilities required of the CSIRT.

Office of Legal Counsel

The Office of Legal Counsel will be responsible for determining obligation of and carrying our reporting of a breach to the State of Oklahoma for compliance with the State of Oklahoma Data Breach Laws.

OU Computer Security Incident Response Team (CSIRT)

The OU CSIRT has primary responsibility for response to, and investigation of, PCI incidents at OU.

Special Requirements and Procedure for Incident Response Stage

Identification

The OU CSIRT identifies potential information security events both by proactive internal detection using security event monitoring systems and by receipt of external notification of system anomalies or suspected security events (for example, by system administrators, business unit staff, and third parties). The OU CSIRT maintains and monitors security event monitoring and alerting systems configured to specially alarm on security events affecting the cardholder data environment. The OU IT CSIRT also reviews security events for systems that are not part of the cardholder data environment.

The OU CSIRT will review any event indicative of the occurrence of a security breach, with determination made according to industry-recognized indicators of compromise, including those of the Global Payment Brands of the payment card industry (see Visa Inc., 2011, pp. 1-5, and MasterCard Worldwide, 2010, p. 2-1). As most campus information security events do not involve systems suspected of hosting cardholder data and not all information security events indicate a suspected security breach, event triage is performed to determine which events are escalated for investigation and appropriate reporting.

Triage

Elements of event triage may take place both by non-CSIRT and OU CSIRT staff. Triage actions may take place both on-site (e.g., at the location of the suspected event or affected system) or in the OU IT Cyber Forensics lab.

Triage (non-CSIRT, on-site)

Payment card data considerations have been incorporated into communicated training, procedures, and documentation for incident triage by non-CSIRT. The incident discovery, reporting, and initial response procedures for non-CSIRT initial response and triage are provided at the end of this addendum.

Triage (CSIRT, onsite or lab)

Upon proactive internal detection or receipt of external notification of a security event, the IT Office of Information Security performs event triage to determine the nature of the compromise, including the type of data assets believed to be involved and the nature of the security event (system compromise, etc.). Payment card data considerations have been incorporated into training, procedures, and documentation for incident triage for OU CSIRT staff.

Containment

Standard CSIRT obligations and responsibilities are maintained and priorities remain as indicated on page 5 of the CSIRP. These priorities are consistent with those of MasterCard Worldwide (*Security Rules and Procedures*, 2011, pp. 10-3 to 10-6), Visa Inc. (*What To Do If Compromised*, 2011, pp. 6-7), American Express (*Data Security Operating Policy for U.S. Merchants, Section 2 – Data Incident Management Obligations*, 2010, pp. 1-2), and Discover Financial Services (*Data Security Breach*, 2011).

Initial Event Assessment

Standard CSIRT initial event assessment procedures are followed. However, due to the University's designation of a Cardholder Data Environment and advance classification of systems within this environment, certain elements of standard event assessment are already known for events affecting systems in the CDE.

Event Escalation

If it is determined that an information security event places cardholder data at risk, then the event is immediately escalated to an information security incident involving cardholder data.

Events that may possibly signify security breaches of a CDE system or system containing cardholder data (e.g., an alert has been received on them or other anomaly detected) need not be immediately escalated without reasonable review. The incident handler's determination of whether either of the following applies is key:

- a security breach capable of exposing data did in fact occur (100% probability), or
- a vulnerability that could have allowed the exposure of data actually existed and the occurrence of a breach of the data could not be ruled out nor confirmed (>0% probability but undetermined)

If there is any risk (>0% probability) that cardholder data was compromised (i.e., the data is at risk), the event must be escalated.

The OU CSIRT will escalate an information security event if at least one criterion from each of the two following tests holds true:

Data Type Test

- the system affected is a component of the Cardholder Data Environment, OR
- the presence of cardholder data is confirmed or suspected for the system

AND

Security Breach/"At-risk" Test

- In the prudent judgment of an OU CSIRT incident handler, an event has occurred that places cardholder data at risk (i.e., if zero risk is determined, then no reporting is required), OR
- Greater than 24 hours have passed since the initial investigation into the event began and determination has not yet been made.

The maximum limit on transpired time is specified to meet the requirements of the Office of the Bursar to notify external entities within the constraints on that Office, as well as prevent a tentative "never-ending" investigation. Some events reported simply due to the timer admittedly may end up being false alarms. The timer applies to the OU CSIRT's internal escalation and notification to the Bursar (and the Office of Legal Counsel); the decision to report externally or not stays with the Bursar and the Office of Legal Counsel.

