DE LA SALLE UNIVERSITY

INFORMATION SECURITY 2

INCIDENT MANAGEMENT

PROF. MICHELLE RENEE D. CHING

3T AY 2016-2017

INTRODUCTION

INFORMATION

- An asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected.

http://www.isaca.org/Journal/archives/2011/Volume-6/Documents/jolv6-11-An-Introduction.pdf

SECURITY

- "The quality or state of being secure—to be free from danger"
- A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

INFORMATION SECURITY

Anderson, J. (2002)

- "Well-informed sense of assurance that the information risks and controls are in balance"

El-Den, J. & Dangi, K. (2015)

- Protects the information from access, use, disclosure, perusal, recording, disruption, or destruction that are not authorized

INFORMATION SECURITY

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information, from a wide range of threats to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information

ISO/IEC TR 18044:2004

- Information Technology — Security Techniques — Information Security Incident Management
- Provides advice and guidance on information security incident management for information security managers and information systems managers

https://www.iso.org/standard/35396.html

ISO/IEC TR 18044:2004 PROVIDES…

- Information on the benefits to be obtained from and the key issues associated with a good information security incident management approach (to convince senior corporate management and those personnel who will report to and receive feedback from a scheme that the scheme should be introduced and used);
- Information on examples of information security incidents, and an insight into their possible causes;
- A description of the planning and documentation required to introduce a good structured information security incident management approach;
- A description of the information security incident management process

https://www.iso.org/standard/35396.html

FACTORS

- The trend of both increased occurrences of and escalating losses from information security incidents that have resulted in serious consequences
- The increase of vulnerabilities in software or systems can affect large parts of an organization's infrastructure and impact operations
- Failure of security controls to prevent incidents
- Legal and regulatory groups requiring the development of an incident management capability
- The growing sophistications and capabilities of profit-oriented attackers

http://www.isaca.org/Journal/archives/2011/Volume-6/Documents/jolv6-11-An-Introduction.pdf

DEFINITIONS

- 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.
- 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.
- Incident management includes incident response. Incident management encompasses a variety of activities including proactive efforts to limit or prevent incidents, whereas incident response is the reactive element in the event of an incident

http://www.isaca.org/Journal/archives/2011/Volume-6/Documents/jolv6-11-An-Introduction.pdf

GOALS

- Detect incidents quickly.
- Diagnose incidents accurately.
- Manage incidents properly.
- Contain and minimize damage.
- Restore affected services.
- Determine root causes.
- Implement improvements to prevent recurrence.

http://www.isaca.org/Journal/archives/2011/Volume-6/Documents/jolv6-11-An-Introduction.pdf

