UNIT-1

Introduction to Incident Response

Why this subject is important?

- Each one needs efficient manager. Managers are not created in a day.
- system/ machine creates incidents that needs management.
- every interviewer asks about system error/incidents and its management strategies.
- need to pass the exam with great marks.
- Apply knowledge for decision making & in industry.

Definition of incident

- an occurrence of an action or situation that is a separate unit of experience
- occurring or likely to occur especially as a minor consequence or accompaniment.
- Incident management refers to the practice of managing IT services causing disruption. It also involves restoring the services to their normal state without affecting SLAs. The process starts when the end user reports an issue and ends when it gets resolved via quick IT service response or action.

Some interview questions asked by incident response manager and forensics professionals

- Are you comfortable working in a stressful environment?
- What are some of the most important skills for a major incident manager to have?
- How would you manage a situation where your team is not getting along?
- What is your process for managing risk when sending your team into a dangerous area?
- Provide an example of a time when you had to make a difficult decision during an emergency situation. What was the result of your decision?
- If your team was struggling to find resources, how would you go about acquiring them?
- What would you do if you felt like your team was not making any progress on the situation at hand?

Continue..

- How well do you work under pressure?
- Do you have any experience working with government agencies?
- When is it appropriate to call in outside resources for assistance?
- We want to ensure that all of our responders are well-fed and rested. How would you go about doing this?
- Describe your process for delegating tasks to your team members.
- What makes you an ideal candidate for this position? (incident manager)
- Which disaster response teams have you worked with in the past?
- What do you think is the most important thing to remember when managing a large-scale emergency or disaster?
- How often do you update your emergency response plan?
- There is a lack of communication between different emergency response teams. How would you address this?

Continue..

- Define An Incident Management Process?
- Name Some Common Incidents At The Workplace
- Why Is Incident Management Necessary?
- What Is A Recurring Incident And How Can It Be Identified?
- Why Is Real-Time Reporting And Analytics Critical In Incident Management Systems?
- State The Steps Involved In Incident Management Process
- In What Ways Can Businesses Make The Incident Management Process Effective?
- What Is IT Incident Management?
- How Do You Prioritize Incidents?
- What Does Security Incident Mean?
- Name some effective ways to Mitigate and prevent Security Incidents?
- Explain Two Incident Management Tools

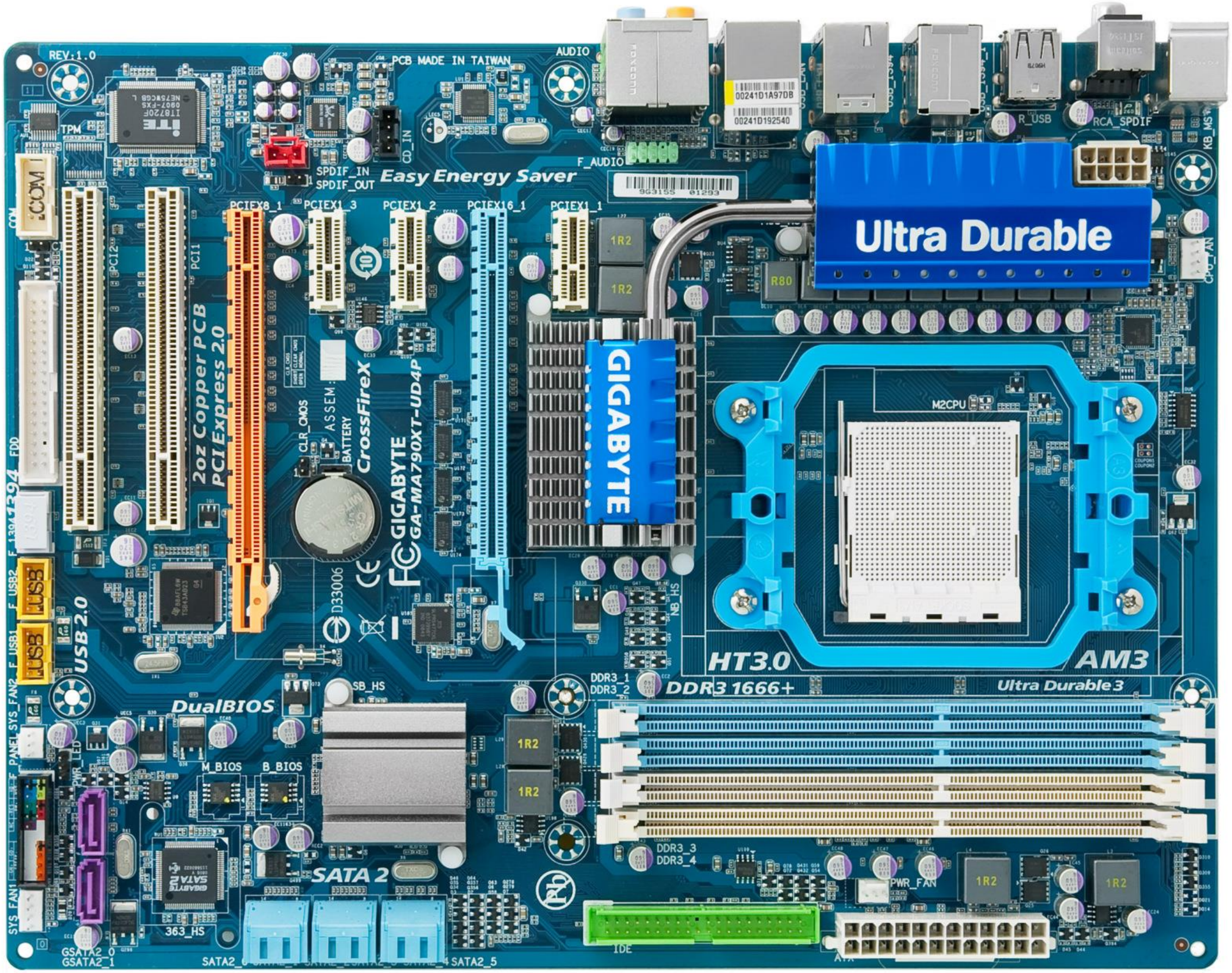
Continue..

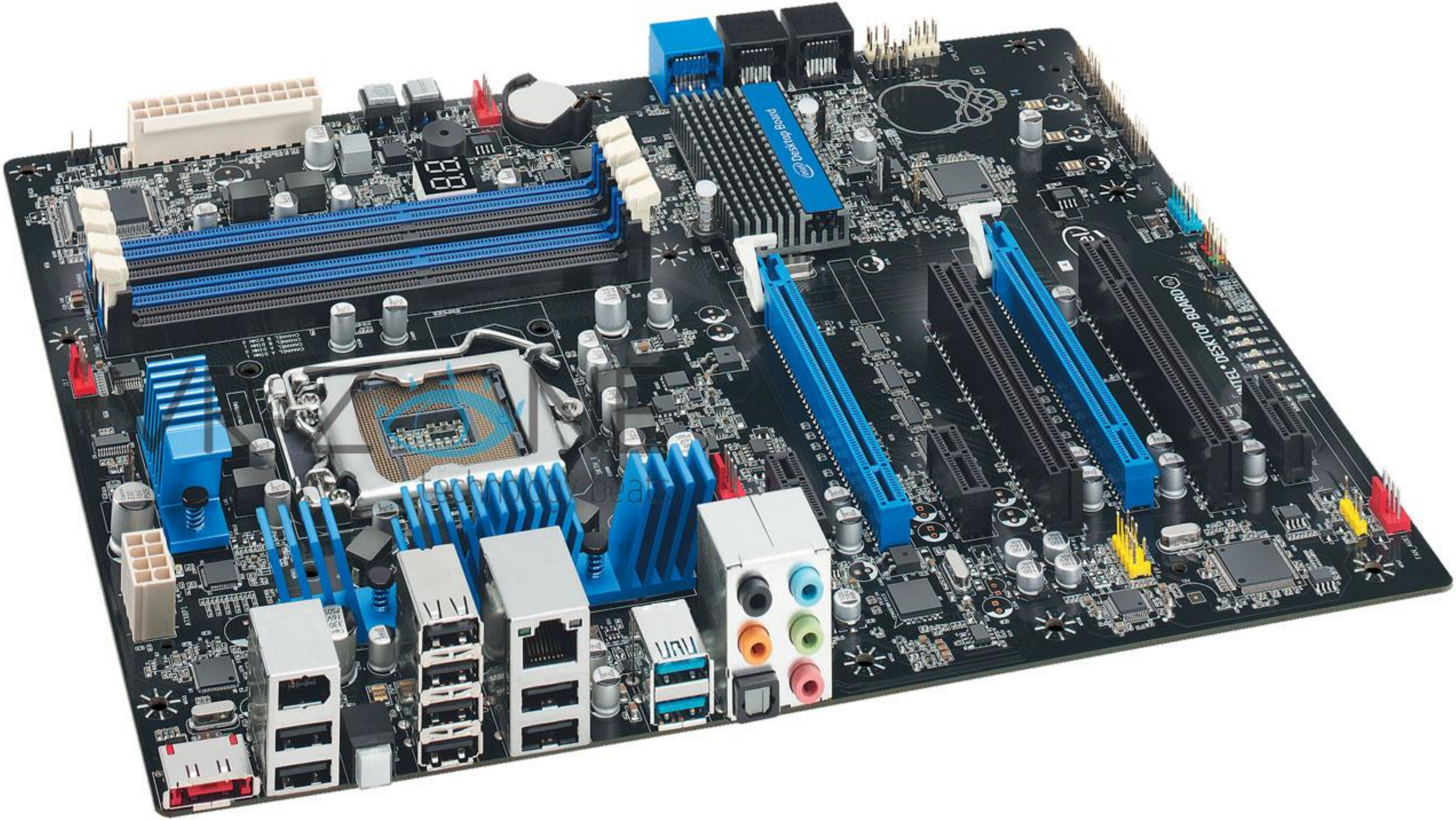
- Is Incident Response Important In Running A Business?
- Why Is It Important To Incorporate Digital Forensics In Incident Response?
- Why is Digital Forensics And Incident Response (DFIR) Important to Businesses That May Be A Target Of Cyber Security Attack?
- Security Information And Event Management (SIEM): What Is It About?
- What Security Incident Management Steps Does ISO/IEC Standard 27035 Outline?
- Explain how you would lead an incident investigation
- How would you maintain a professional demeanor and attitude while being assertive to this person that you will take it from here?
- Share an example of a time when you had to interact with people/groups of widely varying disciplines, cultures, and backgrounds. Explain how you influenced them to follow your lead?
- Please demonstrate your telephone and oral skills by sharing an example of how you would begin the incident investigation and then move through each technology group?
- What are some of the most important skills for an incident response analyst?

