

# CYBERSECURITY INTERMEDIATE TRAINING

RAYMOND BETT

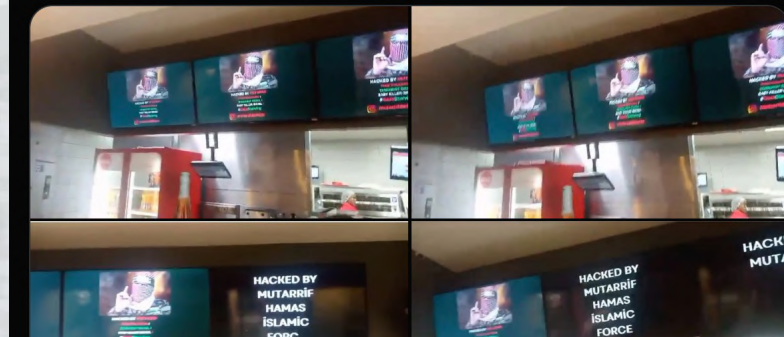
ISACA KENYA

20<sup>th</sup> – 24<sup>th</sup> May 2024

## Growing cyber threat landscape

	Jan-Mar 24	Oct-Dec 23	Variance %
Malware	33,187,524	13,221,698	151%
Brute Force Attacks (DDOS/Botnet)	66,658,474	9,670,849	589%
Web Application Attacks	199,435	72,536	175%
System Vulnerabilities	871,223,680	1,269,267,620	-31%
Mobile Application Attacks	171,232	52,705	225%
Total	971,440,345	1,292,285,408	-25%

### \*Communications Authority of Kenya



**Cybersecurity is concerned with protecting digital assets. Includes:**

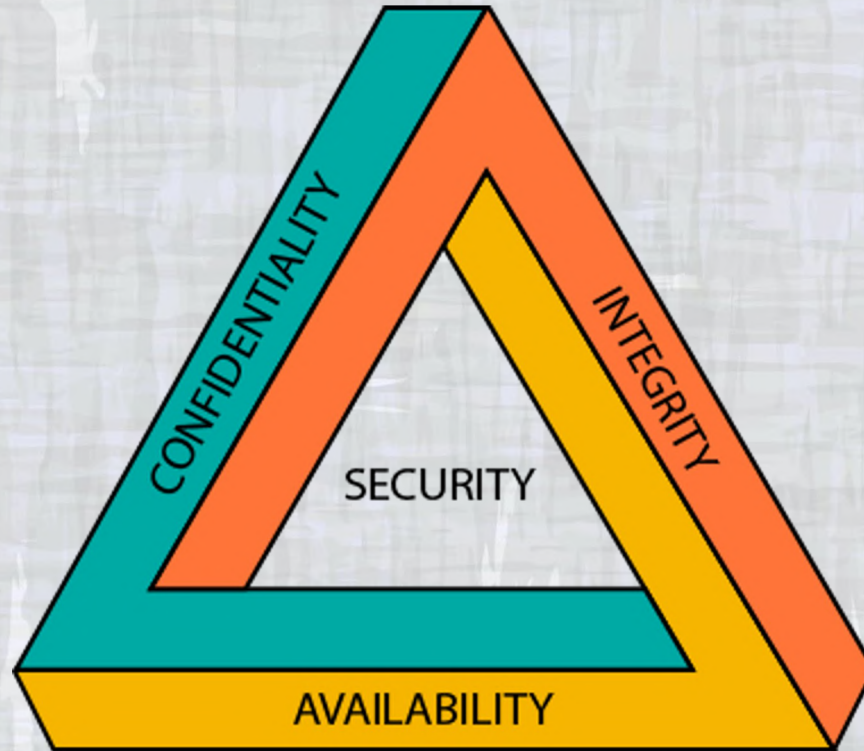
**Networks**

**Hardware**

**Software**

**Information that is processed, stored or transported by internetworked information systems**

## CIA TRIAD



## CONFIDENTIALITY

The protection of information from unauthorized disclosure

## INTEGRITY

The accuracy and completeness of information in accordance with business values and expectations

## AVAILABILITY

The ability to access information and resources required by the business process

## Global Concern



The growth of the Internet across the world – increased connectivity increases attack opportunities



Growing space for collaboration and increased sophistication of hackers



Weak legal international frameworks



Education and awareness lags cybersecurity developments

**The Computer Misuse and Cybercrime  
Act, 2018**

“provides for offences relating to computer systems to enable timely and effective detection, prohibition, prevention, response, investigation, and prosecution of computer and cybercrimes”

- **The Data Protection Act, 2019**

“to make provision for the regulation of the processing of personal data; to provide for the rights of data subjects and obligations of data controllers and processors; and for connected purposes”

# COMPUTER MISUSE AND CYBERCRIME ACT, 2018

Offense	Fine	Imprisonment term
Unauthorized access	5 Million	3 years
Unauthorized interference	10 Million	5 years
Unauthorized interception	10 Million	5 years
Illegal devices and access codes	20 Million	10 years
Unauthorised disclosure of password or access code	5 Million	3 years
Cyber espionage	10 Million	20 years
False publications (“fake News”)	5 Million	2 years
Child pornography	20 Million	25 years
Computer forgery	10 Million	5 years
Computer fraud	20 million	10 years
Cyberstalking, Cyber bullying	20 million	10 years
Cybersquatting	200,000	2 years

# THE DATA PROTECTION ACT

## DATA COMMISSIONER



Establishes the office of the data commissioner. Currently occupied by Immaculate Kassait

## Data Processors and Data Controllers



Provides for registration of Data Controllers and Data processors

## Principles of Data Protection



Provides the underlying principles of data protection



# THE DATA PROTECTION ACT

## Cross Border Transfer



Provides the guidelines for transfer of data outside Kenya

## Exemptions



Provides the basis of exemptions for complying with provisions of the Act

shutterstock.com · 1426079102



Provides the mechanism for enforcement of this provisions

# Application of the Data Protection Act

## Data Handler Role

An organization can both be a data controller as it determines the purpose and means of processing of personal data as well as a data processor as it processes personal data on behalf of other data controllers.



## Processing of Personal Data and Sensitive Data

The processing of the data itself, is restricted under the DPA to certain lawful bases and the collection limited to only what is necessary for the purpose justifying the collection. Companies will have to carefully consider the processing of children's data and financial data as it is classified as sensitive data.



## Incident response

In protecting personal data, there must be incident response to monitor any breach and at the same time this must be reported to the ODPIC within 72 hours after any breach is identified.

# Application of the Data Protection Act

## Third Parties

In engaging third parties, there must be clear contractual requirements in handling personal data and maintaining the lawful basis. You should consider any joint liability for mishandling of data privacy by third parties. In the financial sector such parties include fintech's, associations among others



## Marketing

In using personal data for digital marketing, you should consider it being clear opt in as well as in the message itself a clear opt out.



## Transfer of Data Outside Kenya

In transferring personal data outside Kenya including cloud computing, you should have the consent of the Client to transfer data outside Kenya or be assured of the data privacy and information security safeguards in the receiving countries.

# Application of the Data Protection Act

## Penalties for Non-Compliance

Infringement of the Act will attract a penalty of not more than KES 5 million or, not more than 1% of its annual turnover whichever is lower. Individuals will be liable to a fine not exceeding KES 3 million or to an imprisonment term not exceeding ten years, or to both.