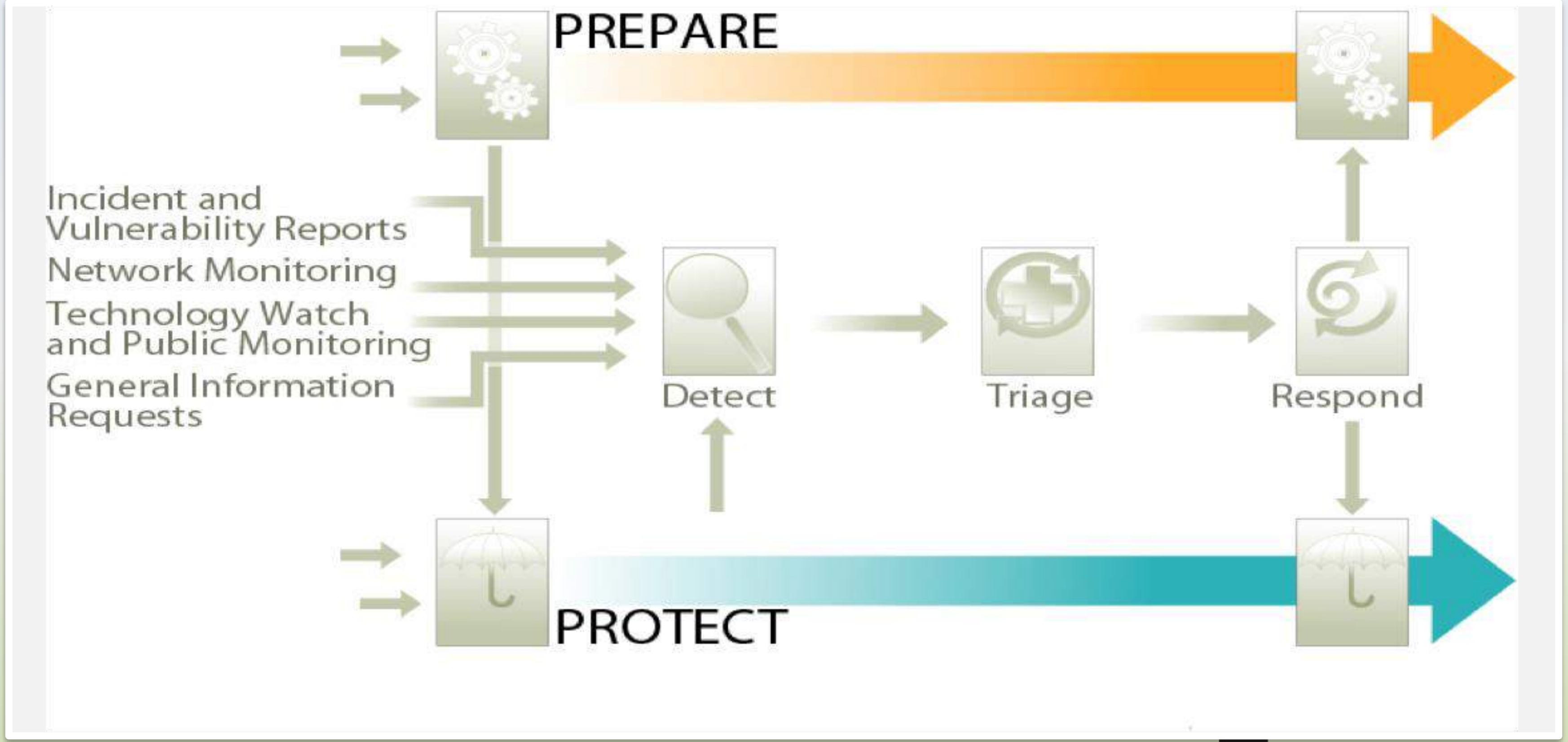
WANNACRY RANSOMWARE

SHORT QUIZ

SHORT QUIZ #1

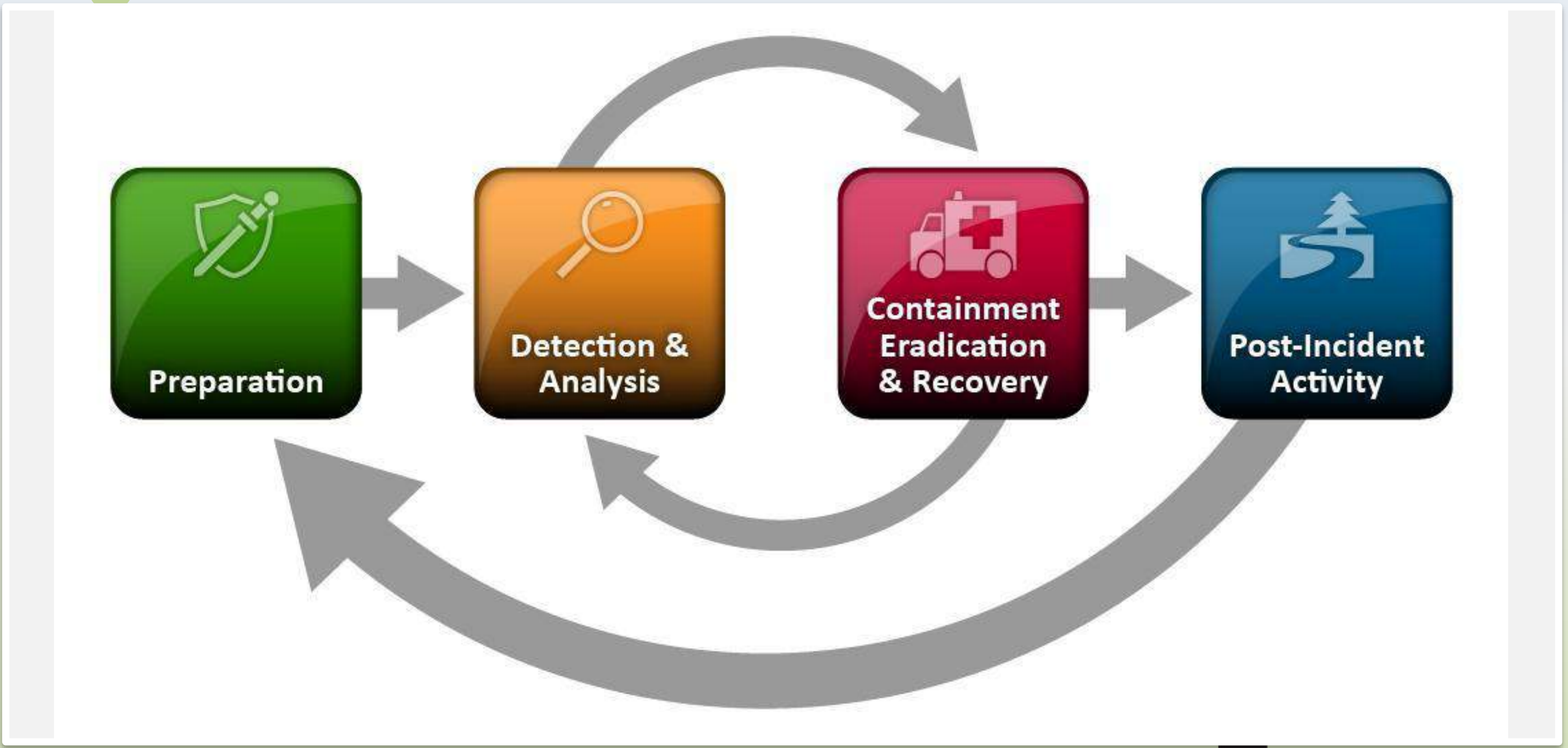
- Differentiate Information Security Event from Information Security Incident
- 10 points

LIFECYCLE


PREPARE
Incident and Vulnerability Reports
Network Monitoring
Technology Watch and Public Monitoring
General Information Requests
Detect
Triage
Respond
PROTECT

https://buildsecurityin.us-cert.gov/sites/default/files/images/221-ImageData-overview-2.png

LIFECYCLE



https://spaces.internet2.edu/download/attachments/50528572/nist_incident-response-life-cycle.bmp?version=1&modificationDate=1389010881078&api=v2

7 STAGES OF INCIDENT RESPONSE

[1] Preparation

- It involves identifying the start of an incident, how to recover, how to get everything back to normal, and creating established security policies including, but not limited to:
  - warning banners
  - user privacy expectations
  - established incident notification processes
  - the development of an incident containment policy
  - creation of incident handling checklists
  - ensuring the corporate disaster recovery plan is up to date
  - making sure the security risk assessment process is functioning and active
- Should contemplate different types of training your team needs such as OS support, specialized investigative techniques, incident response tool usage, and corporate environmental procedure requirements
- Make sure you have certain tools in place in case of a system breach. This includes monitoring your own sensors, probes, and monitors on critical systems, tracking databases in core systems and completing active audit logs for all server network aspects and components

https://phoenixts.com/blog/7-stages-incident-response-plan/

7 STAGES OF INCIDENT RESPONSE

[2] Identification of an Actual Incident

- The first question you want your team to answer is; is the event an unusual activity or more? Once that answer has been established you are going to want to check out some areas of the affected system. This includes suspicious entries in system or network accounting, excessive login attempts, unexplained new user accounts, unexpected new files, etc.
- 6 Levels of Classification
  - Level 1 – Unauthorized Access
  - Level 2 – Denial of Services
  - Level 3 – Malicious Code
  - Level 4 – Improper Usage
  - Level 5 – Scans/Probes/Attempted Access
  - Level 6 – Investigation Incident

https://phoenixts.com/blog/7-stages-incident-response-plan/

7 STAGES OF INCIDENT RESPONSE

[3] Containment

- 2 Coverage Areas
  1. Protecting and keeping available critical computing resources where possible
  2. Determining the operational status of the infected computer, system or network
- 3 Options on Determining Operational Status
  1. Disconnect system from the network and allow it to continue stand-alone operations
  2. Shut down everything immediately
  3. Continue to allow the system to run on the network and monitor the activities

https://phoenixts.com/blog/7-stages-incident-response-plan/

7 STAGES OF INCIDENT RESPONSE

[4] Investigation

- A systematic review needs to take place on all the:
  - bit-stream copies of the drives
  - external storage
  - real-time memory
  - network devices logs
  - system logs
  - application logs
  - and other supporting data
- Able to answer questions such as; what data was accessed? who did it? and what do the log reviews reveal?
- Keep well-written documentation of everything you do during the investigation, especially since external threats may require law enforcement involvement

https://phoenixts.com/blog/7-stages-incident-response-plan/

7 STAGES OF INCIDENT RESPONSE

[5] Eradication

- Process of actually getting rid of the issue on your computer, system or network. This step should only take place after all external and internal actions are completed.
- 2 Important
  - Cleanup usually consists of running your antivirus software, uninstalling the infected software, rebuilding the OS or replacing the entire hard drive and reconstructing the network
  - Notification always includes relevant personnel, both above and below the incident response team manager in the reporting chain

https://phoenixts.com/blog/7-stages-incident-response-plan/

7 STAGES OF INCIDENT RESPONSE

[6] Recovery

- The company or organization returns to normalcy
- 2 Recovery Steps
  1. Service restoration, which is based on implementing corporate contingency plans
  2. System and/or network validation, testing, and certifying the system as operational
- Any component that was compromised must become re-certified as both operational and secure

https://phoenixts.com/blog/7-stages-incident-response-plan/

7 STAGES OF INCIDENT RESPONSE

[7] Follow-Up

- Few follow-up questions that should be answered to ensure the process is sufficient and effective
  - Was there sufficient preparation?
  - Did detection occur in a timely manner?
  - Were communications conducted clearly?
  - What was the cost of the incident? Did you have a Business Continuity Plan in place?
  - How can we prevent it from happening again?