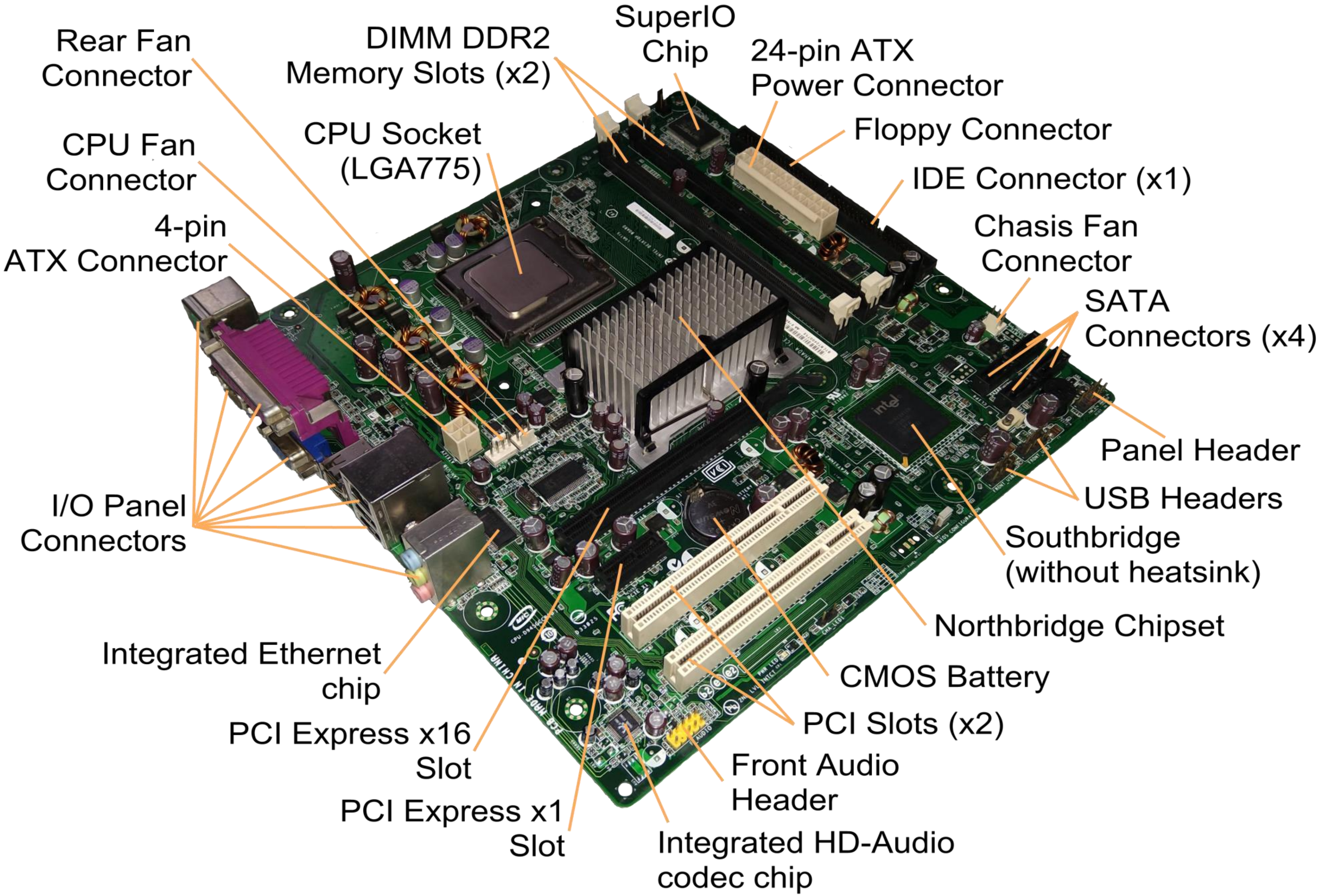
Incident creators

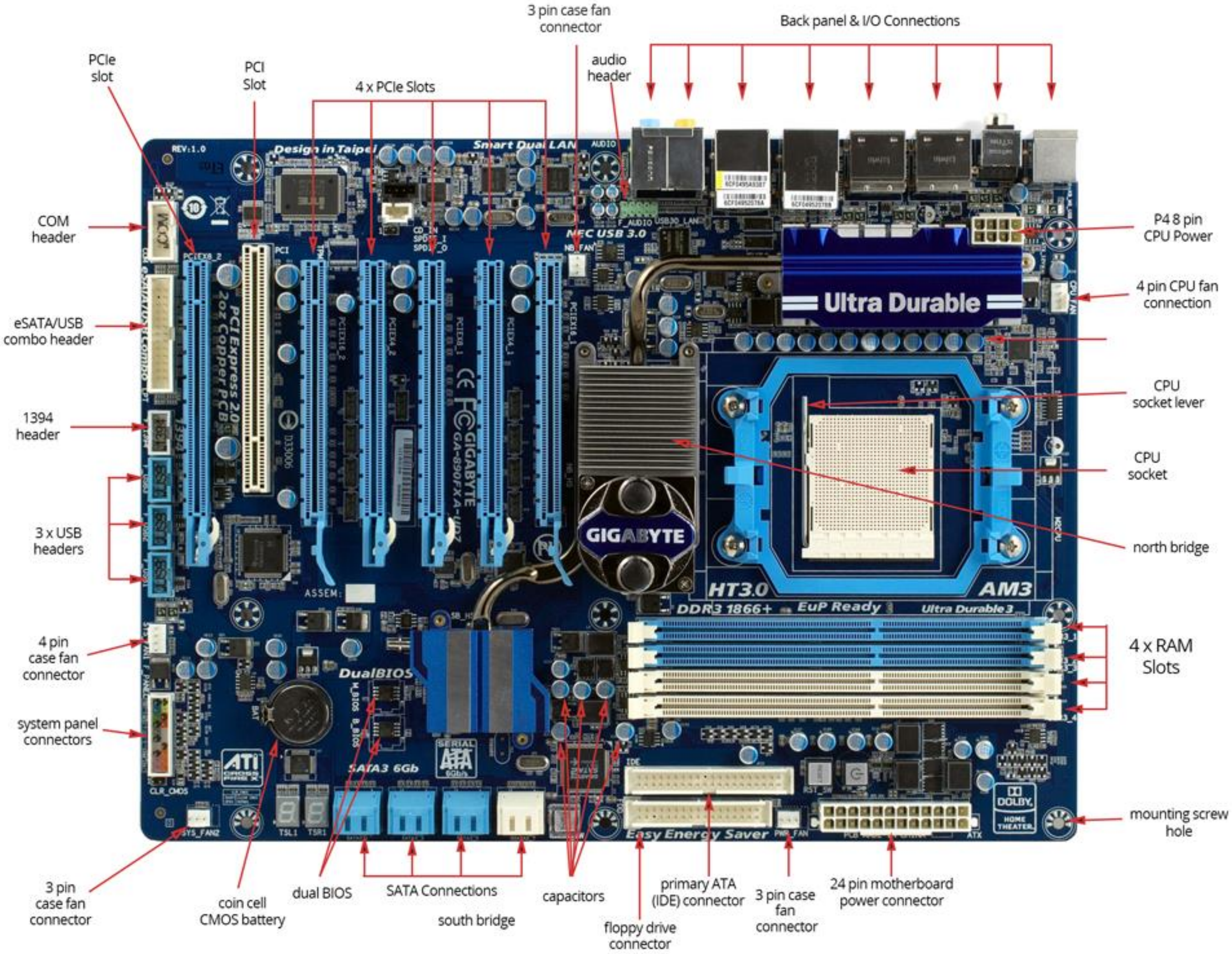
- Computer Hardware and software plays major role in incident creation, handling and management.
- identify components and modules contributing in incident management.

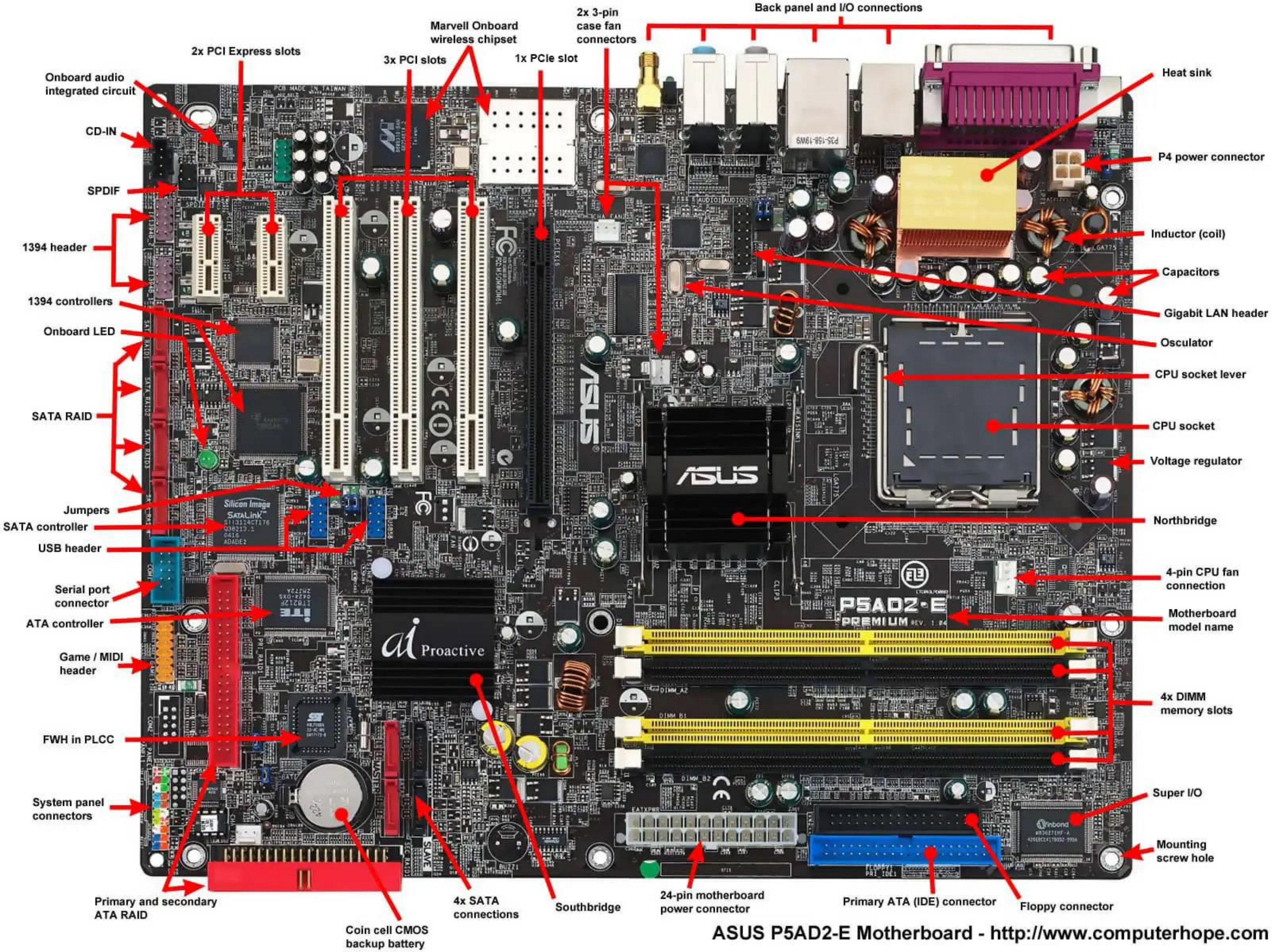
Introduction to Computer




Desktop Board
INTEL • DESKTOP BOARD


Rear Fan Connector
DIMM DDR2 Memory Slots (x2)
SuperIO Chip
24-pin ATX Power Connector
Floppy Connector
CPU Fan Connector
CPU Socket (LGA775)
IDE Connector (x1)
4-pin ATX Connector
Chasis Fan Connector
SATA Connectors (x4)
Panel Header
I/O Panel Connectors
USB Headers
Southbridge (without heatsink)
Northbridge Chipset
Integrated Ethernet chip
CMOS Battery
PCI Express x16 Slot
PCI Slots (x2)
Front Audio Header
PCI Express x1 Slot
Integrated HD-Audio codec chip