## Privacy notices and consent

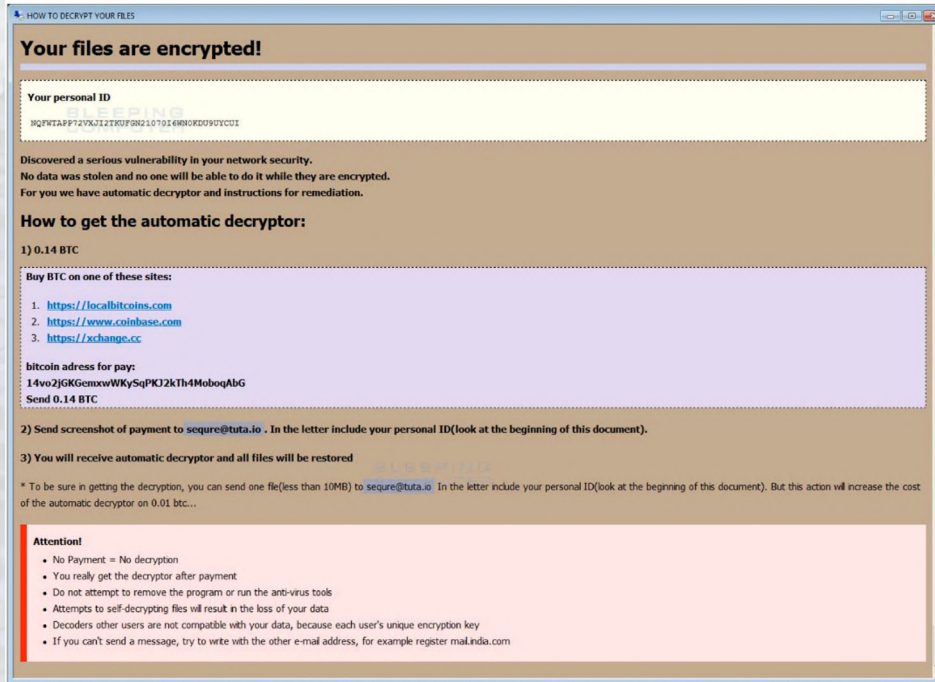
You should now consider carefully how they construct their public-facing privacy policies to provide more detailed information. In addition, the Data Protection Act will retain the notion of consent as one of the conditions for lawful processing, with organisations required to obtain 'freely given, specific, informed and unambiguous' consent, while being able to demonstrate these criteria have been met.



## Privacy by Design and By Default

Organisations need to build a mind set that has privacy at the forefront of the design, build and deployment of new Technologies (by design) and in their business-as-usual operations (by default). One demonstration of is **Data Protection Impact Assessments (DPIA)**, which is now required to be undertaken for new uses of personal data where the risk to individuals is high.

# Ransomware



Ransomware is a form of malicious software (or malware) that, once it's taken over your computer, threatens you with harm, usually by denying you access to your data. The attacker demands a ransom from the victim, promising – not always truthfully – to restore access to the data upon payment.

## How it is delivered

Most ransomware is delivered via email that appears to be legitimate, enticing you to click a link or download an attachment that delivers the malicious software.

Ransomware is also delivered via drive-by-download attacks on compromised or malicious websites.

Some ransomware attacks have even been sent using social media messaging.

# Major ways to Ransomware Protection

*Protect yourself with these quick tips so you don't pay!*



## **Back-Up Your Files**

Ransomware will look for files to encrypt or delete. Ensure all files are backed up to a secondary location like a secure cloud storage service or another storage media. This protection can make files inaccessible to edits or deletion by cybercriminals.



## **Keep Security Software Up to Date**

Security software that is not up to date is an easy target for cybercriminals that try to infiltrate systems. Updates for these types of software are generally done to protect against new cyber threats.



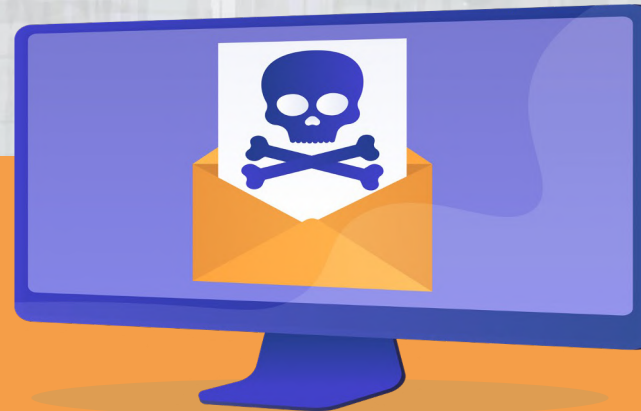
## **Never Pay the Ransom!**

Cybercriminals are always trying to deceive and take advantage of people. If you suspect you have fallen victim to a ransomware attack, make sure to disconnect any devices from your network and contact your organization's IT team immediately.



## **Only Use Secure Networks**

Cybercriminals look for persons connected to unsecured Wi-Fi networks to track their internet usage. Using a verified and secure network will assist in adding a layer of protection.



Social engineering is a deception method that takes advantage of human error to obtain sensitive data, access, or assets. These "human hacking" scams are common in cybercrime because they frequently persuade unwary individuals to expose data, spread malware infections, or grant access to restricted systems. Online, offline, and other encounters can all result in attacks.

Social engineering accounts for 98% of cyber-attacks.

Social engineering is characterized by attackers coercing victims into divulging sensitive information by pretending to be a known person or legitimate entity.

Identity theft through phishing attacks is the most common form of social engineering. Over 70% of data breaches start with phishing or social engineering attacks.



The attack cycle gives these criminals a reliable process for deceiving you. Steps for the social engineering attack cycle are usually as follows:

- **Prepare** by gathering background information on you or a larger group you are a part of.
- **Infiltrate** by establishing a relationship or initiating an interaction, started by building trust.
- **Exploit** the victim once trust and a weakness are established to advance the attack.
- **Disengage** once the user has taken the desired action.



## Phishing Attacks

Attacks using phishing are targeted in one of two ways:

**Spam phishing**, or **mass phishing**, is a widespread attack aimed at many users. These attacks are non-personalized and try to catch any unsuspecting person.

**Spear phishing** and by extension, **whaling**, is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons.

This is achieved by acquiring personal details on the victim such as their friends, hometown, employer, locations they frequent, and what they have recently bought online.

Whaling attacks specifically aim at high-value targets like celebrities, upper management, and high government officials.

Methods used in phishing each have unique modes of delivery, including but not limited to:

**Voice phishing (vishing)** phone calls may be automated message systems recording all your inputs. Sometimes, a live person might speak with you to increase trust and urgency.

**SMS phishing (smishing)** texts or mobile app messages might include a web link or a prompt to follow-up via a fraudulent email or phone number.