https://phoenixts.com/blog/7-stages-incident-response-plan/

INCIDENT IN INCIDENT MANAGEMENT

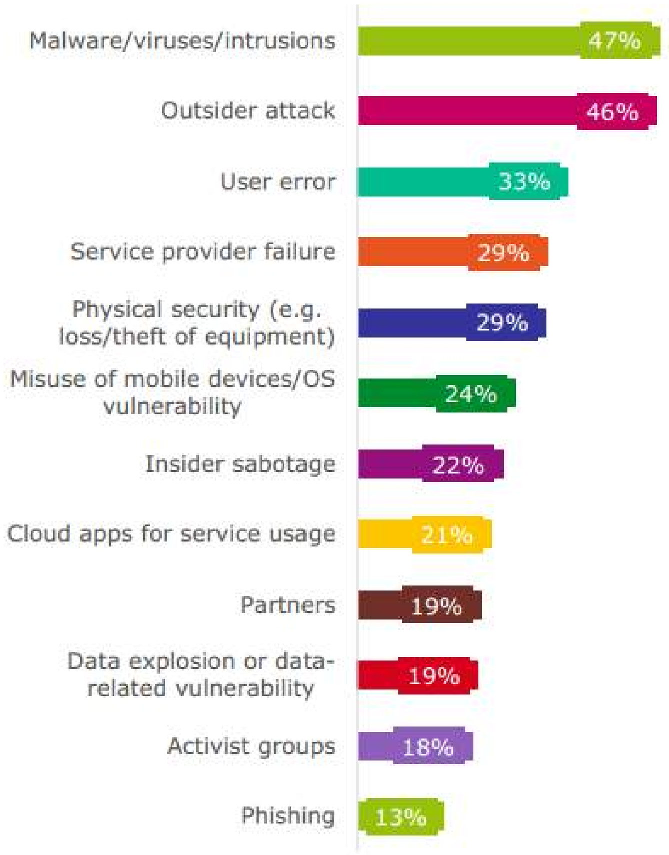
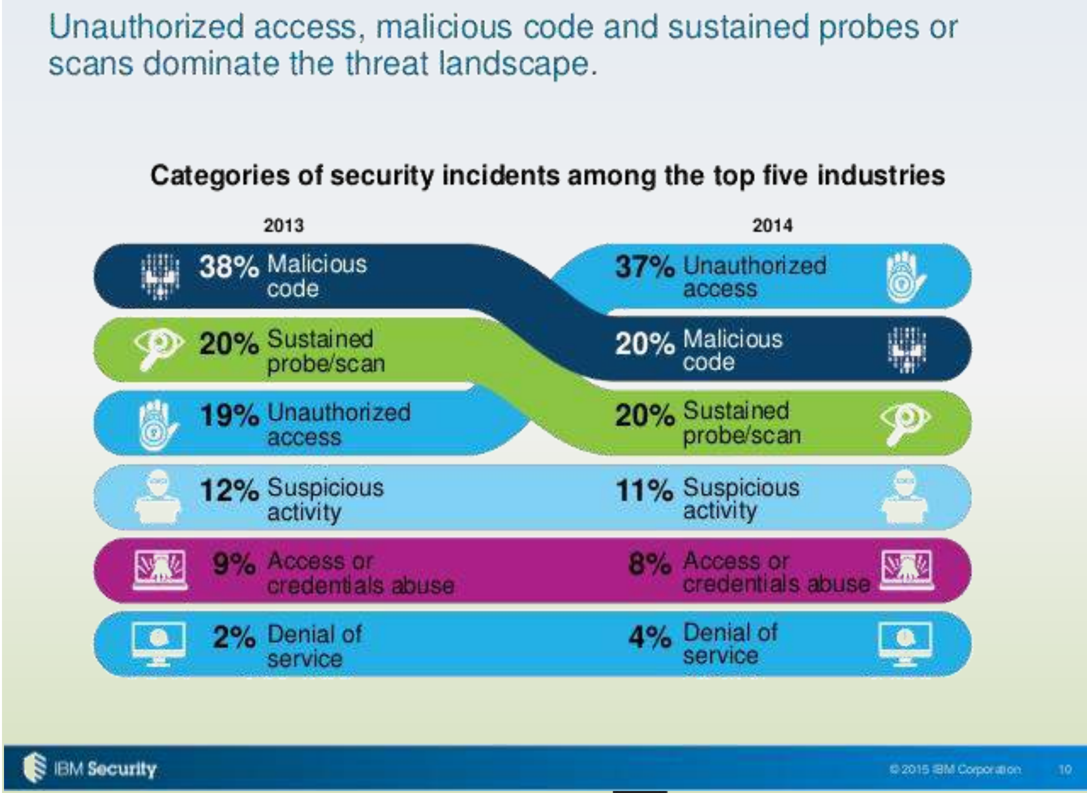


Figure 16: "What was the root cause of the security breaches your organization experienced?", *only asked to respondents that have experienced a security breach (1241 respondents)*