3 pin case fan connector
Back panel & I/O Connections
PCIe slot
PCI Slot
4 x PCIe Slots
audio header
COM header
P4 8 pin CPU Power
4 pin CPU fan connection
eSATA/USB combo header
CPU socket lever
1394 header
CPU socket
3 x USB headers
north bridge
4 x RAM Slots
4 pin case fan connector
system panel connectors
mounting screw hole
3 pin case fan connector
coin cell CMOS battery
dual BIOS
SATA Connections
south bridge
capacitors
floppy drive connector
primary ATA (IDE) connector
3 pin case fan connector
24 pin motherboard power connector



ASUS P5AD2-E Motherboard - http://www.computerhope.com

Computer software's

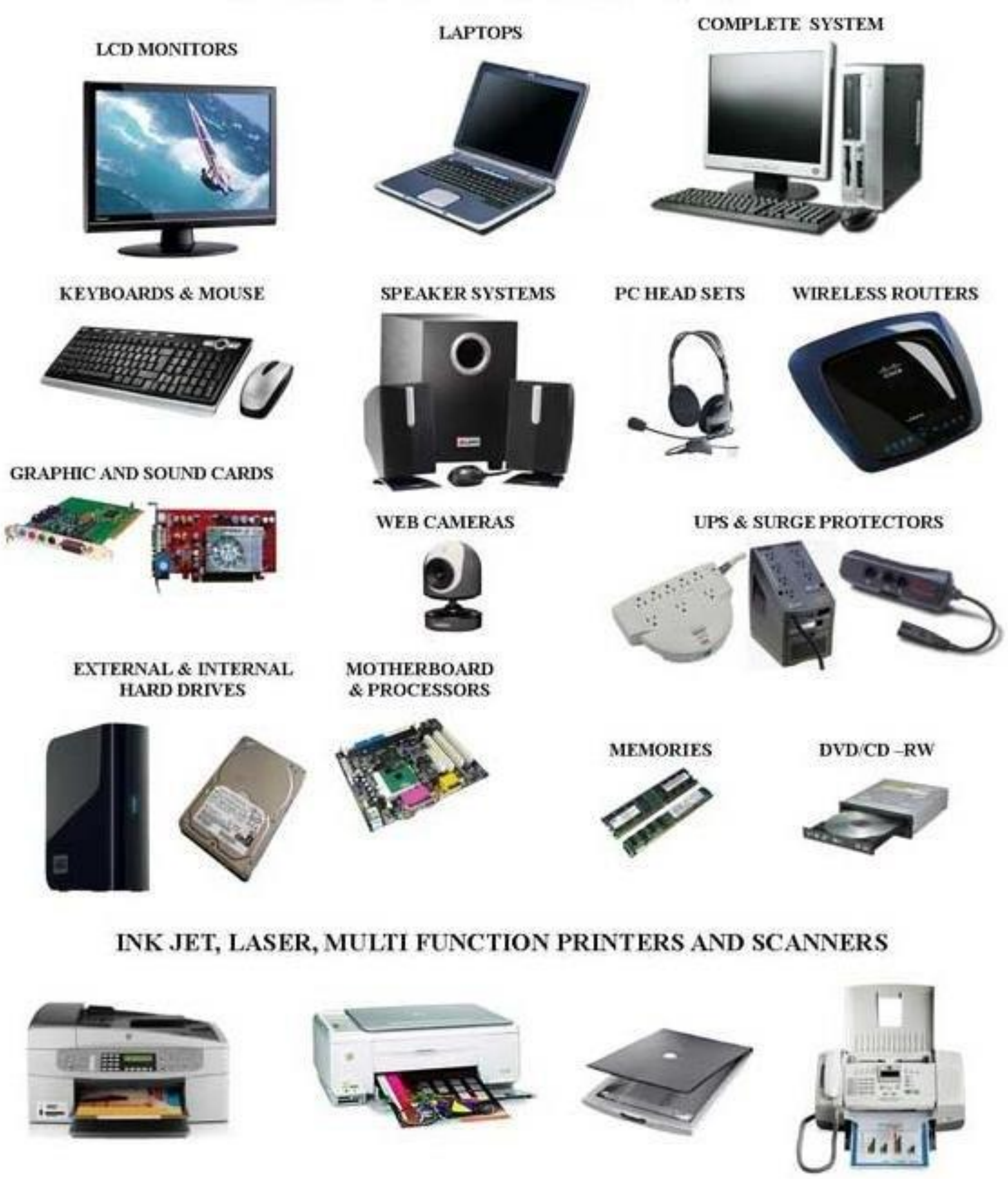
Computer software

- **Computer software** is programming code executed on a computer processor. The code can be machine-level code, or code written for an operating system.

- An **operating system** is software intended to provide a predictable and dependable layer for other programmers to build other software on, which are known as **applications**.

- Operating systems can be found on all smartphones, tablets, and desktop computers. These systems give the device the functionality it needs.

Computer Peripherals

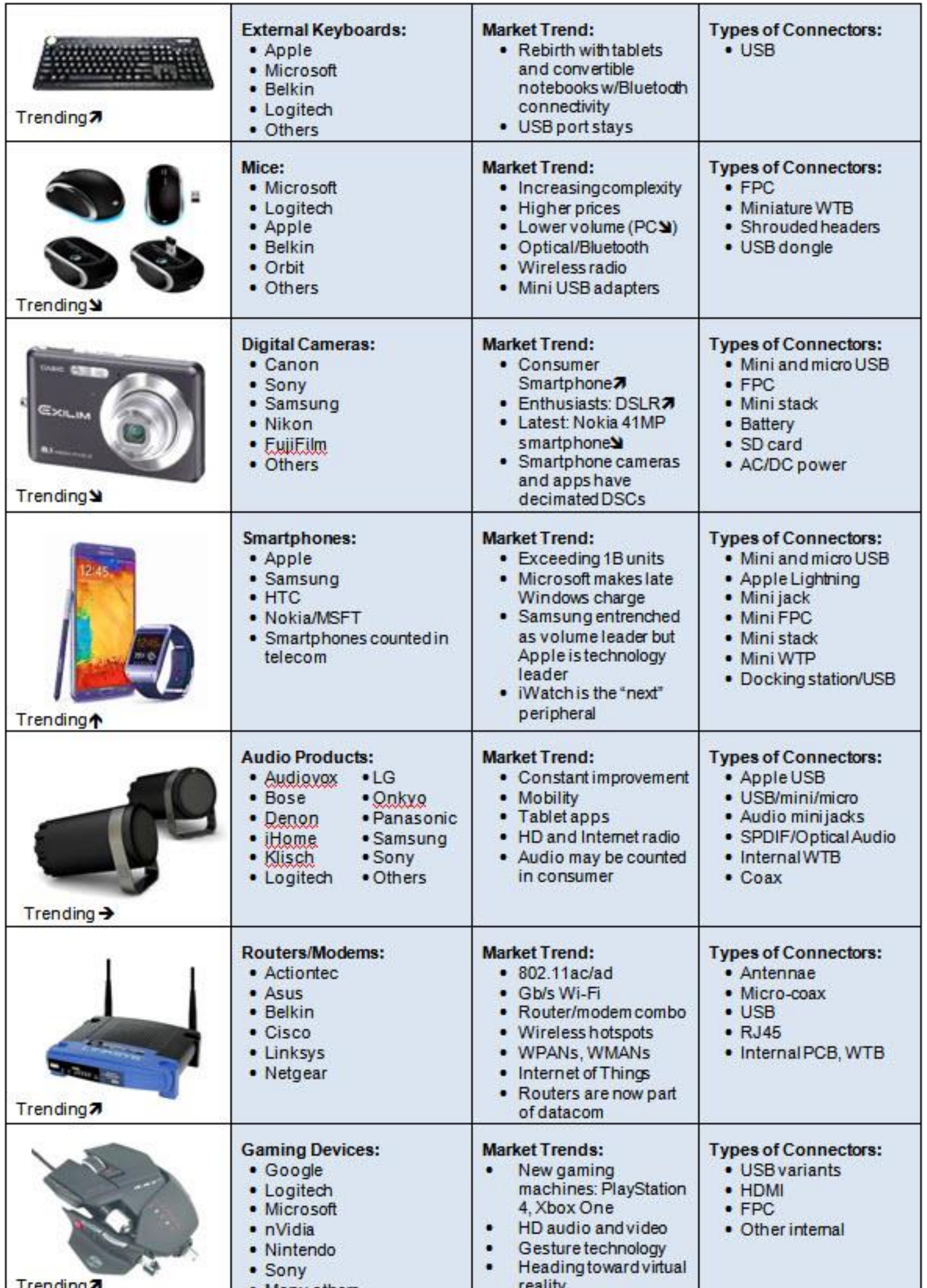


Computer Peripherals

Check for connectors !