Reporting—Internal

For events affecting or potentially involving cardholder data or the cardholder data environment, accelerated reporting is required to meet the immediacy requirements of the card brands (upon escalation, communication is made immediately to the Office of the Bursar and the Office of Legal Counsel). Further incident investigation is then continued. For ongoing investigations, updates will be made to the Office of the Bursar and the Office of Legal Counsel upon key points of case progress, discovery or determination of new relevant facts, and decision points.

The OU CSIRT will adhere to special initial reporting requirements established by the Office of the Bursar. Once an event involving cardholder data is escalated to a security incident, immediate communication to the Office of the Bursar and the Office of Legal Counsel is required. The reports to the Office of the Bursar and the Office of Legal Counsel will be made as follows:

Office of the Bursar

Primary contact			Secondary contact		
Name:	Andrea Peters		**Name:**	Melody Astani	
Title:	Financial Associate I		**Title:**	Internal Operations Manager	
Contact instructions:	Call office phone during business hours and leave message then contact secondary if unavailable. For any after-hours contact needs, contact secondary.		**Contact instructions:**	Call office phone first, then mobile or other phone. Leave message on both.	
Contact Details:	**Business hours**	**Non-business hours**	**Contact Details:**	**Business hours**	**Non-business hours**
Office Phone:	(405) 325-1469	Contact Secondary	**Office Phone:**	(405) 325-1434	N/A
Mobile Phone:	N/A	Contact Secondary	**Mobile Phone:**	(405) 664-5981	(405) 664-5981
Other Phone:	N/A	N/A	**Other Phone:**	N/A	N/A
E-mail Address:	aspeters@ou.edu		**E-mail Address:**	mastani@ou.edu	
Other:	N/A	N/A	**Other:**	N/A	N/A

Office of Legal Counsel

Primary contact			Secondary contact		
Name:	James Murray		**Name:**	Rachel McCombs	
Title:	Staff Attorney		**Title:**	Staff Attorney	
Contact instructions:	Call office phone first; leave message if non-business hours or if unavailable. Then call mobile phone.		**Contact instructions:**	Call office phone only; leave message if non-business hours or if unavailable.	
Contact Details:	**Business hours**	**Non-business hours**	**Contact Details:**	**Business hours**	**Non-business hours**
Office Phone:	(405) 325-4124	(405) 325-4124	**Office Phone:**	(405) 271-2033	(405) 271-2033
Mobile Phone:	(405) 990-5924	405) 990-5924	**Mobile Phone:**	(405) 343-8305	(405) 343-8305
Other Phone:	N/A	N/A	**Other Phone:**	N/A	N/A
E-mail Address:	jpm@ou.edu		**E-mail Address:**	Rachel-McCombs@ouhsc.edu	
Other:	N/A	N/A	**Other:**	N/A	N/A

Reporting—External (Non-CSIRT)

The Office of the Bursar has specially designated responsibility for providing required event reporting to the payment processor and payment cards brands, and will make such reports according to the Office's internal procedures.

Investigation

Standard OU CSIRT procedures will be followed for all investigation activities. Standard OU CSIRT activities are carried out during standard university business hours.

At-Risk Scoping and Quantification (Non-CSIRT)

In the event of a breach of cardholder data, the business unit is responsible for the final identification and quantification of total and unique records at-risk or breached. IT support staff may provide technology assistance in making this determination where required.

Remediation (Non-CSIRT)

Root causes for a breach of a system within the CDE must be fully remediated and all control requirements of the PCI-DSS validated. This is a requirement of the OU-Norman Campus Payment Card Security Standard.

Restoration and Recovery (Non-CSIRT)

Restoration of systems within the CDE having experienced a breach must be fully recertified and accredited for PCI-DSS compliance. Prior to placing a system back into operation after a security breach, all university, Bursar

Office, and business unit requirements for re-certification of the system must be completed and approval granted by the Office of the Bursar.

Breach Victim Notification (Non-CSIRT)

The merchant/business unit involved has specially designated responsibility for providing required breach notification to victims of a breach.