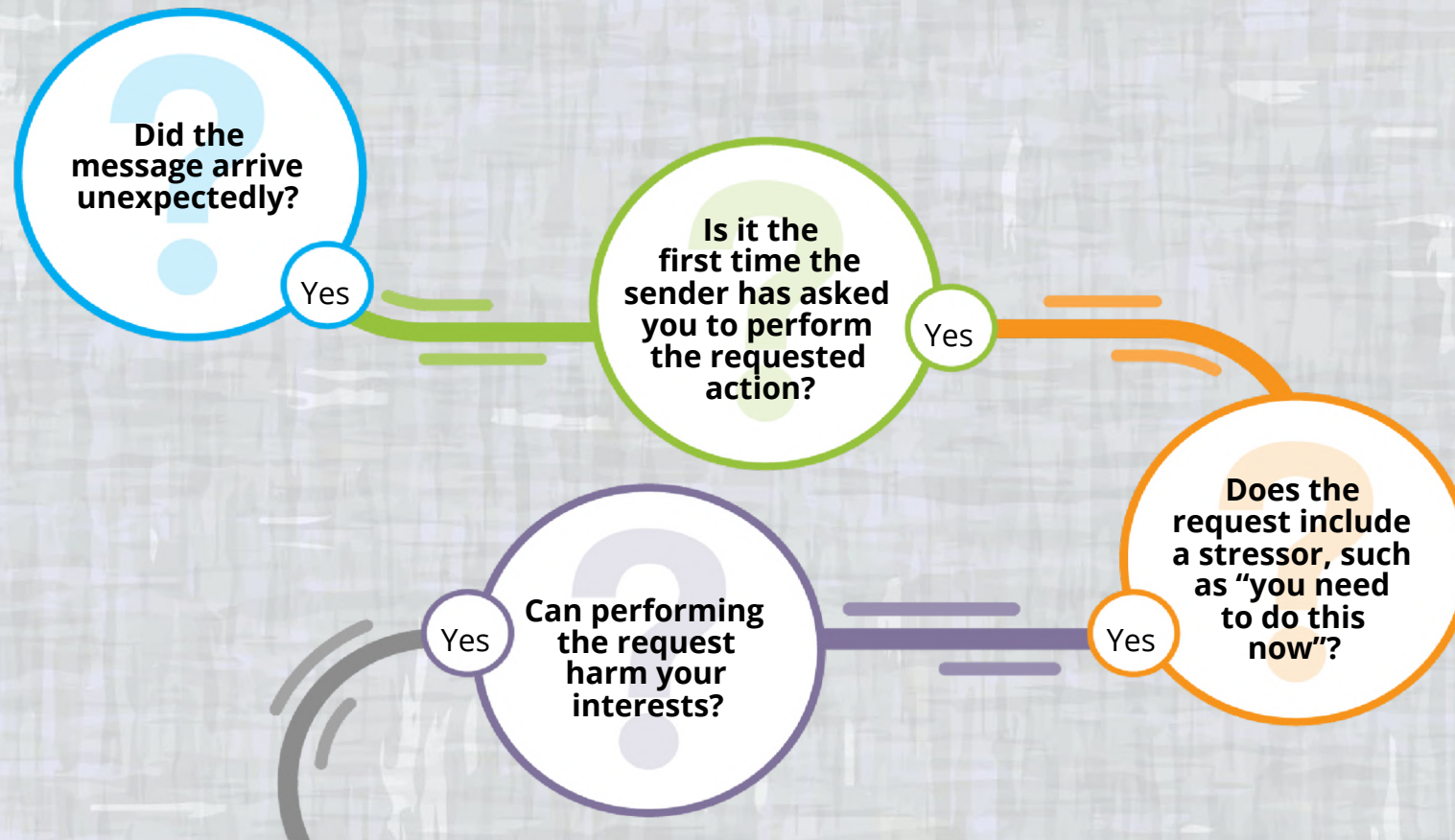
**Email phishing** is the most traditional means of phishing, using an email urging you to reply or follow-up by other means. Web links, phone numbers, or malware attachments can be used.

**Angler phishing** takes place on social media, where an attacker imitates a trusted company's customer service team. They intercept your communications with a brand to hijack and divert your conversation into private messages, where they then advance the attack.

**Search engine** phishing attempt to place links to fake websites at the top of search results. These may be paid ads or use legitimate optimization methods to manipulate search rankings.

- Banks and other financial institutions, etc. will NOT ask for your account details by email; your IT department will NOT ask you to confirm your password over the phone;
- Avoid being too open on social media. It's no harm keeping your friends updated but just consider whether your posts could be used against you. Do not share names of your schools, pets, place of birth, or other personal details. You could be unknowingly exposing answers to your security questions or parts of your password.
- Positioning the mouse over the link – without clicking on it – allows you to examine the URL for anything suspicious.
- Never use your official business account details – particularly your password – when registering with non-work related on-line services or companies.
- Multi-factor Authentication- One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account's protection in the event of

## Questions to ask to avoid being a victim of social engineering attack

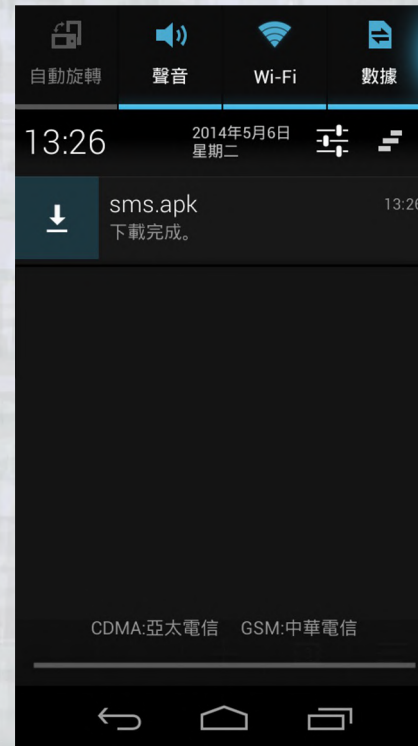


If you answer yes to all of them, you should go out of your way to confirm the request is legitimate. Use a trusted method like calling or texting the sender before taking any action.

## TRENDS

### Mobile Malware (example: Pegasus spyware)

Mobile malware is malicious software specifically written to attack mobile devices such as smartphones, tablets, and smartwatches.



# How mobile malware infects users

**Permissions abuse:** Different forms of malware (often adware) can get on mobile devices when applications ask for more permissions than what are needed and users grant those permissions.

**Jailbroken phones:** Though it is possible that malware can find its way into the official Google and Apple mobile app stores, it isn't common. The vast majority of malware and malware-integrated apps are found in third-party app stores.

**Attacking known vulnerabilities:** This is perhaps the most obvious form of attack, when attackers simply go after known issues.

# What are Signs of malware attack on your phone?

- Device begins to operate slowly.
- Your battery drains more rapidly than usual
- Spikes in data usage.
- Strange charges/usage of airtime.



## Mitigation

- Update your operating system
- Do not jailbreak or root your device
- Only download apps from the official app stores
- Review your access permissions
- Encrypt your device.
- Be wary of public WiFi hotspots -Do not access any sensitive information through public WiFi, such as logging into your bank or checking sensitive work emails, as a hacker may be able to intercept your communication through a "man-in-the-middle" attack. It is far more secure to use a 3G or 4G instead, or to use a VPN.

## Insider Threat

- 60% of cyberattacks come from inside the company.
- Financial firms and financial services are in the top three sectors targeted by insider attacks mostly by disgruntled employees to poorly-compensated bank tellers.
- 75% of internal attacks are intentional.
- Employees can offer up their credentials to a hacker, or simply decline to seriously review cyber security concerns due to poor morale making the employee one of the top cyber security threats to financial services.
- The remaining 25% of internal attacks are due to human error.

## Insider Threat Mitigation



Protect what is most valuable, tighten access controls.



Ensure your employees are satisfied and feel valued for their contributions. A strong organization that protects and rewards employees means your first layer of defense – the people you employ – are ready to make sure institutional assets are safe.



System and transaction monitoring for anomalous activities.

## TRENDS

### Back-door and Supply Chain Attacks



A supply chain attack, also called a value-chain or third-party attack, occurs when someone infiltrates your system through an outside partner or provider with access to your systems and data.

## TRENDS

# Back-door and Supply Chain Attacks

Targeted attacks often use “backdoors” – applications used to obtain remote access.

By using backdoors, hackers gain access to the network while bypassing the corporate security systems.