Book on computer hardware:

https://www.download.booksfree.org/download-book/?dlm-dp-dl=42071



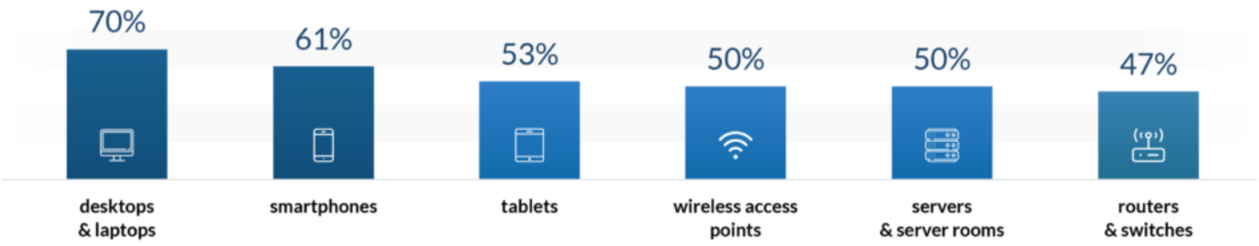
Trending↗	**External Keyboards:** • Apple • Microsoft • Belkin • Logitech • Others	**Market Trend:** • Rebirth with tablets and convertible notebooks w/Bluetooth connectivity • USB port stays	**Types of Connectors:** • USB
Trending↘	**Mice:** • Microsoft • Logitech • Apple • Belkin • Orbit • Others	**Market Trend:** • Increasing complexity • Higher prices • Lower volume (PC↘) • Optical/Bluetooth • Wireless radio • Mini USB adapters	**Types of Connectors:** • FPC • Miniature WTB • Shrouded headers • USB dongle
Trending↘	**Digital Cameras:** • Canon • Sony • Samsung • Nikon • FujiFilm • Others	**Market Trend:** • Consumer Smartphone↗ • Enthusiasts: DSLR↗ • Latest: Nokia 41MP smartphone↘ • Smartphone cameras and apps have decimated DSCs	**Types of Connectors:** • Mini and micro USB • FPC • Mini stack • Battery • SD card • AC/DC power
Trending↑	**Smartphones:** • Apple • Samsung • HTC • Nokia/MSFT • Smartphones counted in telecom	**Market Trend:** • Exceeding 1B units • Microsoft makes late Windows charge • Samsung entrenched as volume leader but Apple is technology leader • iWatch is the "next" peripheral	**Types of Connectors:** • Mini and micro USB • Apple Lightning • Mini jack • Mini FPC • Mini stack • Mini WTP • Docking station/USB
Trending→	**Audio Products:** • Audiovox • LG • Bose • Onkyo • Denon • Panasonic • iHome • Samsung • Klisch • Sony • Logitech • Others	**Market Trend:** • Constant improvement • Mobility • Tablet apps • HD and Internet radio • Audio may be counted in consumer	**Types of Connectors:** • Apple USB • USB/mini/micro • Audio mini jacks • SPDIF/Optical Audio • Internal WTB • Coax
Trending↗	**Routers/Modems:** • Actiontec • Asus • Belkin • Cisco • Linksys • Netgear	**Market Trend:** • 802.11ac/ad • Gb/s Wi-Fi • Router/modem combo • Wireless hotspots • WPANs, WMANs • Internet of Things • Routers are now part of datacom	**Types of Connectors:** • Antennae • Micro-coax • USB • RJ45 • Internal PCB, WTB
Trending↗	**Gaming Devices:** • Google • Logitech • Microsoft • nVidia • Nintendo • Sony • Many others	**Market Trends:** • New gaming machines: PlayStation 4, Xbox One • HD audio and video • Gesture technology • Heading toward virtual reality	**Types of Connectors:** • USB variants • HDMI • FPC • Other internal

Cyber incidents statistics

1 Desktops & laptops are most vulnerable to cybercrimes

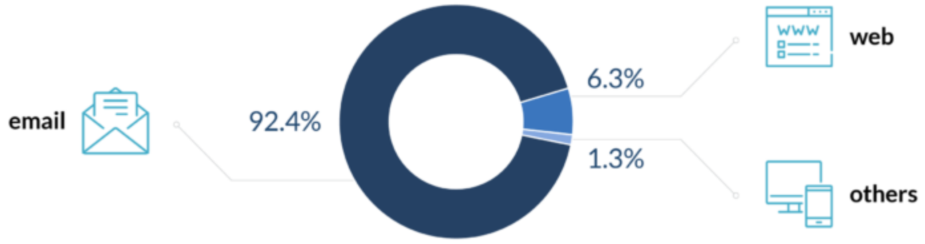
Source: AT&T 2018 Cybersecurity Report

Devices most vulnerable to cybercrimes:



2 Leading malware carriers

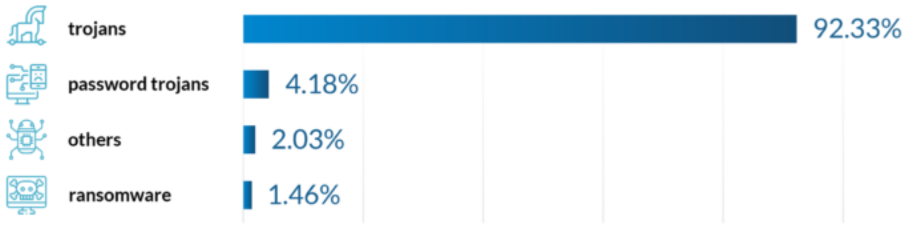
Source: Verizon



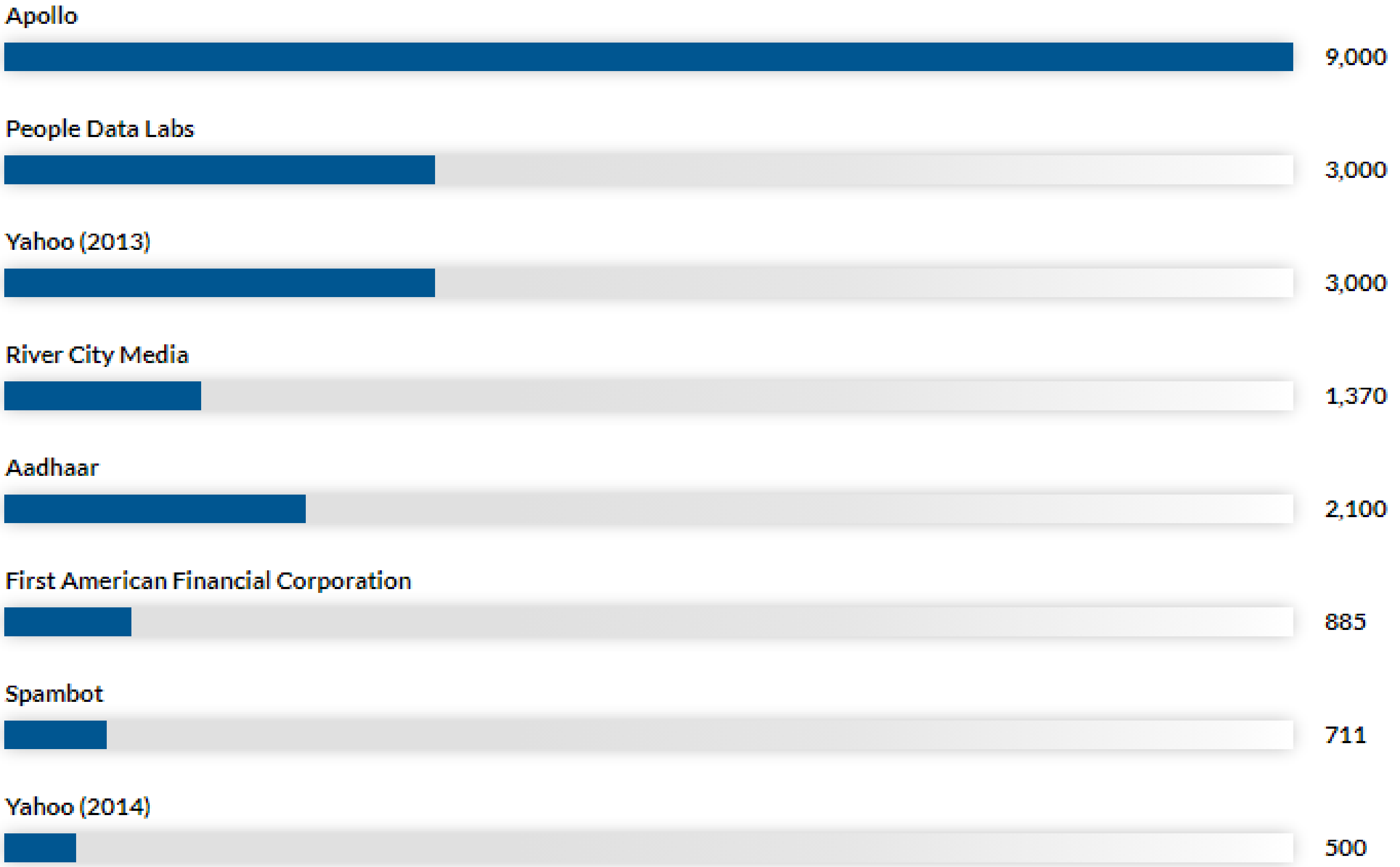
3 Trojans are the leading form of malware on Android

Source: AV-TEST

Distribution of Android malware, by types:



Number of Compromised Data Records in Data Breaches (as of April 2020, in millions)



Sources: Information is Beautiful; Thomson Reuters (2020)

Designed by

More information:

https://financesonline.com/cybercrime-statistics/

Relevant references for more info…

- https://ieeexplore.ieee.org/document/8793072
- https://ieeexplore.ieee.org/document/8531544
- https://ieeexplore.ieee.org/document/8167093
- https://ieeexplore.ieee.org/document/5421283
- https://ieeexplore.ieee.org/document/5401320

Computer security incidents

Incident	How to handle
Unusual behavior from privileged user accounts	
Unauthorized insiders trying to access servers and data	
Anomalies in outbound network traffic	
Traffic sent to or from unknown locations	
Changes in configuration	
Abnormal browsing behavior	
Suspicious registry entries	

Information warfare

- Information warfare can be a combination of lies, manipulated truths, manufactured media, or in some cases exploiting human nature to sow confusion.
- information warfare as a battle fought in cyberspace, online and over computer networks.
- Sometimes the information itself is weaponized to mislead or confuse, other times it does not matter what the information is–the sheer volume of data is used as a weapon in the form of online hacking attempts such as a distributed denial of service (DDS) where millions of emails flood a server at the same time or similar tactics.
- E.g. Hardenberg report recently published.
- E.g. china has not occupied any part of our nation.

Key concept of information security

What is Information Security (InfoSec)?

- Information security (sometimes referred to as InfoSec) covers the tools and processes that organizations use to protect information. This includes policy settings that prevent unauthorized people from accessing business or personal information. InfoSec is a growing and evolving field that covers a wide range of fields, from network and infrastructure security to testing and auditing.
- Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

Three pillars of information security: the CIA triad

Confidentiality: Privacy is a major component of InfoSec, and organizations should enact measures that allow only authorized users access to information. Data encryption, multi-factor_authentication, and data loss prevention are some of the tools enterprises can employ to help ensure data confidentiality.