Breach Victim Post-Ex (Non-CSIRT)

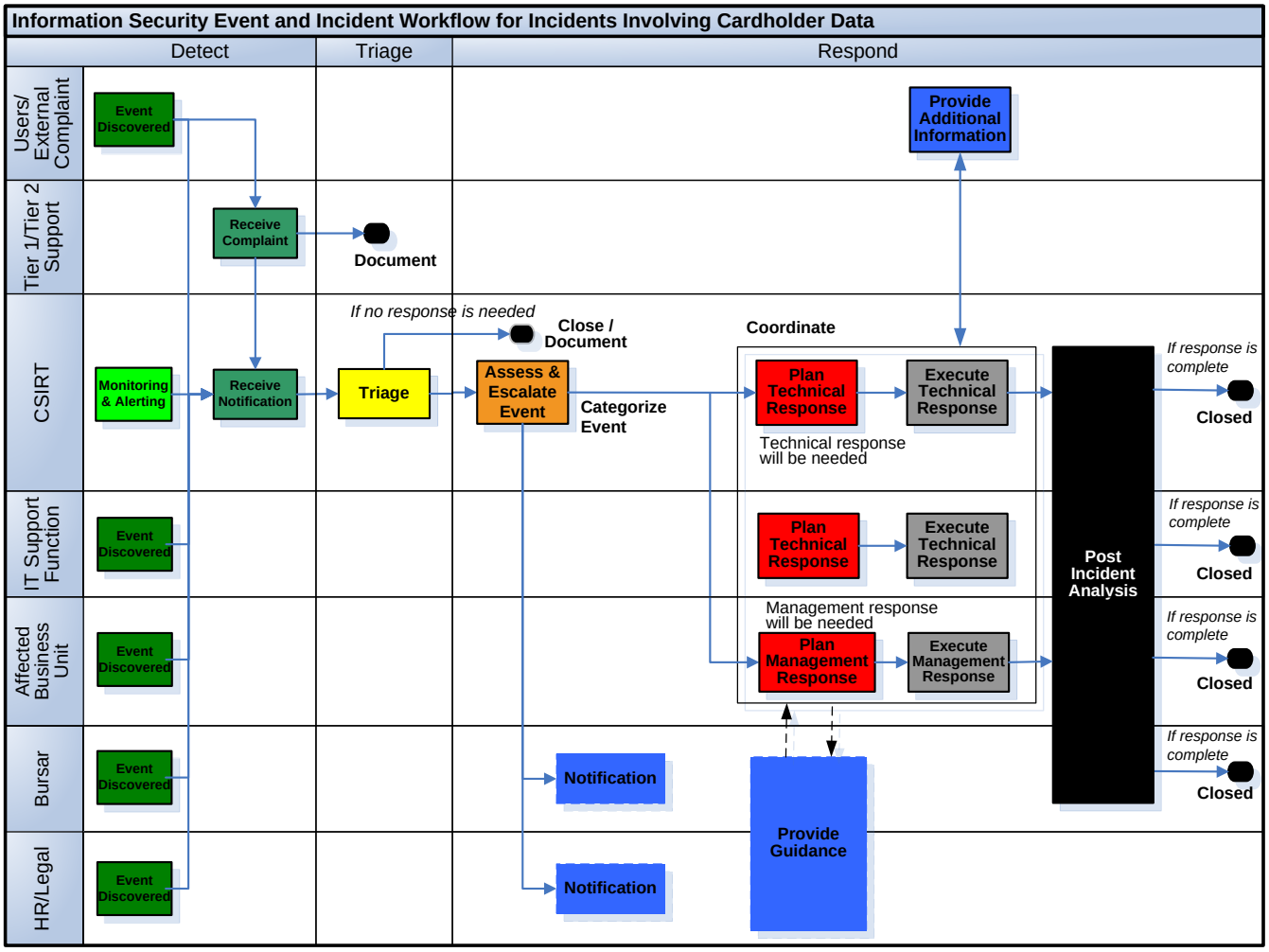
If pursued, breach victim redress is the responsibility of the business unit involved.

Incident Response Post-Ex

A final forensics report must always be made. Post-incident review elements may involve members of the Office of the Bursar and the PCI Steering Committee.