The screenshot shows the top of a Financial Times article. At the top, the 'FINANCIAL TIMES' logo is centered. Below it is a navigation bar with links for 'US', 'COMPANIES', 'TECH', 'MARKETS', 'CLIMATE', 'OPINION', 'WORK & CAREERS', 'LIFE & ARTS', and 'HOW TO SPEND IT'. A dark banner contains the text: 'We believe in capitalism. But the model is under strain. We need to reform in order to preserve. If you think the same, join us.' with a 'Join us now' button. Below the banner, the article title 'African Union' is visible. Three small article teasers are shown: 'Africa celebrates suspension of Covid vaccine patents', 'African Union halts AstraZeneca vaccine purchases over supply concerns', and 'Africa will pay more for Russian Covid vaccine than 'western' jobs'. The main article title is 'Africa + Add to myFT African Union accuses China of hacking headquarters'. Below the title is the sub-headline 'Beijing funded the AU's \$200m building in Addis Ababa'. A large photograph shows the African Union headquarters building in Addis Ababa, featuring a row of flags on tall poles in the foreground and a modern, curved building structure. At the bottom of the image, a caption reads: 'Analysts said the Addis Ababa hack was 'really alarming', partly because it exposed that 'African countries have no leverage over China' © Getty'.

## TRENDS

# Back-door and Supply Chain Attacks Mitigation

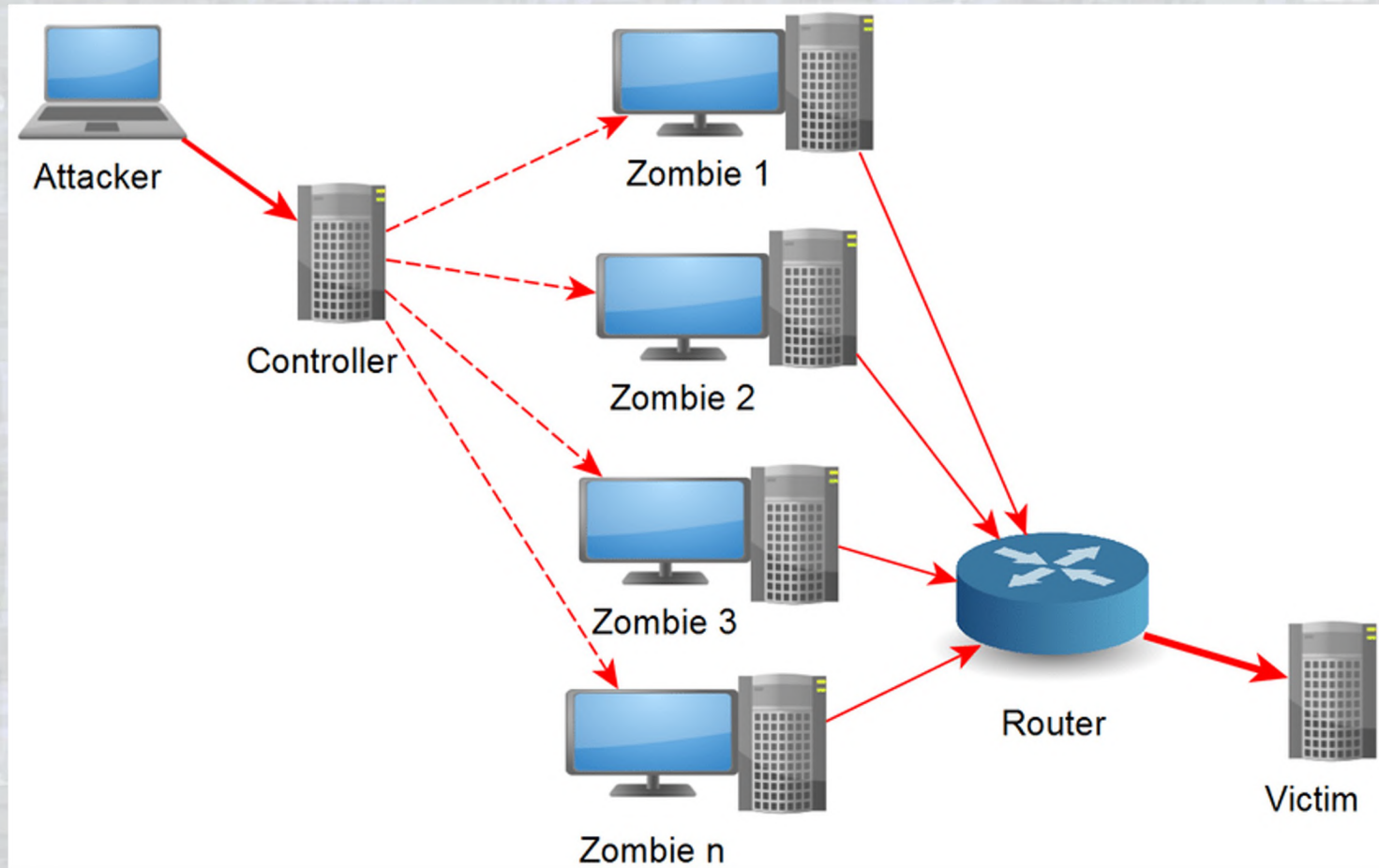
System, Network auditing and monitoring are the surest ways to detect supply-chain attacks.

Vendors may be asked to do self-assessments, allow customer visits and audits.

An agreement from the provider showing their commitment to security including their partners.

Companies should review how third parties access their confidential data to make sure that only the right people can access the data for only approved purposes.

# Denial of Service (DoS) Attack



## TRENDS

# Denial of Service (DoS) Attack Mitigation

1

Keep your security software, operating system, and applications updated.