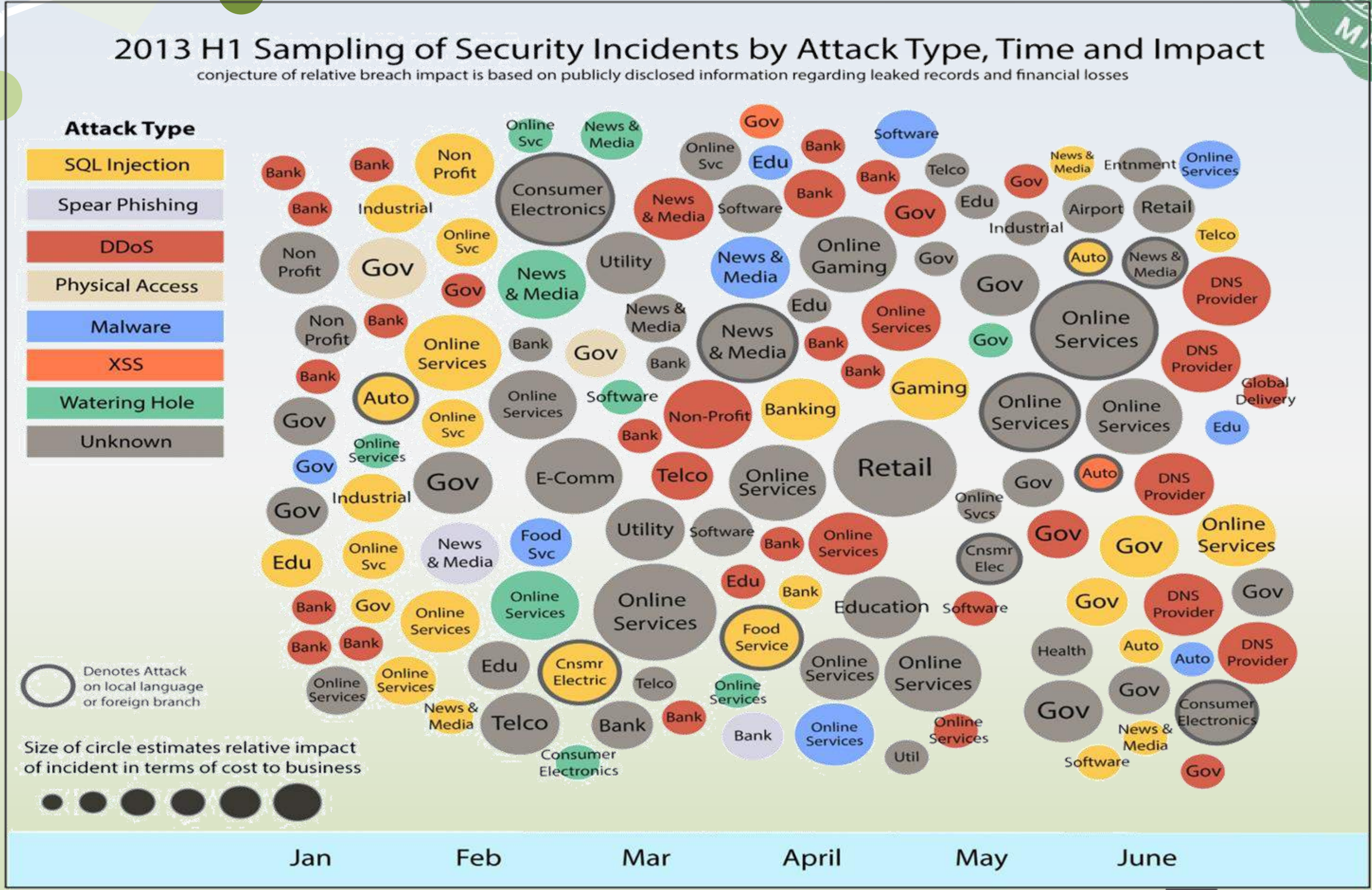


Unauthorized access, malicious code and sustained probes or scans dominate the threat landscape.

Categories of security incidents among the top five industries

2013	2014
38% Malicious code	37% Unauthorized access
20% Sustained probe/scan	20% Malicious code
19% Unauthorized access	20% Sustained probe/scan
12% Suspicious activity	11% Suspicious activity
9% Access or credentials abuse	8% Access or credentials abuse
2% Denial of service	4% Denial of service

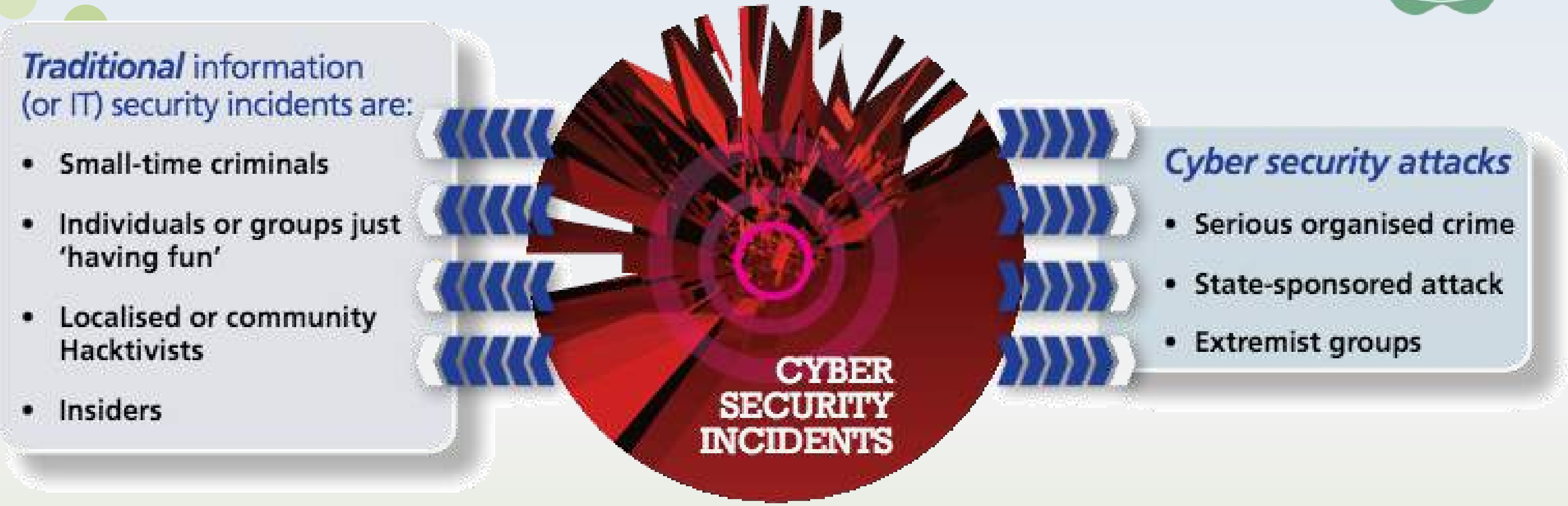
IBM Security © 2015 IBM Corporation 10



2013 H1 Sampling of Security Incidents by Attack Type, Time and Impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

Source: IBM X-Force® Research and Development



Traditional **information (or IT) security incidents are:**

- Small-time criminals
- Individuals or groups just ‘having fun’
- Localised or community Hacktivists
- Insiders