Integrity: Enterprises must maintain data's integrity across its entire lifecycle. Enterprises with strong InfoSec will recognize the importance of accurate, reliable data, and permit no unauthorized user to access, alter, or otherwise interfere with it. Tools like file permissions, identity management, and user access controls help ensure data integrity.

Availability: InfoSec involves consistently maintaining physical hardware and regularly completing system upgrades to guarantee that authorized users have dependable, consistent access to data as they need it.

Types of computer security incidents/Attacks

- **MAN-IN-THE-MIDDLE ATTACK**

A man-in-the-middle (MitM) attack is a difficult security breach to recognize because it involves a bad actor taking advantage of a trusted “man in the middle” to infiltrate your system. Most often, the hacker will start by compromising a customer’s system to launch an attack on your server.

Suggest preventive measures.

Types of computer security incidents/Attack

DENIAL-OF-SERVICE AND DISTRIBUTED-DENIAL-OF-SERVICE ATTACKS

A denial-of-service (DoS) attack attempts to knock a network or service offline by flooding it with traffic to the point the network or service can’t cope. A distributed-denial-of-service (DDoS) attack hijacks devices (often using botnets) to send traffic from multiple sources to take down a network.

Suggest preventive measures.

Types of computer security incidents/Attack

PHISHING AND SPEAR PHISHING

Phishing involves the hacker sending an email designed to look like it has been sent from a trusted company or website. The email will often sound forceful, odd, or feature spelling and grammatical errors.

Spear phishing, on the other hand, has a specific target. With spear phishing, the hacker may have conducted research on the recipient. For example, they might look through an individual's social media profiles to determine key details like what company the victim works for.

Suggest preventive measures.

Types of computer security incidents/Attack

PASSWORD ATTACK

what are some common passwords ?

the hacker guesses just one of the passwords, they can try that password on other services and get a match. For example, they may get an email and password combination, then try them on bank accounts, looking for a hit. Hackers can use password attacks to compromise accounts, steal your identity, make purchases in your name, and gain access to your bank details.

Suggest preventive measures.

Types of computer security incidents/Attack

CROSS-SITE SCRIPTING ATTACK

A cross-site (XXS) attack attempts to inject malicious scripts into websites or web apps. Launching a successful XXS attack is a reasonably complicated process, which requires the victim to visit a website and have the network translate the website with the attacker’s HTML. This means that when the website reaches the victim’s browser, the website automatically executes the malicious script. The aim of this attack is to capture screenshots, log keystrokes, collect network information, steal cookies, and even remotely access the victim’s device.

Suggest preventive measures.

Types of computer security incidents/Attack

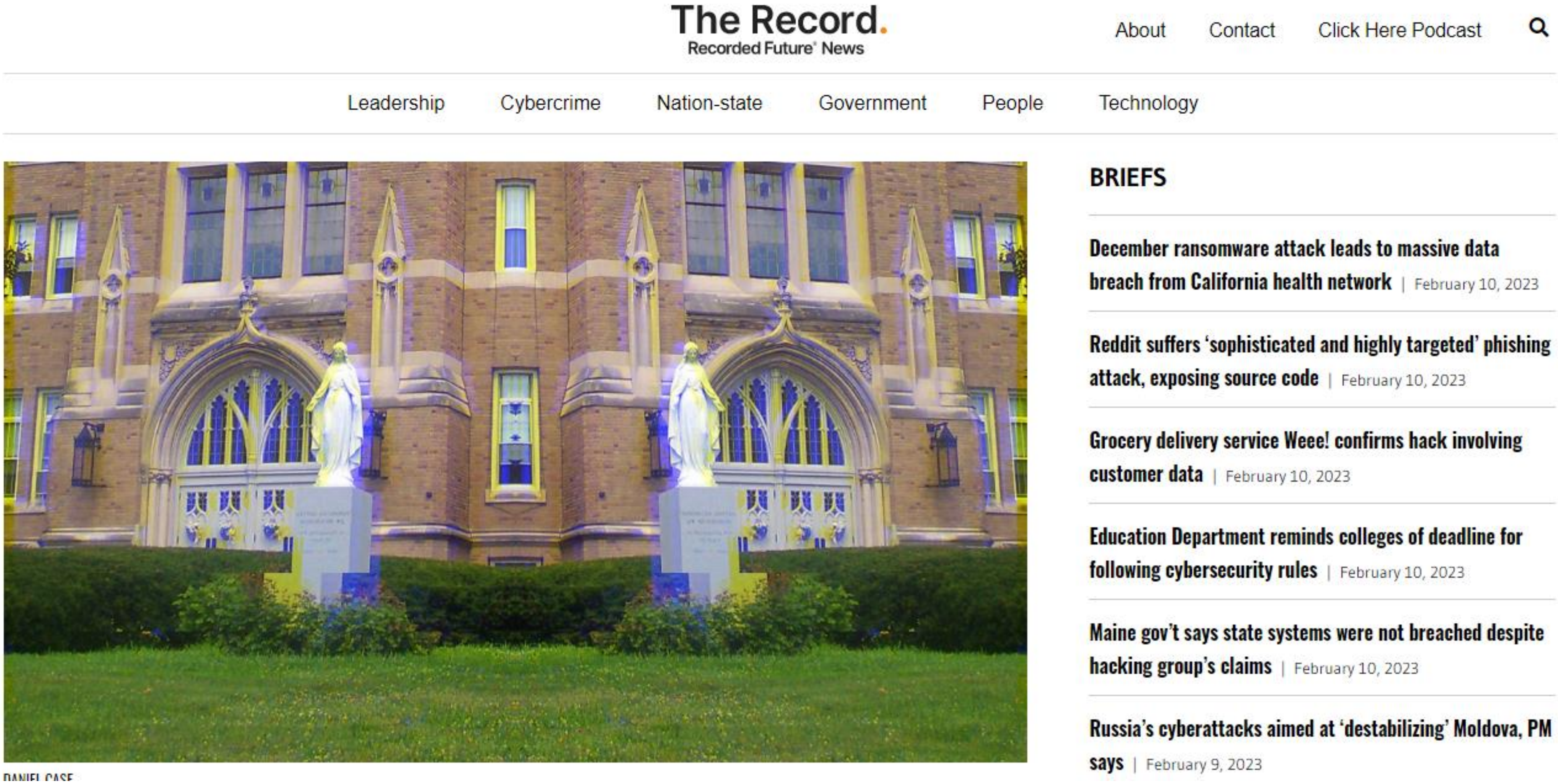
- **MALWARE ATTACK**

A malware attack is an umbrella term that refers to a range of different types of security breaches. This includes the following:

- Polymorphic viruses, which change their signatures frequently to evade signature-based antivirus (AV)
- Systems or boot-record infectors, which are viruses that attach themselves to your hard disk
- Trojan or trojan horses, which are programs that appear as a typical file like an MP3 download but that hide malicious behavior
- File infectors, which are viruses that attach themselves to code on files
- Macro viruses, which are viruses that target and infect major applications
- Stealth viruses, which take control over your system and then use obfuscation methods like changing the filename to avoid detection
- Worms, which are viruses that propagate across a network
- Logic bombs, which are malicious software programs that are triggered by a specific condition, such as a date and time
- Ransomware, which are malware viruses that block access to the victim’s sensitive data until the victim pays a specific amount of money

Suggest preventive measures.

Examples- computer security incidents



The Record.
Recorded Future® News

About Contact Click Here Podcast

Leadership Cybercrime Nation-state Government People Technology

DANIEL CASE

BRIEFS

December ransomware attack leads to massive data breach from California health network | February 10, 2023

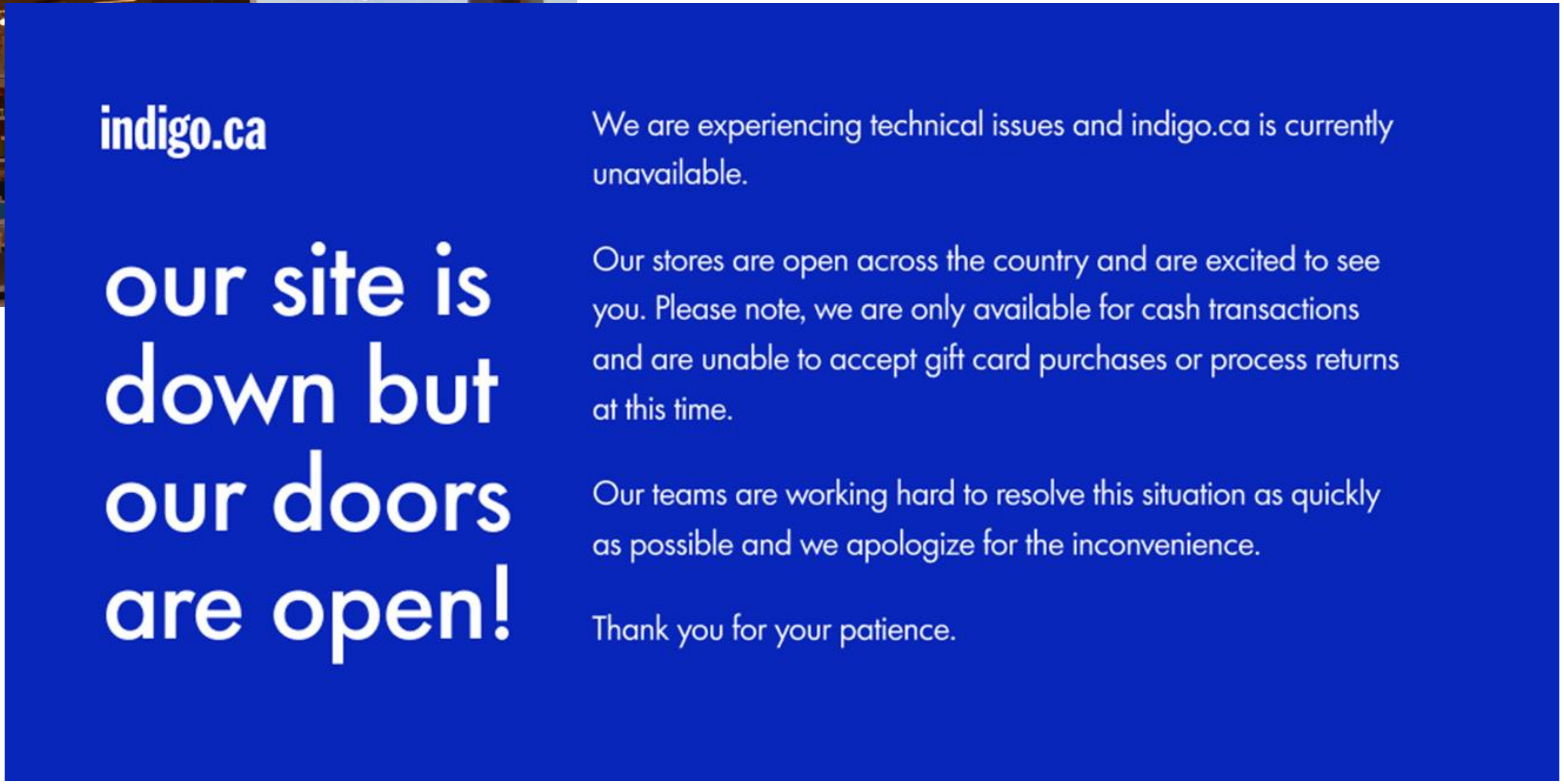
Reddit suffers 'sophisticated and highly targeted' phishing attack, exposing source code | February 10, 2023