2

Build redundancy into your infrastructure

3

Buy more bandwidth

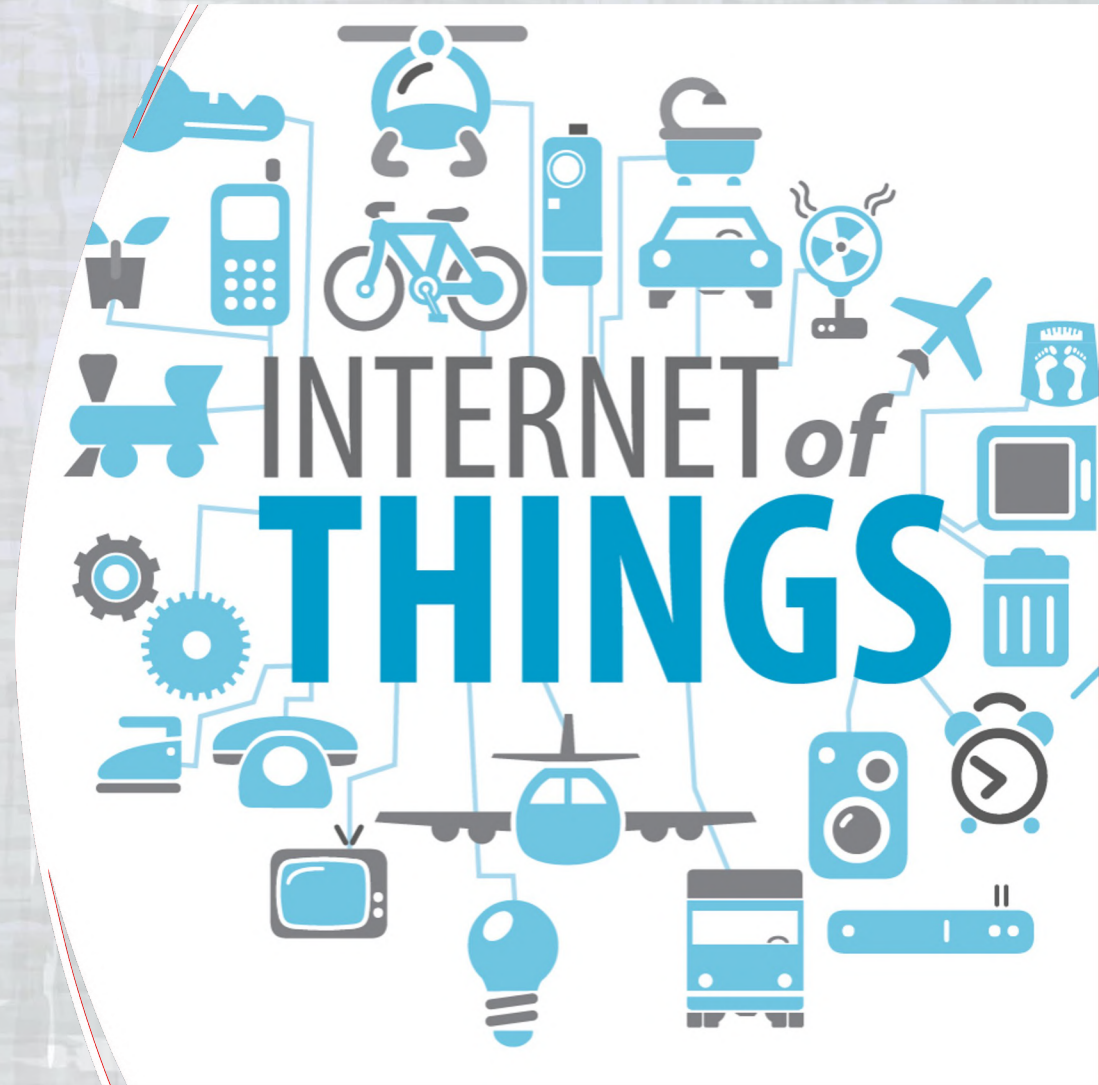
4

Deploy anti-DDoS hardware and software modules



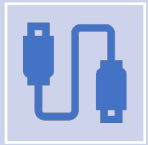
## Internet of Things

“scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention”





## Internet of Things Mitigation



Keep tabs on mobile devices-  
Make sure mobile devices like tablets are checked in and locked up at the end of every business day.



Keep software updated  
including automatic antivirus  
update.



Require strong login  
credentials



Deploy end-to-end  
encryption

## Our imagination of a cybercriminal



Or This



# ■ The Unusual Suspects

Cyber threats, methods and motivations



- They're too young to go to jail – and know that, even if they're caught, they'll get away with little more than a slap on the wrist for their actions.
- Often blessed with merely basic hacking skills, the script kiddie is curious, keen to learn, and also keen to impress peers or more senior cybercriminals. They may not understand the consequences or illegality of their actions.

## Script Kiddie



- Whatever their cause, it's a burning one – and the Activist takes their political, religious or social cause outside the rule of law and on to the Internet. The Activist targets adversaries with data theft, reputational damage and the defacement of web sites and social media accounts  
E.g. WikiLeaks, local bloggers

**Hacktivist**





- They work at what looks like a legitimate '8 to 5' job – but it's anything other than law abiding. The Professional has built a career out of committing or supporting cyber crime. They target customers of financial institution through social engineering.

**Professional**



- They may only be 20% of the threat, but they produce 60% of the damage. These attackers are considered to be the highest risk. To make matters worse, as the name suggests, they often reside within an organization either current employees, former employees, employees of related organizations etc. The threat comes in because they know how the company operates, which are the weak points and so on.

## Insiders



- This group is responsible for highly targeted attacks carried out by extremely organized state-sponsored groups. Their technical skills are deep and they have access to vast computing resources. The US election was influenced by Russians who favoured a certain candidate and this was done by hacking the Democratic party systems

## Nation State Actor



# Footprinting

## Definition

- Footprinting also known as reconnaissance is the act of gathering information about a target's computer system
- An attacker would carry out footprinting to gather information to create a profile of the target

## Active vs. Passive Footprinting

- Active footprinting involves gathering information by interacting with the target. This include visiting the client premises, scanning their ports, carrying out Domain Name Service (DNS) enumeration etc.
- Passive footprinting is a technique that involves gathering information about the target without interacting with the target. The attacker would gather information using publicly available sources such as; search engines, social networking sites, websites, email search etc.

## Threats posed by footprinting

- Information gathered through footprinting can be used to **social engineer** the target. An example is where an attacker sends an email to the targets employees with phishing links.
- The target can suffer from **information leakage** on their website when sensitive information is inadvertently shared with the public.
- Footprinting is usually the first phase of penetration testing and as such will be used to launch attacks on the network that can lead to **financial losses, lawsuits, reputational damage** among others.

# Information Gathering on the web

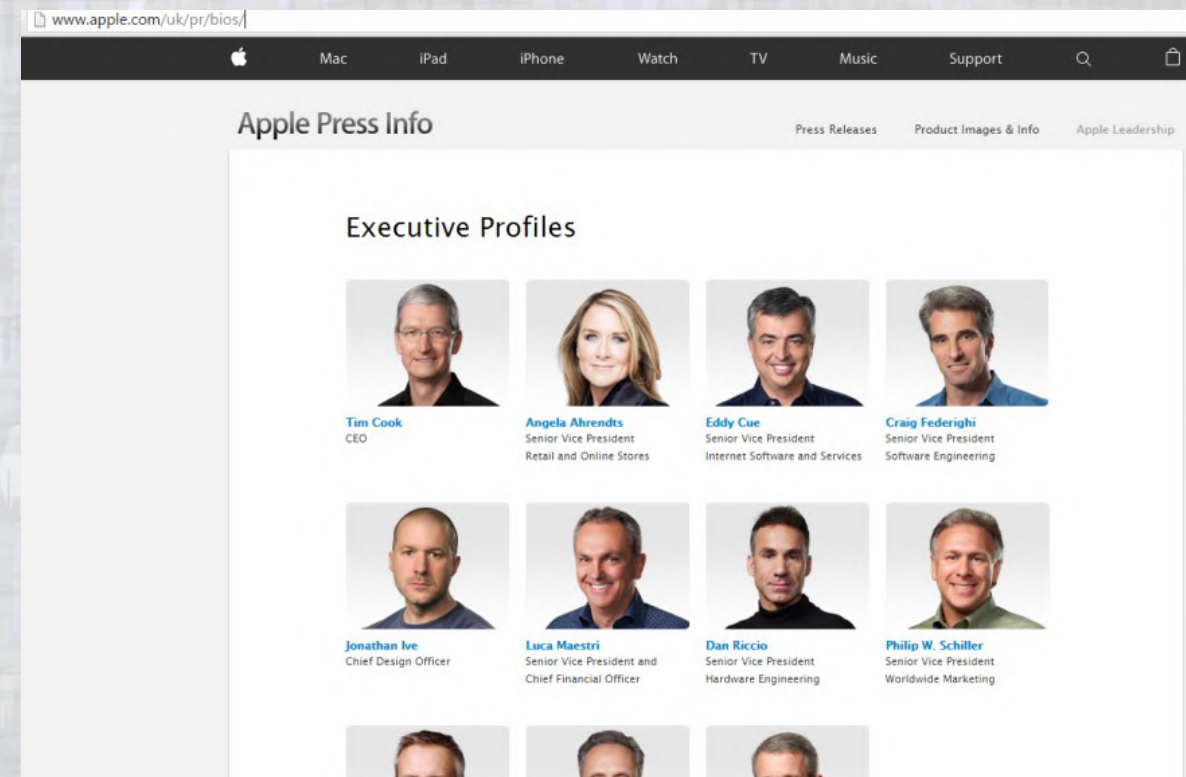
## Company website

- Searching on the internet about the target company or individual will reveal information about the
  - Company size
  - Senior leadership team
  - Directories and subdomains
  - Products and services
  - Operating system in place