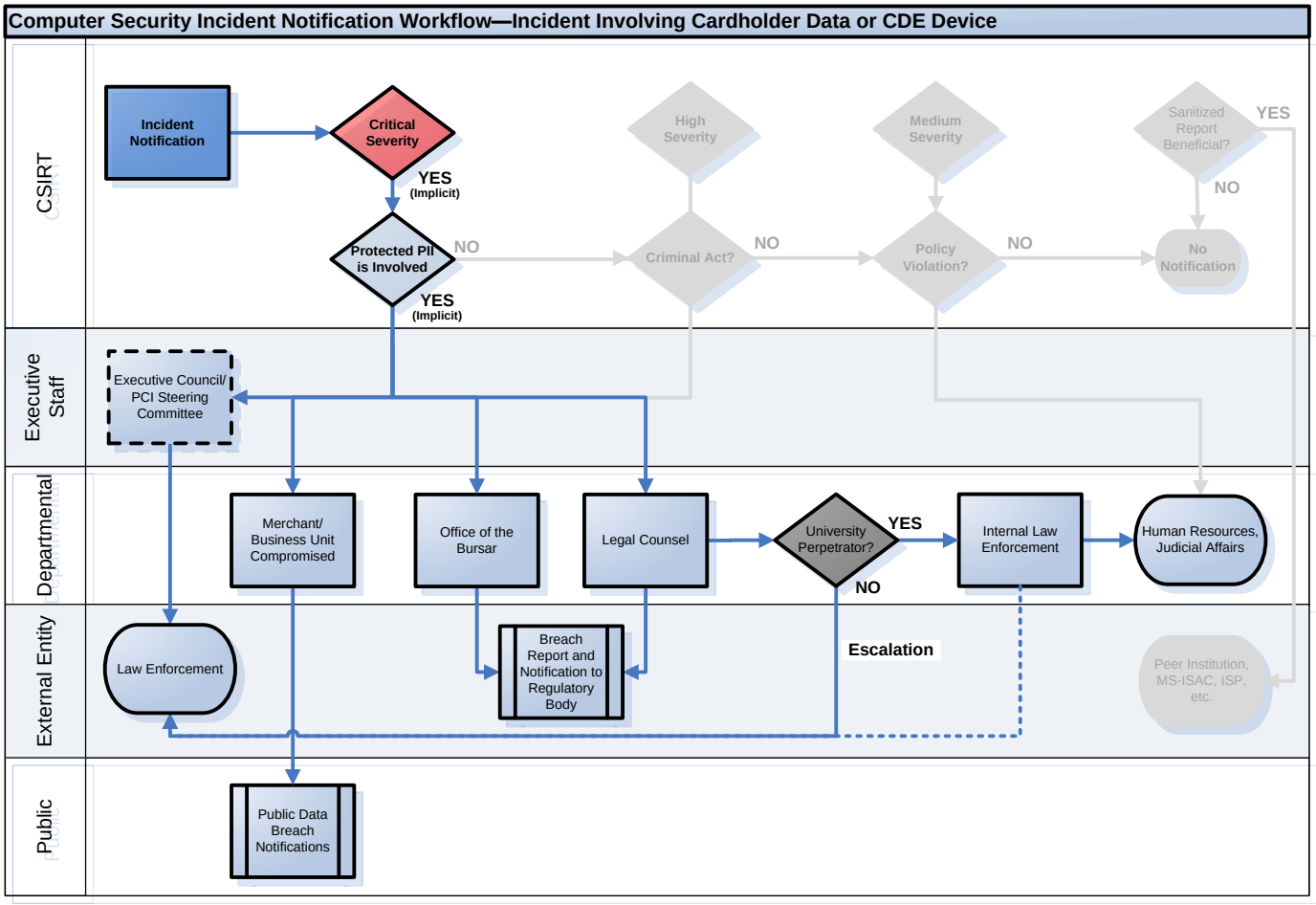
Computer Security Incident Workflow Specific for Incidents Involving Cardholder Data

Cardholder data is inherently personally identifiable information. Any actual or suspected breach involving cardholder data by definition involves the potential exposure of personally identifiable Information and is therefore classified as a Critical Security Event.



Incident Notification Workflow Specific for Incidents Involving Cardholder Data

This table shows the communication paths that are to be followed if the indicated communications are required. Processes and procedures within each functional area will determine whether communication notice is actually appropriate or necessary.