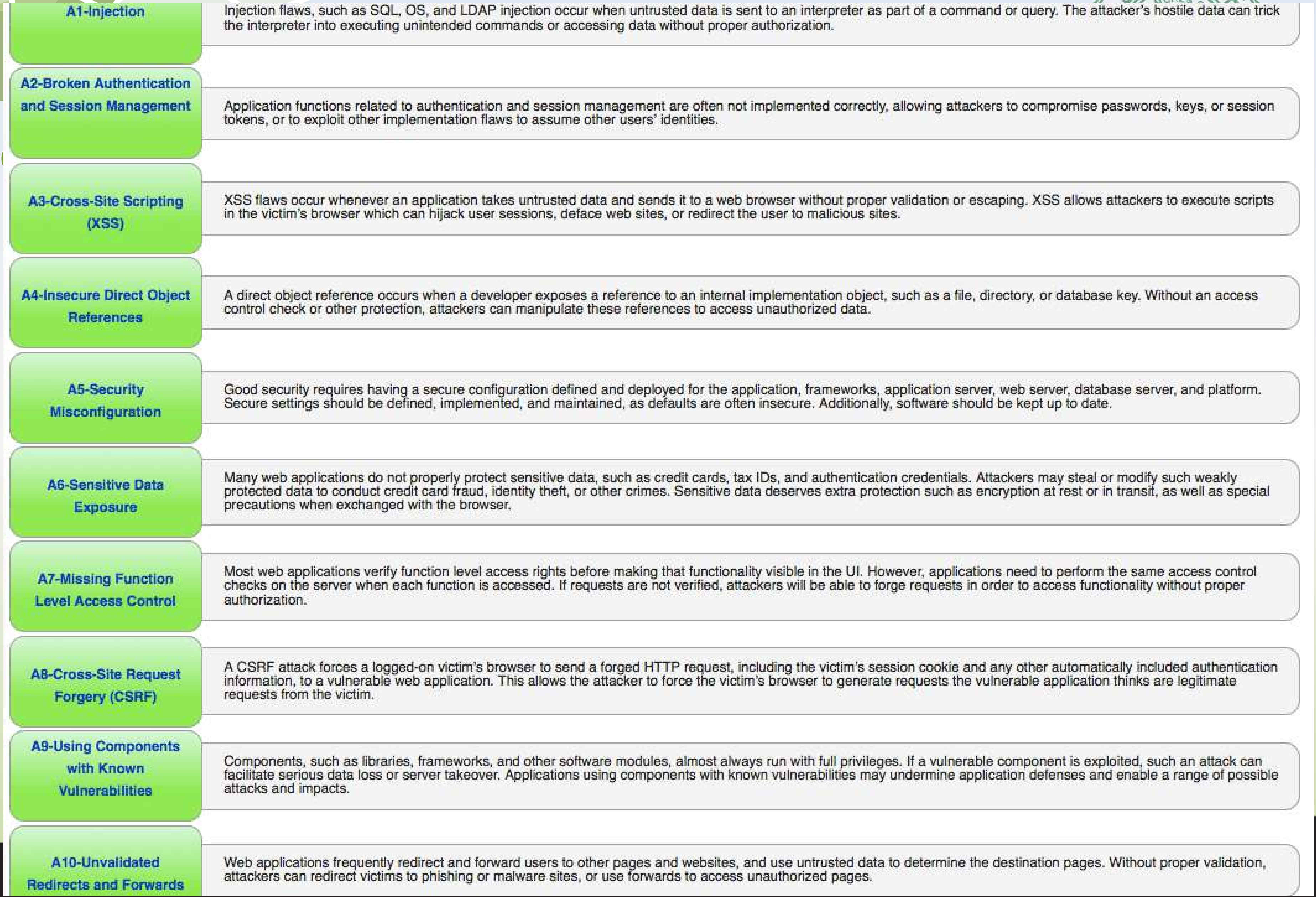
CYBER SECURITY INCIDENTS

Cyber security attacks

- Serious organised crime
- State-sponsored attack
- Extremist groups

Figure 2: Different types of cyber security incidents

> “We classify all information security incidents as Social; Hacking; Malware; or Misuse; as that is what is commonly understood”



A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2-Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4-Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5-Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
A6-Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A7-Missing Function Level Access Control	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
A8-Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
A9-Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
A10-Unvalidated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

CLASS ACTIVITY

TERMINOLOGIES

- Intrusion
- Unauthorized access
- Compromise of system integrity
- Theft
- Web site defacement
- Email Hoax
- Denial of resources
- Virus
- Trojan
- IP spoofing
- Email SPAM
- Unauthorized use
- Port scan
- War dialing
- Email bomb
- Buffer overflow exploit
- Repeated failed login attempts
- Unexpected network bandwidth consumption
- Unexplained system behavior
- Session hijacking

SECURITY ATTACKS

Class Activity #2

- Based on the list of terminologies:
  - Define each and include
    - How does it work
    - What is its effect
    - Why is it being done
  - Give an actual example
- 2 pts each

TERMINOLOGIES

Intrusion

- Unauthorized act of bypassing the security mechanisms of a system

Unauthorized access

- Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use
- Any access that violates the stated security policy

Compromise of system integrity

- Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occured

Theft

- Any circumstance or event with the potential to adversely impact organizational operations, assets, individuals, other organizations, or the National through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service

TERMINOLOGIES

Web site defacement

- An attack on a website that changes the visual appearance of the site or a webpage, where attackers break into a web server and replace the hosted website with one of their own

Email Hoax

- A scam that is distributed in email form that is designed to deceive and defraud email recipients, often for monetary gain

Denial of resources

- The prevention of authorized access to resources or the delaying of time-critical operations

Virus

- A computer program that can copy itself and infect a computer without permission or knowledge of the user that might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk

TERMINOLOGIES

Trojan

- A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program

IP Spoofing

- Sending a network packet that appears to come from a source other than its actual source

Email SPAM

- The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages

Unauthorized use

- The use of a computer or its data for unapproved or possibly illegal activities

TERMINOLOGIES

Port scan

- Using a program to remotely determine which ports on a system are open, whether systems allow connections through those ports

War dialing

- A technique to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for modems, computers, bulletin board systems or computer servers, and fax machines

Email bomb

- A form of Internet abuse which is perpetrated through the sending of massive volumes of email to a specific email address with the goal of overflowing the mailbox and overwhelming the mail server hosting the address, making it into some form of denial of service attack

Buffer overflow exploit

- A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information, where attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system

TERMINOLOGIES

- Repeated failed login attempts
- Unexpected network bandwidth consumption
- Unexplained system behavior
- Session hijacking

SHORT QUIZ

SHORT QUIZ #2

- Define the following:
  1. Intrusion
  2. Theft
  3. Virus
  4. Website Defacement
  5. Port Scan
- 2 points each

Are attacks the same as an incident?

ATTACK IS DEFINED AS

An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself

FORMALLY, INCIDENT IS DEFINED AS

"any unlawful, unauthorized, or unacceptable action that involves a computer system, cell phone, tablet, and any other electronic device with an operating system or that operates on a computer network."

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

IT IS ALSO DEFINED AS

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies

Computer Security Incident
vs.
IT Security Incident
vs.
Information Security Incident

How do they differ?

Computer Security Incident

- An event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed.