## Pentesting tools

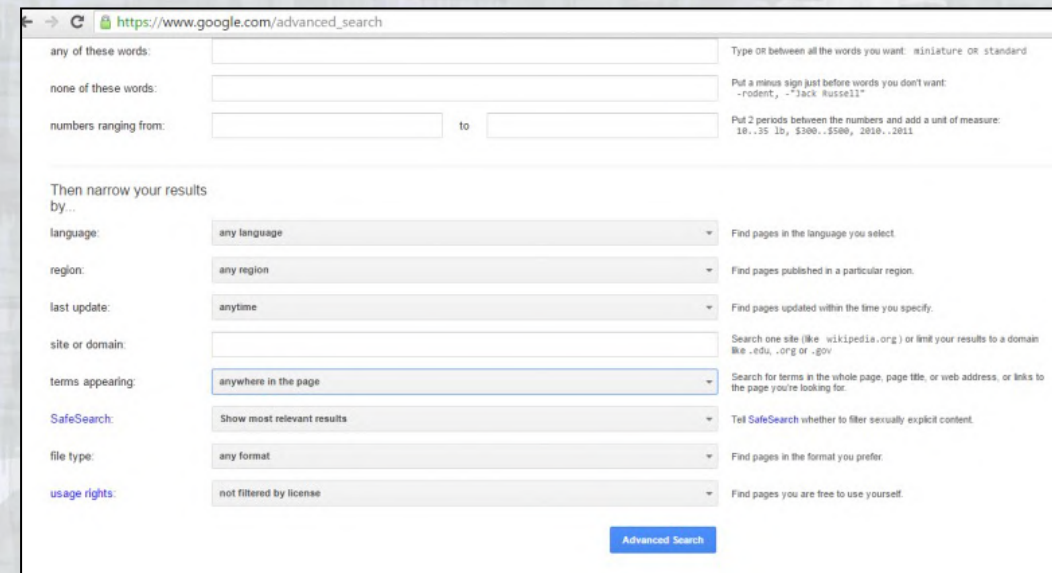
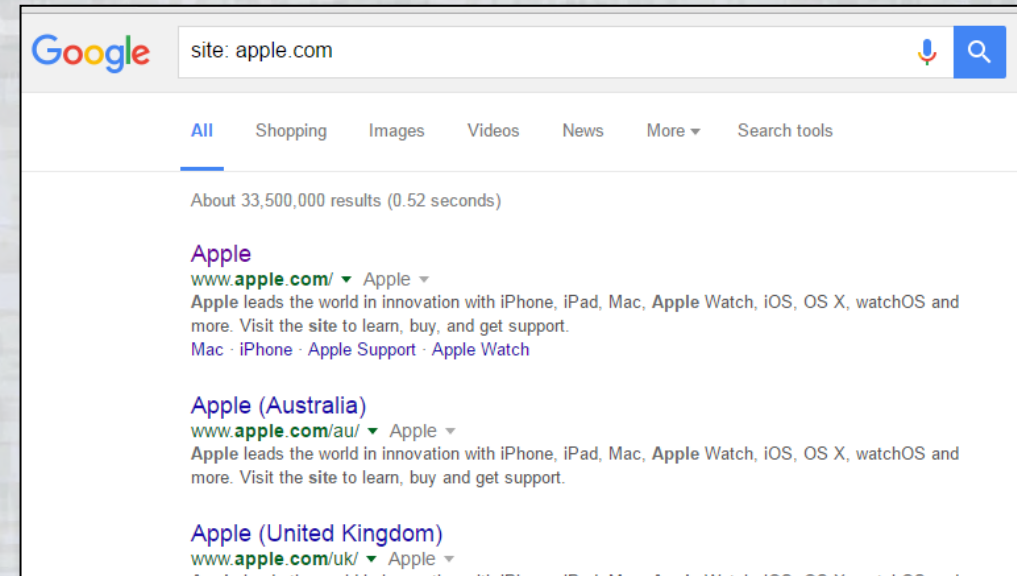
- Tools that can be used to gather information on a company's website include:
  - HTTRACK to copy entire website for offline analysis
  - Firebug used in editing, a website HTML and JavaScript code
  - Web Data Extractor for data extraction on a given website

## Apple's website which shows the senior leadership team



# Google Search

- There are various search parameter that can be used on Google to collect information about the target.
- **Site:** parameter can be used to narrow search results to a particular domain. For example using this search parameter on apple.com, we can get the results for various website that Apple maintains across various countries. One can also quickly see the format that Apple uses which is to add the country's top level domain after **apple.com** such as **apple.com/uk** , **apple.com/au**, **apple.com/in** etc.
- Google advanced search also provides a means to customize search results to be in a particular



# Google hacking

- Google search engine can be used to refine searches by using advanced operators
- Google hacking is a means of using Google advanced search operators to find vulnerabilities, log files and misconfigurations on the internet.
- Google hacking database is a collection of search terms that can be used to find vulnerabilities on the internet. It is maintained by offensive security.
- Many of the advanced searches are listed on Google hacking database which can be found on the exploit database website.
- Google hacking methods have since been extended to other search engines such as Bing, Yahoo and so on.

## Google advanced search operators

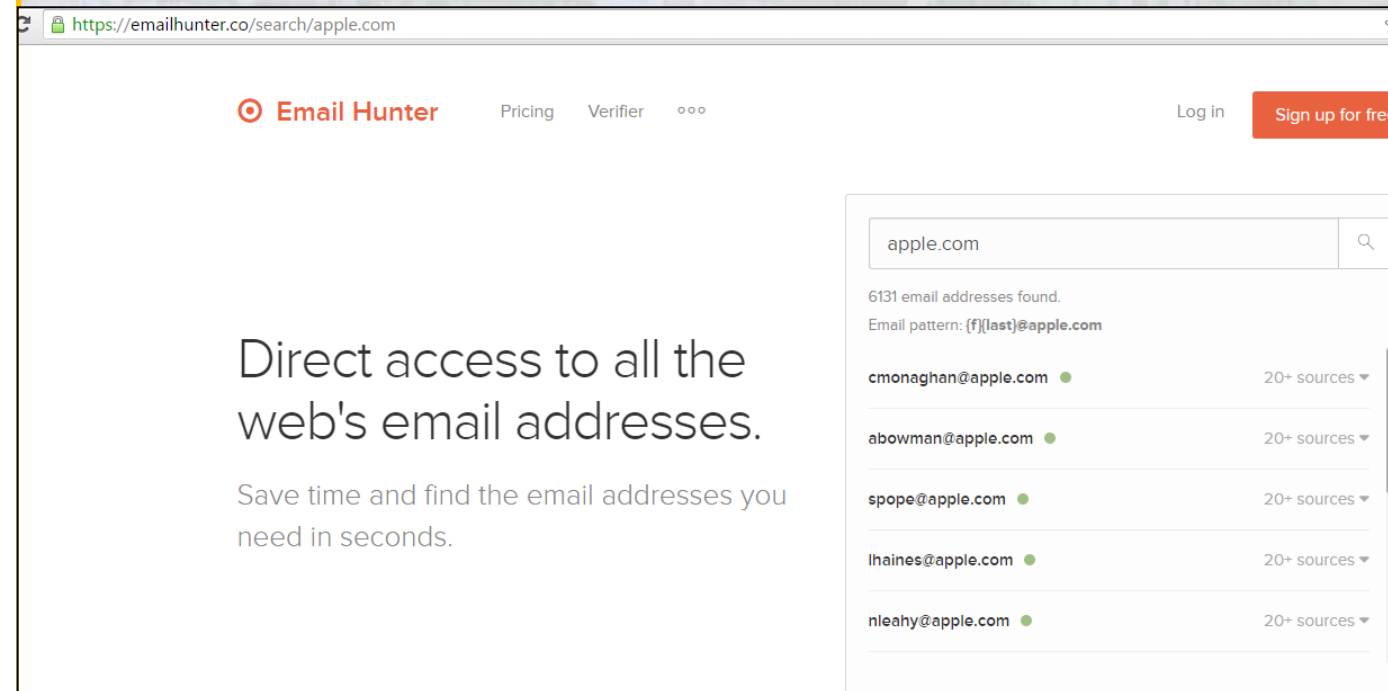
Operator	Purpose	Example
<b>allinanchor</b>	Restricts results to pages with links specified.	<u>allinanchor:apple.com</u> will give you all links to Apple.com site
<b>intitle</b>	Search term in the title	<u>Intitle:apple.com</u> search for all pages with the title apple.com
<b>inurl</b>	Search for pages where the URL contains the search term	<u>Inurl: apple.com</u> will return all sites with URL name containing apple.com
<b>filetype</b>	specific files	<u>Apple filetype:pdf</u> will return all pdf files with the specified files
<b>intext</b>	Search for text within a page	<u>intext: apple.com</u> will give all pages with the text containing apple.com.
<b>site</b>	Search terms in a given domain	<u>Site: apple.com</u> will return sites within apple.com website
<b>link</b>	Search for links to pages	<u>Link:apple.com</u> will return pages that link to applecom site.
<b>inanchor</b>	Restricts results to pages with links specified.	<u>inanchor:apple.com</u> will give you all links to Apple.com site