Definitions

Cardholder data	Any or all of the following data types associated with a payment card of a global payment brand: Primary Account Number (PAN), Cardholder Name, Expiration Date, Service Code
Cardholder data environment	The environment comprised of the people, processes and technology that store, process or transmit cardholder data or sensitive authentication data
CDE	Cardholder data environment
Global payment brand	Any of the following five payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.
Information Security Event	An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant. (as defined by ISO 18044:2004)
Information Security Incident	An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. (as defined by ISO 18044:2004)
PAN	Primary account number
PCI DSS	Payment Card Industry Data Security Standard
Primary account number	A bank card number found on credit cards, debit cards, charge cards, and stored-value cards
Sensitive authentication data	Any or all of the following data types associated with a payment card: Full magnetic stripe data or equivalent on a chip, CAV2/CVC2/CVV2/CID, PINs/PIN blocks

References

American Express. (2011) *American Express Data Security Operating Policy for U.S. Merchants* [PDF file] URL https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Merchant_US.pdf

DFS Services, LLC. (2013) *Discover Information Security & Compliance (DISC)* [WWW page]. URL http://www.discovernetwork.com/merchants/data-security/disc.html

MasterCard Worldwide. (2014) *Account Data Compromise User Guide* [PDF file]. URL http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf

MasterCard Worldwide. (2014) *MasterCard Worldwide Security Rules and Procedures: Merchant Edition* [PDF file]. URL http://www.mastercard.com/us/merchant/pdf/SPME-Entire_Manual_public.pdf

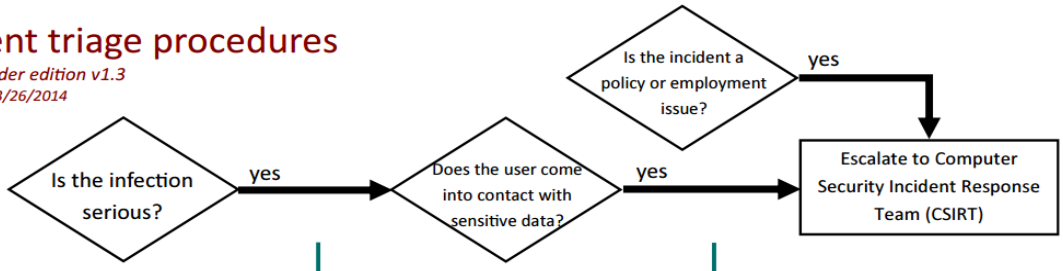
Visa Inc. (2011) What To *Do If Compromised: Visa Inc. Fraud Control and Investigations Procedures, Version 3.0 (Global) Effective May 2011* [PDF file]. URL http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf

Visa International. (2013) *Visa International Operating Regulations* [PDF file]. URL http://usa.visa.com/download/merchants/visa-international-operating-regulations-main.pdf

Incident Triage Procedures: Discovery, Reporting, and Initial Response

incident triage procedures

first responder edition v1.3
last revised 03/26/2014



1. Is the malware a known data-stealer, backdoor Trojan, or rootkit? If so, the infection is serious, otherwise continue to step 2.
2. Is the malware an innocuous threat such as adware, spyware, or tracking cookie? If so, the infection is not serious, otherwise continue to step 3.

   To look up the functionality of malware, use Microsoft's Threat Encyclopedia and/or Sophos:

   - Microsoft (www.microsoft.com/security/portal/Threat/Encyclopedia/Browse.aspx)
   - Sophos (www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware.aspx)

3. Is the infection system-level? If so, the infection is serious.

System-level infections are those found in a directory not writable by standard users (e.g. C:\Windows, C:\Windows\Program Files, C:\Program Files (x86)), and C:\Windows\System32).

Malware that is not a known data-stealer, backdoor, or rootkit that is limited to the user's profile directory does not require escalation.

If you are unable to determine the nature of the infection, escalate to CSIRT.

If the user comes into contact with any of the following data items, escalation is required.

DATA ELEMENT OR TYPE	REF.
Social security number (SSN)	1,2
Driver license number or state ID card number	1,2
Any financial account number	1,2
Any credit or debit card number	1,2,4
Any security code, access code, or password providing access to a financial account	1,2
Any personal health-related data	3

1. Oklahoma Statues §24-161ff and §74-3113.1ff
2. GLBA 501(b), per FIL-27-2005
3. HIPAA/HI-TECH
4. PCI, e.g. VISA CISP, etc.

If the infection is serious but the user does not come into contact with sensitive information, a rebuild is necessary.