Grocery delivery service Weee! confirms hack involving customer data | February 10, 2023

Education Department reminds colleges of deadline for following cybersecurity rules | February 10, 2023

Maine gov't says state systems were not breached despite hacking group's claims | February 10, 2023

Russia's cyberattacks aimed at 'destabilizing' Moldova, PM says | February 9, 2023



indigo.ca

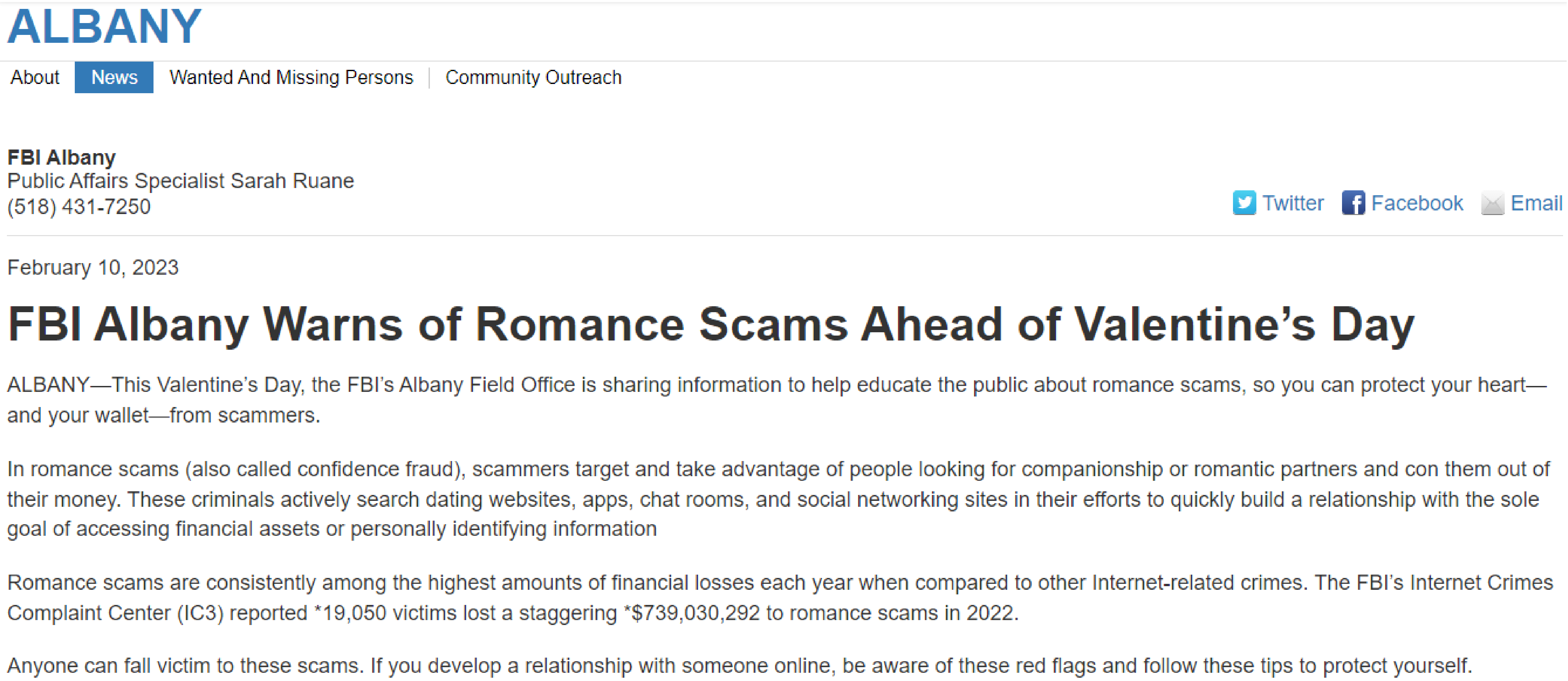
our site is down but our doors are open!

We are experiencing technical issues and indigo.ca is currently unavailable.

Our stores are open across the country and are excited to see you. Please note, we are only available for cash transactions and are unable to accept gift card purchases or process returns at this time.

Our teams are working hard to resolve this situation as quickly as possible and we apologize for the inconvenience.

Thank you for your patience.



ALBANY

FBI Albany
Public Affairs Specialist Sarah Ruane
(518) 431-7250

February 10, 2023

FBI Albany Warns of Romance Scams Ahead of Valentine’s Day

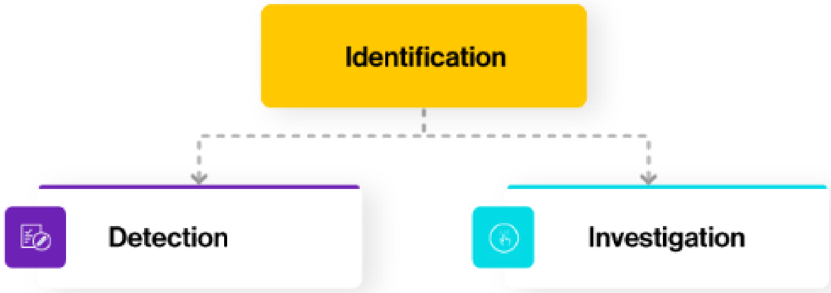
ALBANY—This Valentine’s Day, the FBI’s Albany Field Office is sharing information to help educate the public about romance scams, so you can protect your heart—and your wallet—from scammers.

In romance scams (also called confidence fraud), scammers target and take advantage of people looking for companionship or romantic partners and con them out of their money. These criminals actively search dating websites, apps, chat rooms, and social networking sites in their efforts to quickly build a relationship with the sole goal of accessing financial assets or personally identifying information

Romance scams are consistently among the highest amounts of financial losses each year when compared to other Internet-related crimes. The FBI’s Internet Crimes Complaint Center (IC3) reported *19,050 victims lost a staggering *$739,030,292 to romance scams in 2022.

Anyone can fall victim to these scams. If you develop a relationship with someone online, be aware of these red flags and follow these tips to protect yourself.

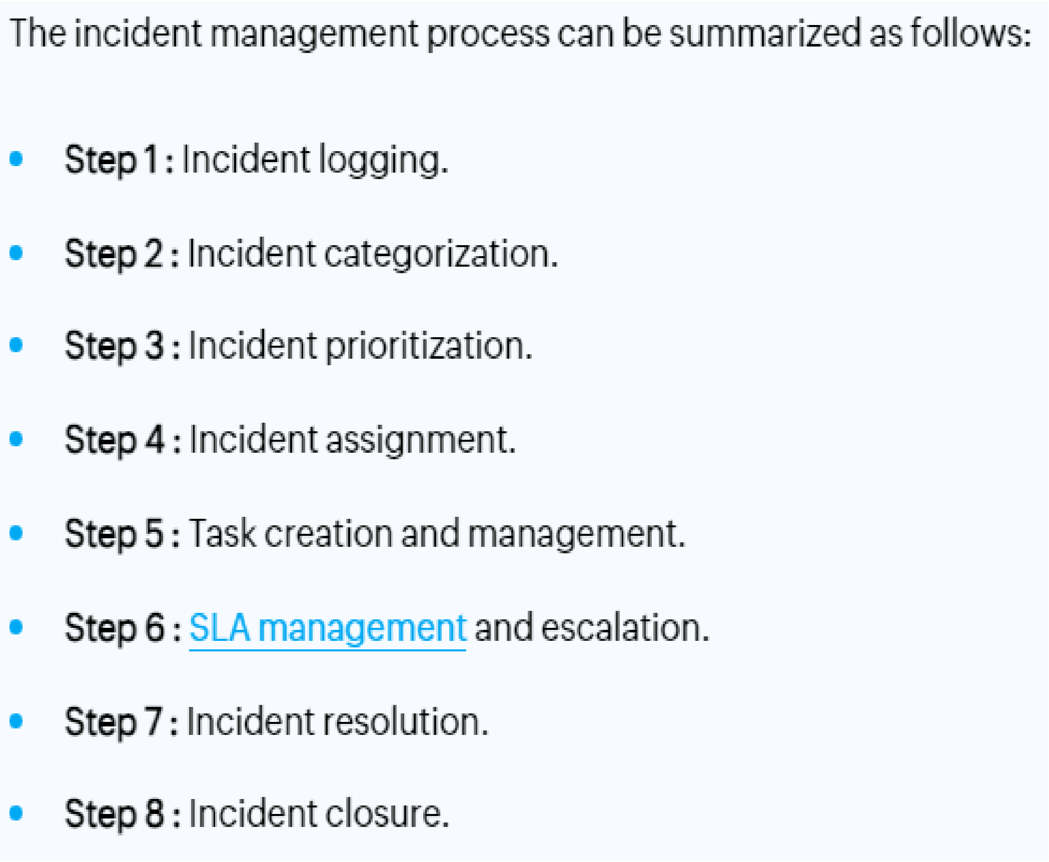
How to identify an incidents



Identification

Detection

Investigation



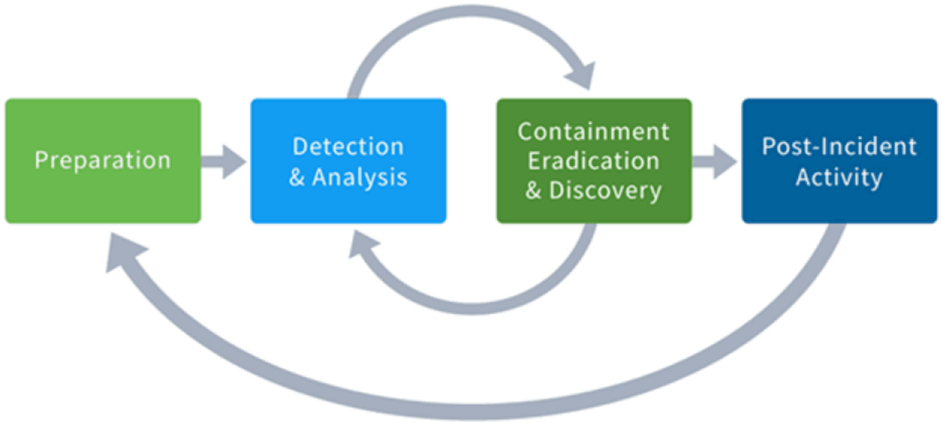
The incident management process can be summarized as follows:

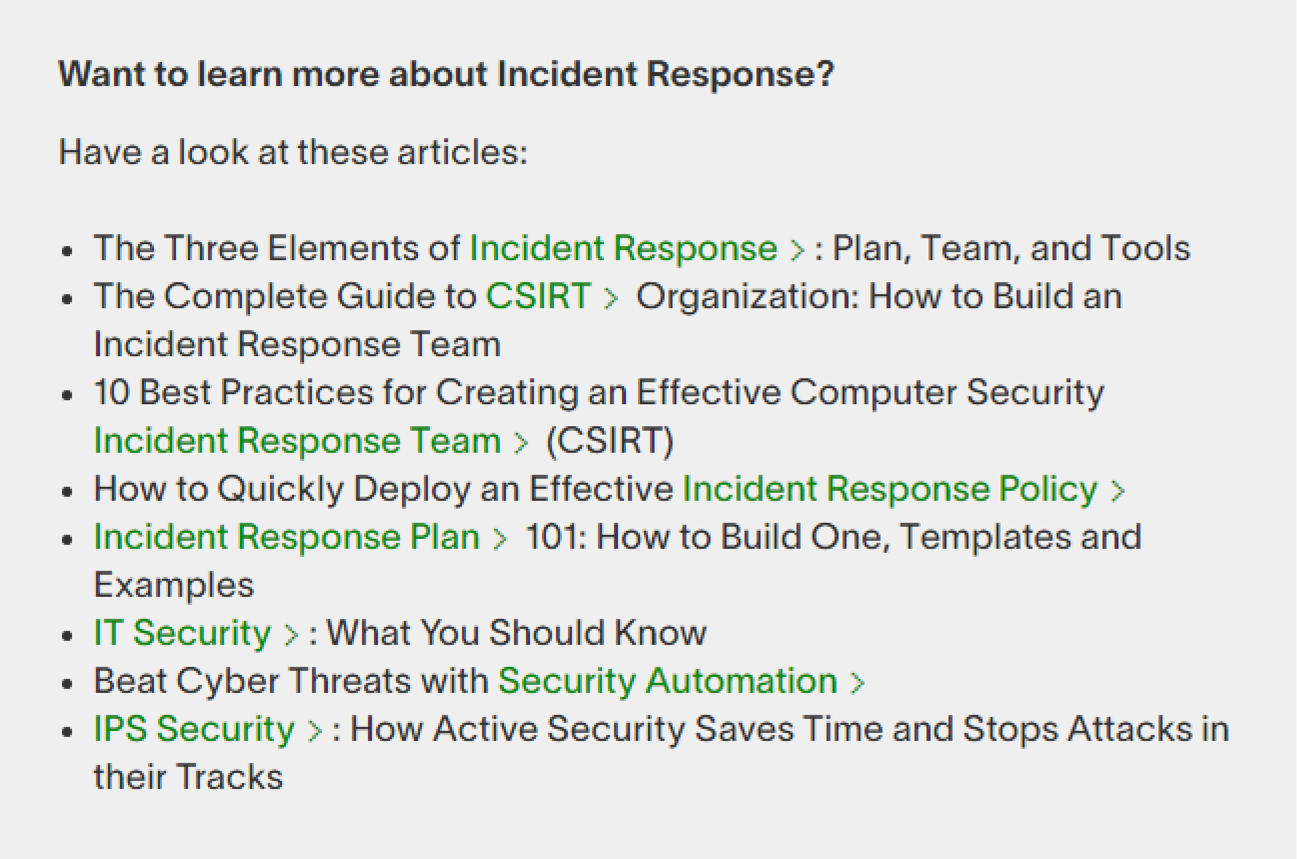
- **Step 1 :** Incident logging.
- **Step 2 :** Incident categorization.
- **Step 3 :** Incident prioritization.
- **Step 4 :** Incident assignment.
- **Step 5 :** Task creation and management.
- **Step 6 :** SLA management and escalation.
- **Step 7 :** Incident resolution.
- **Step 8 :** Incident closure.

Need for incident response

- To detect cyber security incident
- To eradicate incident
- To technically analyze incident.
- To recover from the incident.

steps for Incident Response



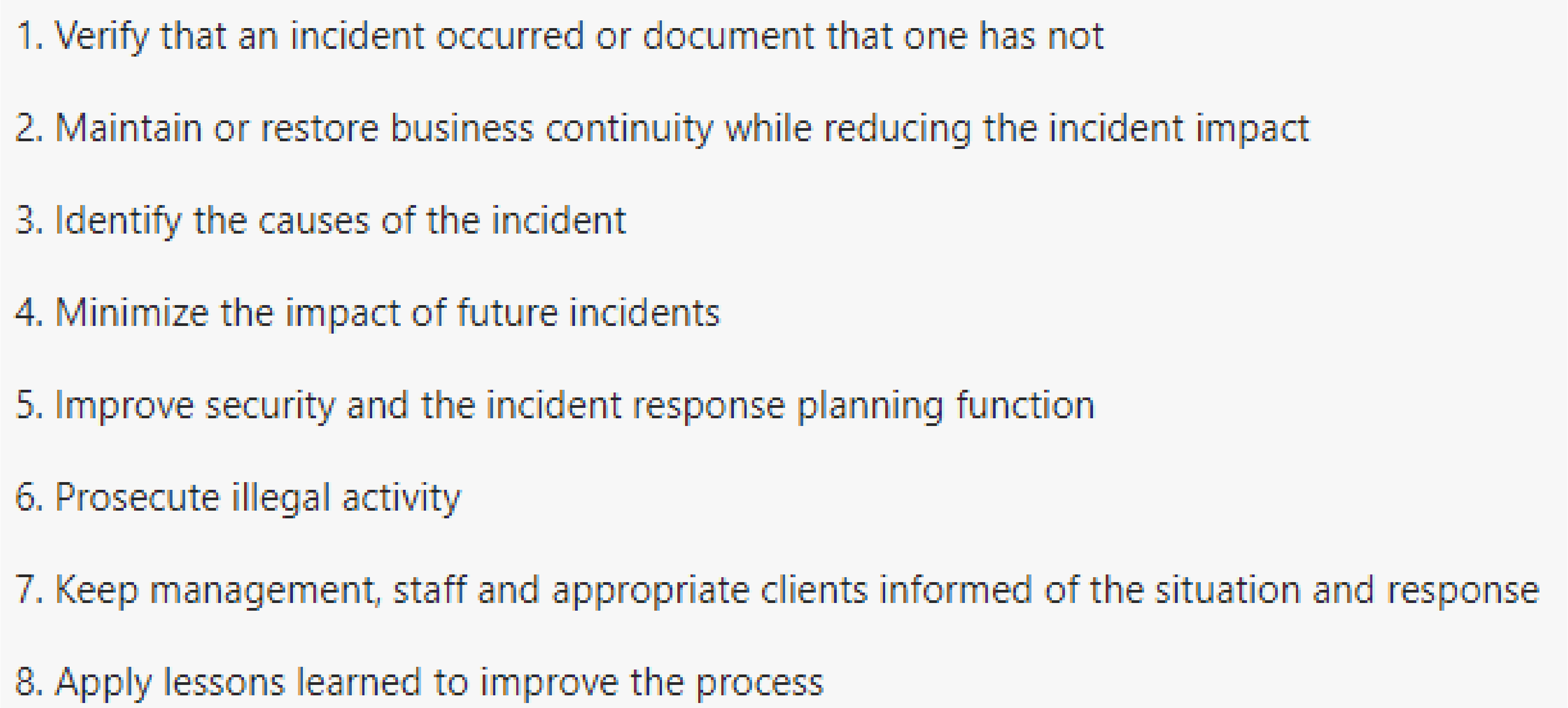


Want to learn more about Incident Response?

Have a look at these articles:

- The Three Elements of Incident Response › : Plan, Team, and Tools
- The Complete Guide to CSIRT › Organization: How to Build an Incident Response Team
- 10 Best Practices for Creating an Effective Computer Security Incident Response Team › (CSIRT)
- How to Quickly Deploy an Effective Incident Response Policy ›
- Incident Response Plan › 101: How to Build One, Templates and Examples
- IT Security › : What You Should Know
- Beat Cyber Threats with Security Automation ›
- IPS Security › : How Active Security Saves Time and Stops Attacks in their Tracks