# Email harvesting

- Harvesting emails on the internet is an important part of information gathering.
- Gathering the emails will enable the penetration tester target it's victim more precisely.
- In most organizations the first part of an email are used as usernames for various applications.
- Mails also provide the naming convention of users within the organization.
- There are online tools that can scrape emails from the company website, social media platforms and so on.
- Emails can also be traced to the company's geographical location.

## Tools

- Email Hunter – Online tool to search for sites
- Theharvester – a linux tool that can search for emails for a specific target on a search engine



The screenshot shows the Email Hunter website interface. The URL in the browser is <https://emailhunter.co/search/apple.com>. The page features the Email Hunter logo, navigation links for Pricing, Verifier, and a menu icon, along with Log in and Sign up for free buttons. A search bar contains the text 'apple.com'. Below the search bar, it states '6131 email addresses found.' and 'Email pattern: {f}[last}@apple.com'. A list of email addresses is displayed, each with a green dot indicating a match and a dropdown arrow showing '20+ sources'. The visible email addresses are: cmonaghan@apple.com, abowman@apple.com, spope@apple.com, lhaines@apple.com, and neahy@apple.com.

File Edit View Search Terminal Help

```
root@kali:~# theharvester -d apple.com -b google >google.txt
```



ISACA

communication



# Labs

---

SQL Lab

Scanning Ports and Utilizing SSH

site:ke filetype.doc confidential

site:ke password filetype.txt

**CYBERSECURITY AND EMERGING TECHNOLOGIES**

# EMERGING TECHNOLOGY



Mobile Devices



# Emerging Technologies



Mobile Computing

Social Media

Cloud Computing

Consumerization of IT

Blockchain

Big Data and Analytics

# Mobile payments ecosystem

## Mobile Network Operators

- Telcom operators, who can provide actual mobile payments or can just provide network service. e.g. Airtel, Safaricom etc.

## Banks, MFIs Saccos

- The core of the mobile payment space and sometimes can provide mobile payment services e.g. Equitel, Pesalink

## Merchants

- Accept payments through mobile channels, e.g. restaurant, supermarkets etc.

## Agents

- Increases the coverage of mobile payments by accepting cash deposits and withdrawals

# Modes of mobile payment

## SIM toolkit

- Carried out through the SIM card

## USSD

- **USSD** (Unstructured Supplementary Service Data) is a Global System for Mobile(GSM) communication technology that is used to send text between a mobile phone and an application program in the network. E.g \*270#

## Apps

- Mobile application that work on smartphones and can be used for mobile payments
- Increased usage of apps such as Whatsapp banking

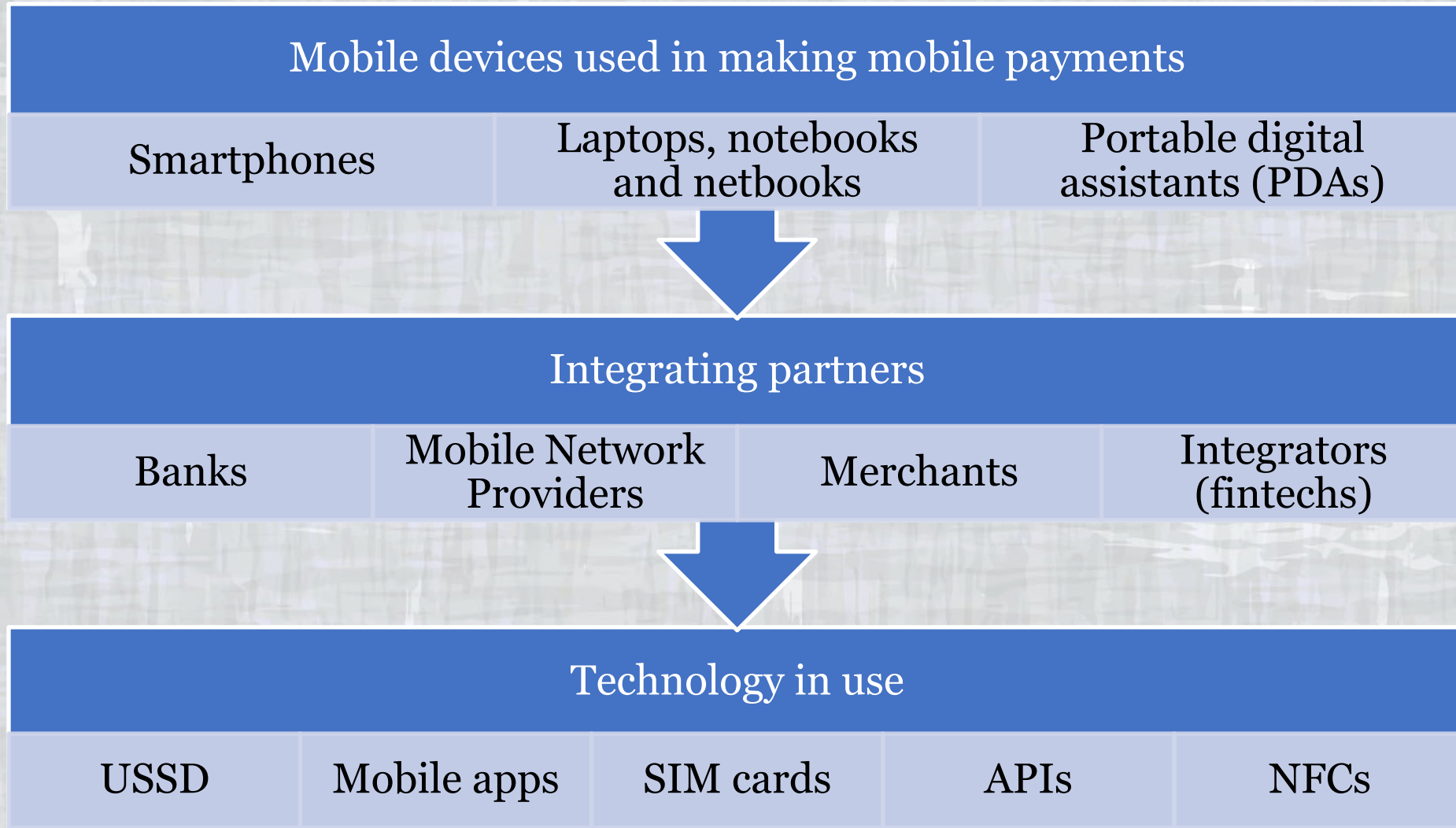
## APIs

- Application Programming Interface (API) that provide a link between the various mobile payment applications.