IT Security Incident

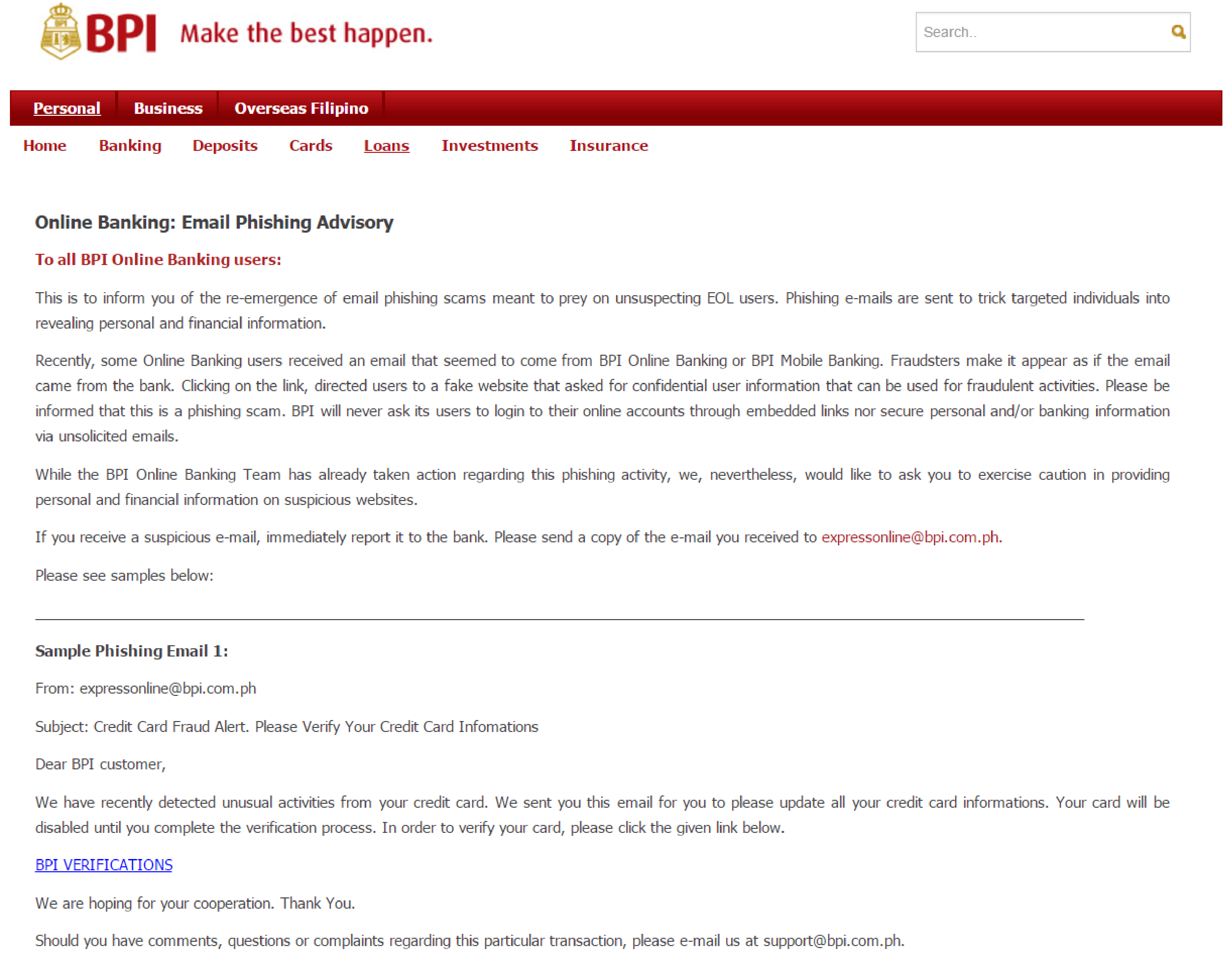
- Any event or set of circumstances threatening its confidentiality, its integrity or its availability

Information Security Incident

- Is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of responsible use policy

So how do we detect, identify, measure, classify and prepare for an incident?

How do we begin and what can we use?



Online Banking: Email Phishing Advisory

To all BPI Online Banking users:

This is to inform you of the re-emergence of email phishing scams meant to prey on unsuspecting EOL users. Phishing e-mails are sent to trick targeted individuals into revealing personal and financial information.

Recently, some Online Banking users received an email that seemed to come from BPI Online Banking or BPI Mobile Banking. Fraudsters make it appear as if the email came from the bank. Clicking on the link, directed users to a fake website that asked for confidential user information that can be used for fraudulent activities. Please be informed that this is a phishing scam. BPI will never ask its users to login to their online accounts through embedded links nor secure personal and/or banking information via unsolicited emails.

While the BPI Online Banking Team has already taken action regarding this phishing activity, we, nevertheless, would like to ask you to exercise caution in providing personal and financial information on suspicious websites.

If you receive a suspicious e-mail, immediately report it to the bank. Please send a copy of the e-mail you received to expressonline@bpi.com.ph.

Please see samples below:

Sample Phishing Email 1:

From: expressonline@bpi.com.ph

Subject: Credit Card Fraud Alert. Please Verify Your Credit Card Infomations

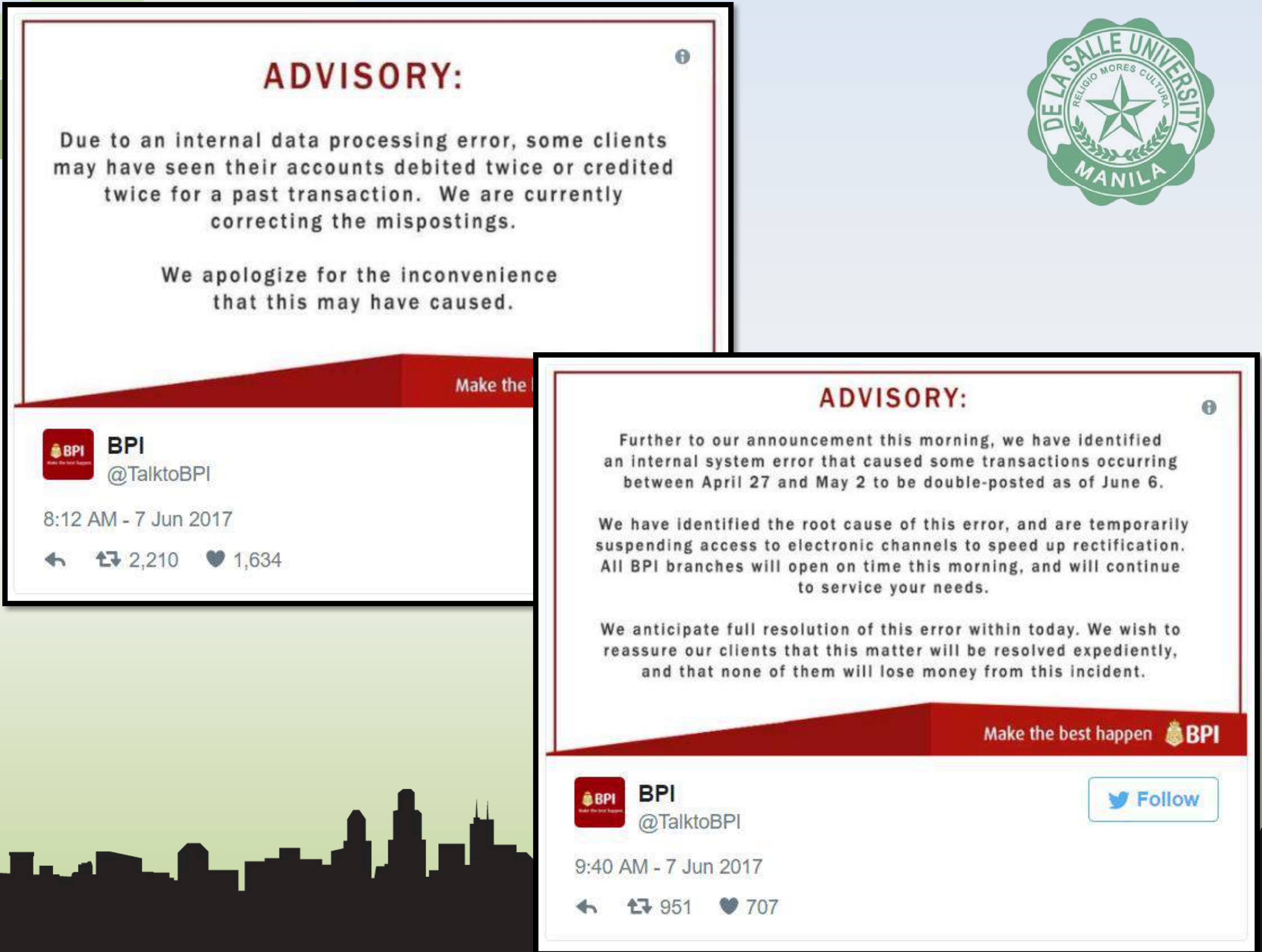
Dear BPI customer,

We have recently detected unusual activities from your credit card. We sent you this email for you to please update all your credit card informations. Your card will be disabled until you complete the verification process. In order to verify your card, please click the given link below.

BPI VERIFICATIONS

We are hoping for your cooperation. Thank You.

Should you have comments, questions or complaints regarding this particular transaction, please e-mail us at support@bpi.com.ph.



ADVISORY:

Due to an internal data processing error, some clients may have seen their accounts debited twice or credited twice for a past transaction. We are currently correcting the mispostings.

We apologize for the inconvenience that this may have caused.

BPI
@TalktoBPI

8:12 AM - 7 Jun 2017

ADVISORY:

Further to our announcement this morning, we have identified an internal system error that caused some transactions occurring between April 27 and May 2 to be double-posted as of June 6.

We have identified the root cause of this error, and are temporarily suspending access to electronic channels to speed up rectification. All BPI branches will open on time this morning, and will continue to service your needs.

We anticipate full resolution of this error within today. We wish to reassure our clients that this matter will be resolved expediently, and that none of them will lose money from this incident.

BPI
@TalktoBPI

9:40 AM - 7 Jun 2017

LET'S START WITH DETECTION…

How do we detect that there is an incident (potentially a security incident)?

How do we detect incidents beyond IT security Incidents?

What do we identify?

DETECTION

Repeated Failed Login Attempts

- When one tries to login to an account but is greeted with an error message even if they enter what they know to be the correct username/email & password combination

Unexpected Network Bandwidth Consumption

- When the bandwidth of a network is being eaten up by other hosts or applications that the user is not aware of

Unexplained System Behavior

When a system is not behaving like normal or as it should, such as glitches or other components not being responsive

Session Hijacking

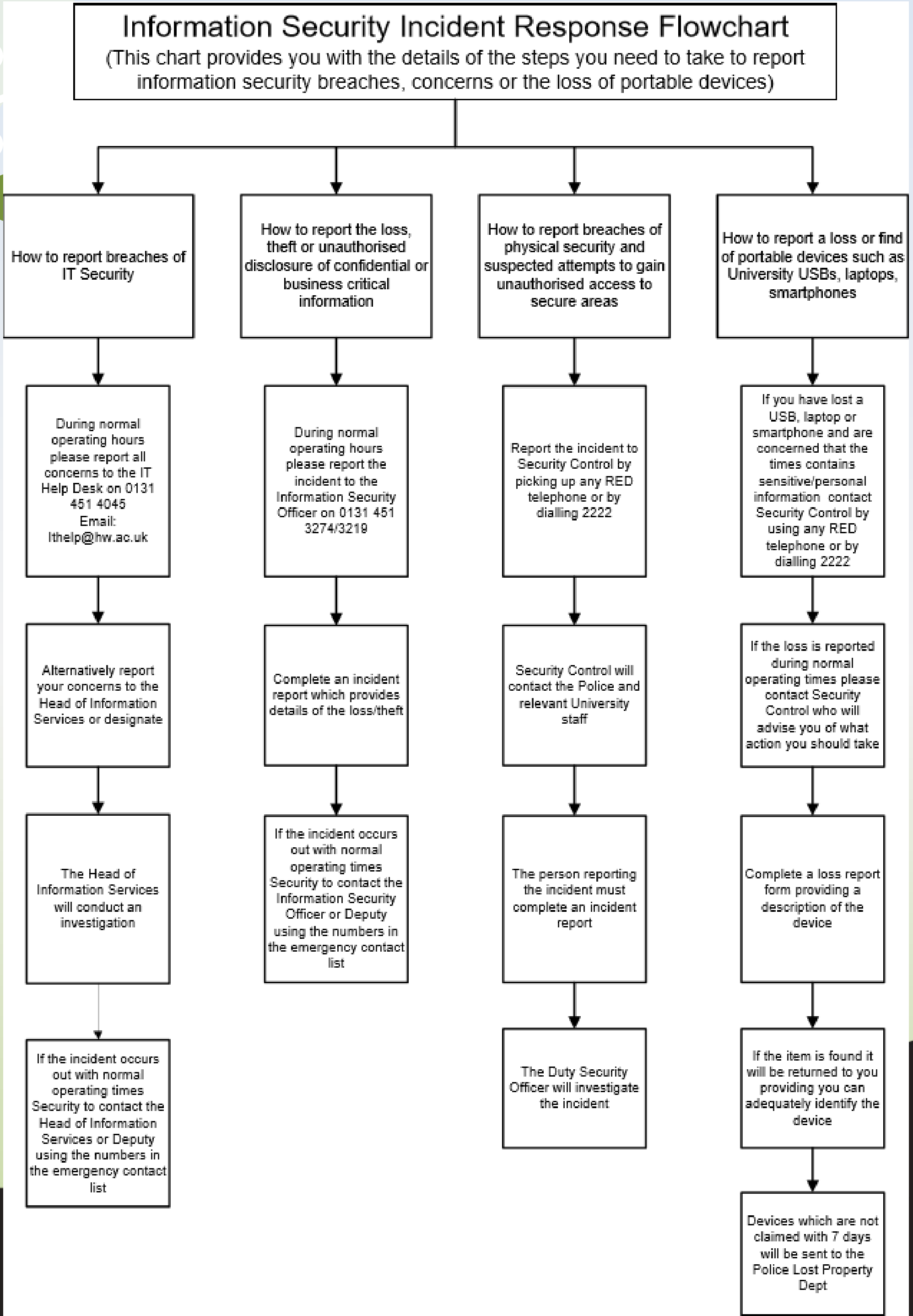
the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system

AFTER DETECTING, WE NEED TO IDENTIFY IT

The question is, when was the incident detected?