Note: Breach reporting requirements do not apply to the user's own personal information, only institutionally-owned and maintained data.

Escalation

1. Contact the CSIRT to begin the escalation process (325-7258, csirt@ou.edu), making a note of what you have done on the system since being dispatched.
2. Run the incident response script as instructed. At minimum this will include performing a memory dump, running an incident response script, and copying off antivirus logs.
3. Unplug the network cable or disable the network interface
4. Shut down the computer and bring hard drive or system and the live analysis results to the CSIRT team (DEH B40).

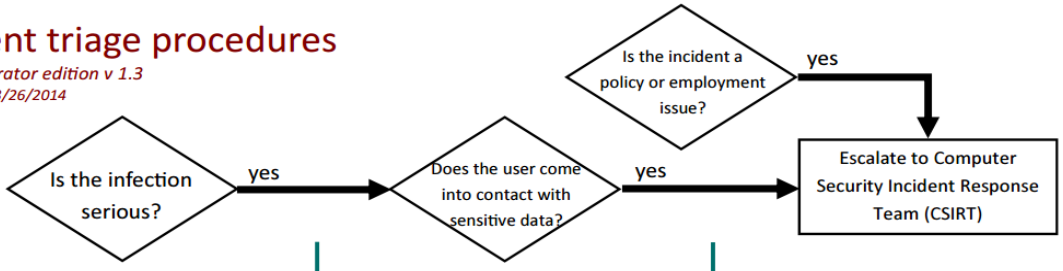
Measures for preventing malware infections

- Ensure all 3rd party applications are up to date (e.g. Adobe Reader, Flash, Java Runtime Environment)

  Qualys BrowserCheck
  https://browsercheck.qualys.com/
- Upgrade the computer to Windows 7 or Windows 8.
- Ensure computer has the latest antivirus client
- Ensure that Microsoft patches are up to date
- Ensure the system is on the SOONER domain

incident triage procedures

IT Administrator edition v 1.3
last revised 03/26/2014



1. Is the malware a known data-stealer, backdoor Trojan, or rootkit? If so, the infection is serious, otherwise continue to step 2.
2. Is the malware an innocuous threat such as adware, spyware, or tracking cookie? If so, the infection is not serious, otherwise continue to step 3.

   To look up the functionality of malware, use Microsoft's Threat Encyclopedia and/or Sophos:

   - Microsoft (www.microsoft.com/security/portal/Threat/Encyclopedia/Browse.aspx)
   - Sophos (www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware.aspx)

3. Is the infection system-level? If so, the infection is serious.

System-level infections are those found in a directory not writable by standard users (e.g. C:\Windows, C:\Windows\Program Files, C:\Program Files (x86)), and C:\Windows\System32).

Malware that is not a known data-stealer, backdoor, or rootkit that is limited to the user's profile directory does not require escalation.

If you are unable to determine the nature of the infection, escalate to CSIRT.

If the user comes into contact with any of the following data items, escalation is required.

DATA ELEMENT OR TYPE	REF.
Social security number (SSN)	1,2
Driver license number or state ID card number	1,2
Any financial account number	1,2
Any credit or debit card number	1,2,4
Any security code, access code, or password providing access to a financial account	1,2
Any personal health-related data	3

1. Oklahoma Statues §24-161ff and §74-3113.1ff
2. GLBA 501(b), per FIL-27-2005
3. HIPAA/HI-TECH
4. PCI, e.g. VISA CISP, etc.

If the infection is serious but the user does not come into contact with sensitive information, a rebuild is necessary.

Note: Breach reporting requirements do not apply to the user's own personal information, only institutionally-owned and maintained data.

Escalation

1. Contact the CSIRT to begin the escalation process (325-7258, csirt@ou.edu), making a note of what you have done on the system since being dispatched.
2. Leave the computer running. Do not shutdown or move the computer.
3. Leave the computer connected to the network. If you are unable to promptly reach the CSIRT team for guidance, please unplug the network cable or disable the network interface.

Measures for preventing malware infections

- Ensure all 3rd party applications are up to date (e.g. Adobe Reader, Flash, Java Runtime Environment)

  Qualys BrowserCheck
  https://browsercheck.qualys.com/
- Upgrade the computer to Windows 7 or Windows 8.
- Ensure computer has the latest antivirus client
- Ensure that Microsoft patches are up to date
- Ensure the system is on the SOONER domain