Goals and Purpose of Incident Response



1. Verify that an incident occurred or document that one has not

2. Maintain or restore business continuity while reducing the incident impact

3. Identify the causes of the incident

4. Minimize the impact of future incidents

5. Improve security and the incident response planning function

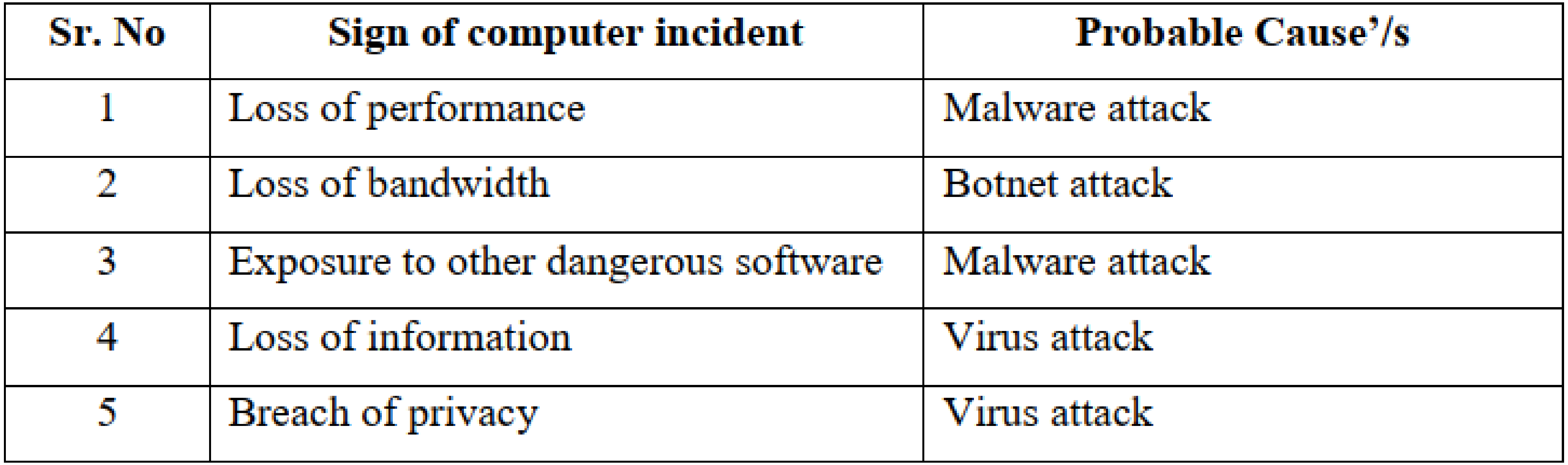
6. Prosecute illegal activity

7. Keep management, staff and appropriate clients informed of the situation and response

8. Apply lessons learned to improve the process

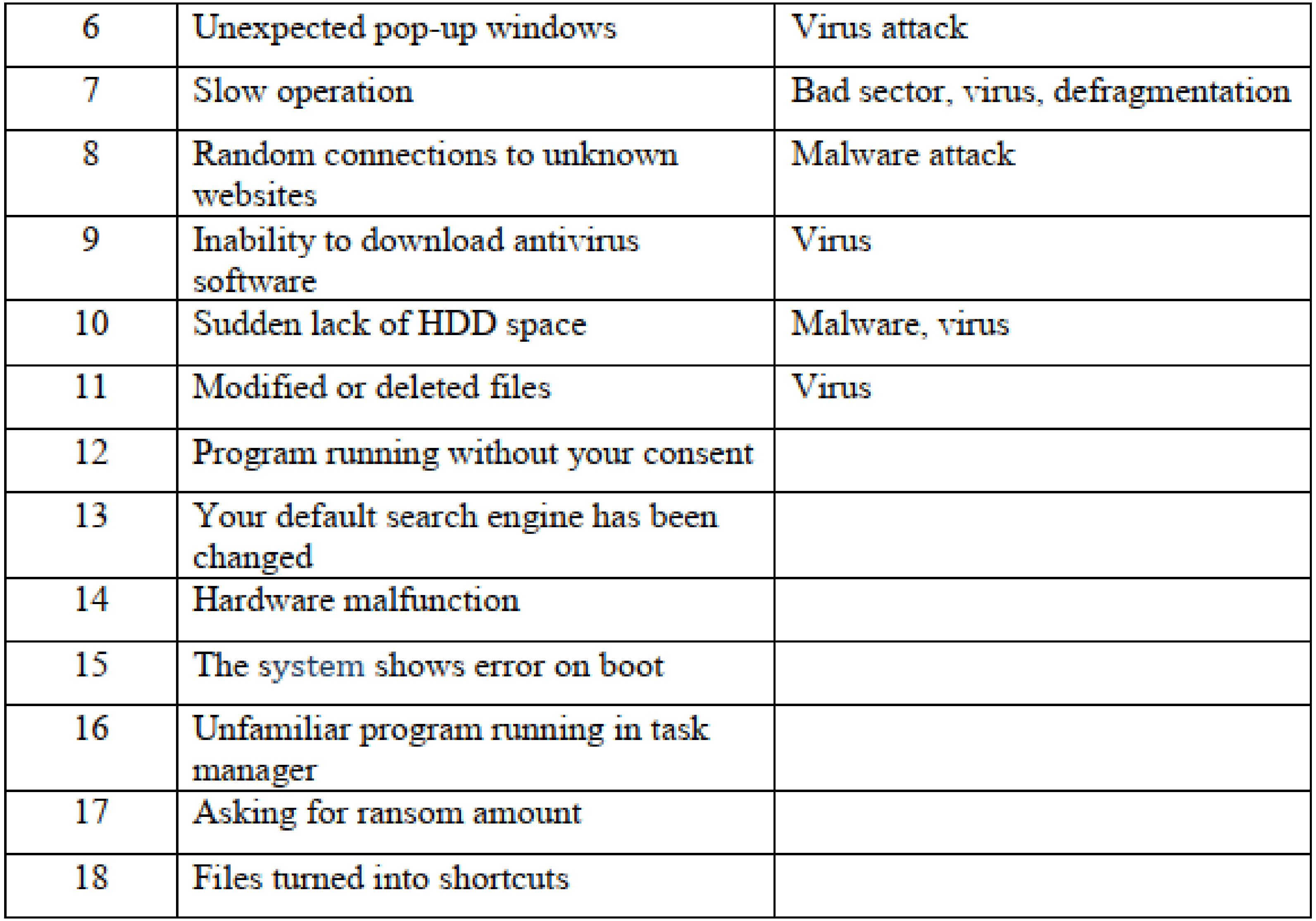
- The purpose of incident management is to return the service organization’s services to the user entities back to normal operations as quickly as possible, after an event, to minimize the impact of the event on the service organization’s achievement of its service commitments and system requirements.

Signs of computer incidents



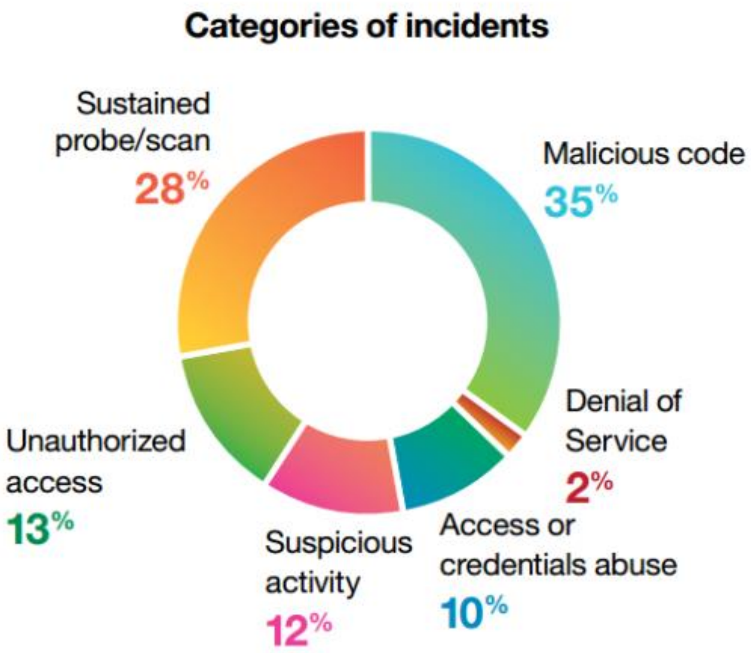
Sr. No	Sign of computer incident	Probable Cause'/s
1	Loss of performance	Malware attack
2	Loss of bandwidth	Botnet attack
3	Exposure to other dangerous software	Malware attack
4	Loss of information	Virus attack
5	Breach of privacy	Virus attack

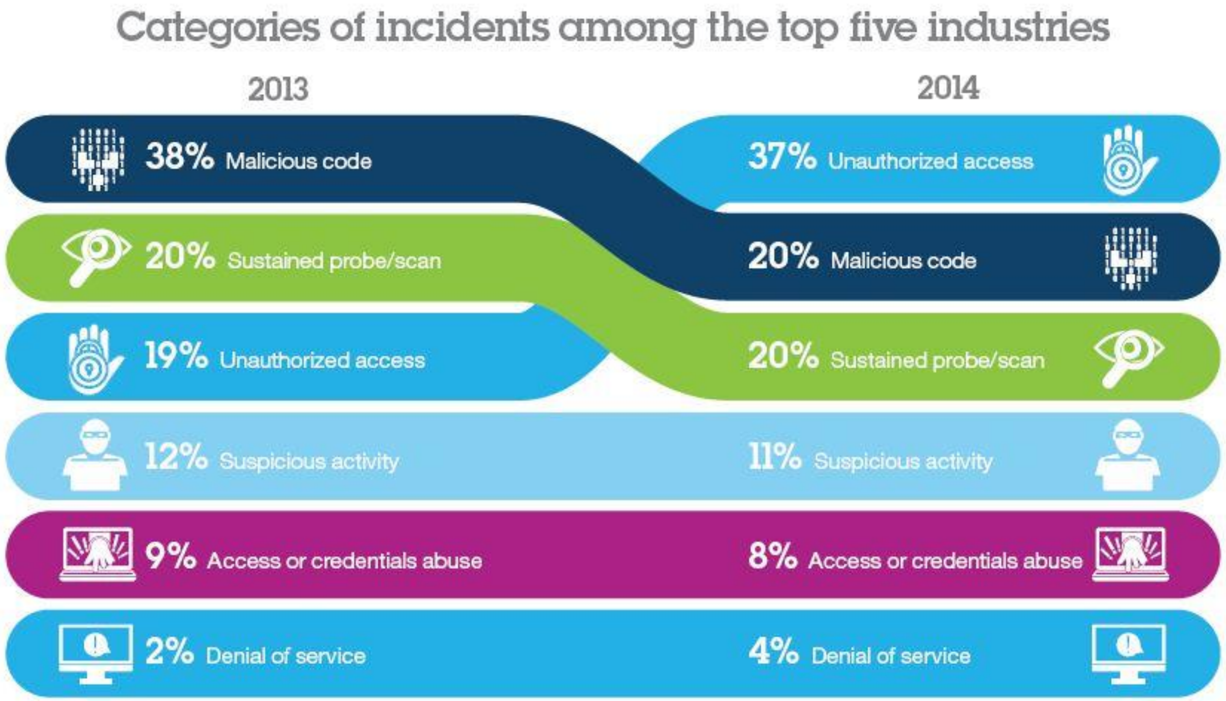
Signs of computer incidents



6	Unexpected pop-up windows	Virus attack
7	Slow operation	Bad sector, virus, defragmentation
8	Random connections to unknown websites	Malware attack
9	Inability to download antivirus software	Virus
10	Sudden lack of HDD space	Malware, virus
11	Modified or deleted files	Virus
12	Program running without your consent	
13	Your default search engine has been changed	
14	Hardware malfunction	
15	The system shows error on boot	
16	Unfamiliar program running in task manager	
17	Asking for ransom amount	
18	Files turned into shortcuts	

Incident categories


Categories of incidents
Sustained probe/scan
Malicious code
Denial of Service
Unauthorized access
Suspicious activity
Access or credentials abuse


Categories of incidents among the top five industries
38% Malicious code
20% Sustained probe/scan
19% Unauthorized access
12% Suspicious activity
9% Access or credentials abuse
2% Denial of service
37% Unauthorized access
20% Malicious code
20% Sustained probe/scan
11% Suspicious activity
8% Access or credentials abuse
4% Denial of service