How do we know that it is actually an incident and not a false alarm?

Do we know what it is trying to accomplish?



Information Security Incident Response Flowchart

(This chart provides you with the details of the steps you need to take to report information security breaches, concerns or the loss of portable devices)

How to report breaches of IT Security

During normal operating hours please report all concerns to the IT Help Desk on 0131 451 4045 Email: Ithelp@hw.ac.uk

Alternatively report your concerns to the Head of Information Services or designate

The Head of Information Services will conduct an investigation

If the incident occurs out with normal operating times Security to contact the Head of Information Services or Deputy using the numbers in the emergency contact list

How to report the loss, theft or unauthorised disclosure of confidential or business critical information

During normal operating hours please report the incident to the Information Security Officer on 0131 451 3274/3219

Complete an incident report which provides details of the loss/theft

If the incident occurs out with normal operating times Security to contact the Information Security Officer or Deputy using the numbers in the emergency contact list

How to report breaches of physical security and suspected attempts to gain unauthorised access to secure areas

Report the incident to Security Control by picking up any RED telephone or by dialling 2222

Security Control will contact the Police and relevant University staff

The person reporting the incident must complete an incident report

The Duty Security Officer will investigate the incident

How to report a loss or find of portable devices such as University USBs, laptops, smartphones

If you have lost a USB, laptop or smartphone and are concerned that the times contains sensitive/personal information contact Security Control by using any RED telephone or by dialling 2222

If the loss is reported during normal operating times please contact Security Control who will advise you of what action you should take

Complete a loss report form providing a description of the device

If the item is found it will be returned to you providing you can adequately identify the device

Devices which are not claimed with 7 days will be sent to the Police Lost Property Dept

SHORT QUIZ

SHORT QUIZ #3

- Define the following:
  - Computer Security Incident
  - IT Security Incident
  - Information Security Incident
- 10 points

Computer Security Incident

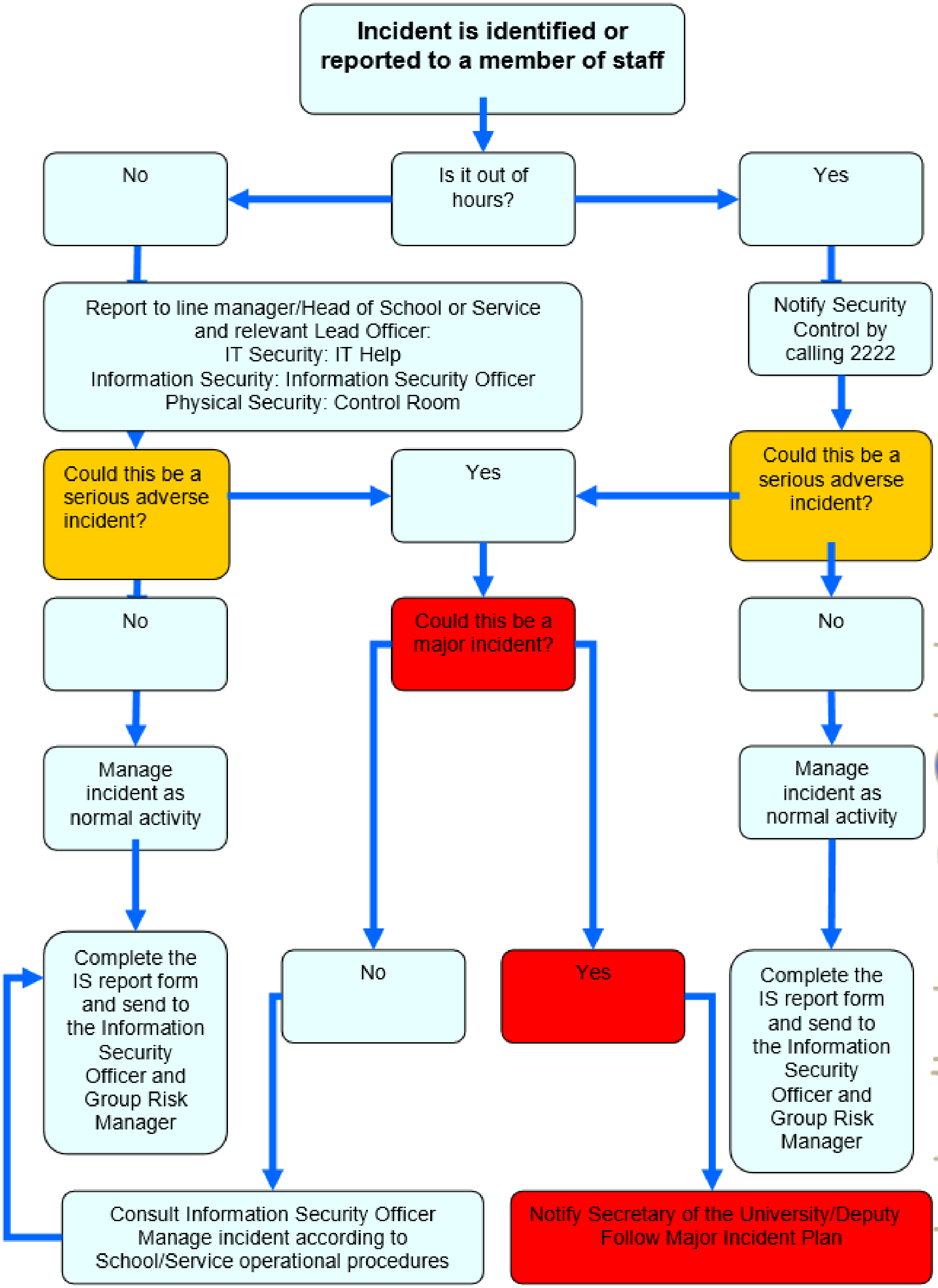
- An event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed.

IT Security Incident

- Any event or set of circumstances threatening its confidentiality, its integrity or its availability

Information Security Incident

- Is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of responsible use policy



Incident is identified or reported to a member of staff

Is it out of hours?

No

Yes

Report to line manager/Head of School or Service and relevant Lead Officer:
IT Security: IT Help
Information Security: Information Security Officer
Physical Security: Control Room

Notify Security Control by calling 2222

Could this be a serious adverse incident?

Yes

Could this be a serious adverse incident?

No

Could this be a major incident?

No

Manage incident as normal activity

Manage incident as normal activity

Complete the IS report form and send to the Information Security Officer and Group Risk Manager

No

Yes

Complete the IS report form and send to the Information Security Officer and Group Risk Manager

Consult Information Security Officer
Manage incident according to School/Service operational procedures

Notify Secretary of the University/Deputy
Follow Major Incident Plan

MEASURE TO PRIORITIZE

Can we always put a dollar/peso value to an incident? Is this the only measure?

How do we measure the impact of an incident with respect to confidentiality, integrity, and availability?

How do we classify incidents in order to manage and respond to it?