## NFC

- Near-field communication (NFC) is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 cm (1.6 in) of each other.

# Mobile payment risk profile



# Social Media

“Social media” is defined as using Internet-based applications or broadcast capabilities to disseminate and/or collaborate on information. This is different than traditional advertising and marketing channels due to the populist nature of social media, in which anyone with an Internet-attached device can, with near anonymity and without accountability, participate in public or private information or disinformation sharing, depending on access privileges to a social media web site.

Current social media tools include:

- Blogs (e.g., WordPress, Drupal™, TypePad®)
- Microblogs (e.g., Twitter, Tumblr)
- Instant messaging (e.g, Whatsapp, Microsoft® Windows Live Messenger)
- Online communication systems (e.g., Skype™)
- Image and video sharing sites (e.g., Flickr®, YouTube)
- Social networking sites (e.g., Facebook, Instagram, Tiktok)
- Professional networking sites (e.g., LinkedIn, Plaxo)



# Social Media Use

Enterprises are discovering numerous uses for social media, including:

- Increasing brand recognition
- Increasing sales
- Immediately connecting with perspective customers
- Exploring new advertising channels
- Monitoring competition
- Researching perspective employees

Social media do have a dark side. Social media sites can be used by dissatisfied customers, employees or individuals with a grudge against an enterprise to disseminate misinformation and negative information.

# Social Media Use

Policies for social media should address the following specific areas:

- Communication protocol
- Standardized terms/key words that may convey the company brand, product, image, campaign, business initiative, corporate social responsibility
- Use of standard logos, images, pictures, etc.
- Employee personal use of social media in the workplace
- Employee personal use of social media outside the workplace
- Employee use of social media for business purposes (personally owned devices)
- Use of mobile devices to access social media
- Required review, monitoring and follow-up processes for brand protection
- Communication of policy via social media sites
- Notification that compliance monitoring will be the right of the company
- Management procedures for company accounts on social media sites

# Social Media Training and Awareness

Training awareness program should address:

- Business social media activities using enterprise-owned equipment
- Business social media activities using personally or third-party owned equipment
- Personal social media activities using enterprise-owned equipment
- Personal social media activities using personally or third-party owned equipment during business hours
- Personal social media activities discussing enterprise activities using personally or third-party owned equipment outside business hours
- Alignment of both business and social media activities with the data classification scheme

# Social Media Training and Awareness

## **Social Media Alignment With Business Processes**

- Processes exist to manage new and existing social media programs to adhere to enterprise strategy, governance and management objectives and policies.

## **Social Media Brand Protection**

- The enterprise brand is protected from negative publicity or adverse reputational issues.

## **Social Media Monitoring**

- Social media sites are monitored for adverse posts, publicity, etc.

## **Social Media Branding Enforcement**

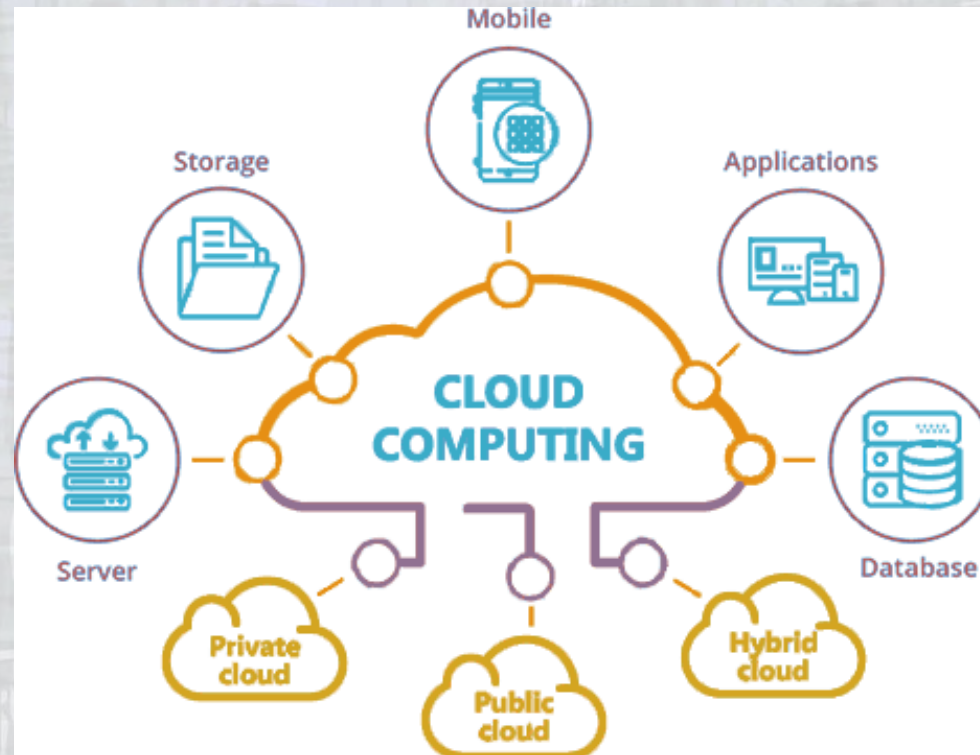
- Management actively litigates brand infringement.

## **Access Management of Social Media Data**

- Enterprise information is protected from unauthorized access or leakage through/by social media.

# Cloud Computing

Cloud computing has the advantage of lower IT costs, less complex infrastructure, better flexibility and increased operating efficiencies



# Cloud Computing Service Models

Service Model	Definition	To be considered
Infrastructure as a Service (IaaS) e.g Safaricom Cloud, Liquid Telecom	Capability to provision processing, storage, networks and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include operating systems and applications. IaaS puts these IT operations into the hands of a third party	Options to minimize the impact if the cloud provider has a service interruption
Platform as a Service (PaaS) e.g Amazon Web services	Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider	Availability Confidentiality Privacy and legal liability in the event of a security breach (as databases housing sensitive information will now be hosted offsite) Data ownership Concerns around e-discovery

# Cloud Computing Service Models

Service Model	Definition	To be considered
Software as a Service (SaaS) e.g. Microsoft 365	Capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).	<ul style="list-style-type: none"><li>• Who owns the applications?</li><li>• Where do the applications reside?</li></ul>
Mobile "backend" as a service (MBaaS) e.g.	In the mobile "backend" as a service (m) model, also known as backend as a service (BaaS), web app and mobile app developers are provided with a way to link their applications to cloud storage and cloud computing services with application programming interfaces (APIs) exposed to their applications and custom software development kits (SDKs).	<ul style="list-style-type: none"><li>• Integration</li><li>• Data ownership</li></ul>

# Cloud Computing Deployment Models

Deployment Model	Description of Cloud Infrastructure	To be considered
Private cloud	<ul style="list-style-type: none"><li>• Operated solely for an organization May be managed by the organization or a third party</li><li>• May exist on-premise or off-premise</li></ul>	<ul style="list-style-type: none"><li>• Cloud services with minimum risk</li><li>• May not provide the scalability and agility of public cloud services</li></ul>
Community cloud	<ul style="list-style-type: none"><li>• Shared by several organizations Supports a specific community that has shared mission or interest.</li><li>• May be managed by the organizations or a third party</li><li>• May reside on-premise or off-premise</li></ul>	<ul style="list-style-type: none"><li>• Same as private cloud, plus:</li><li>• Data may be stored with the data of competitors</li></ul>



# Cloud Computing Deployment Models

Deployment Model	Description of Cloud Infrastructure	To be considered
Public cloud	<ul style="list-style-type: none"><li>• Made available to the general public or a large industry group</li><li>• Owned by an organization selling cloud services</li></ul>	<ul style="list-style-type: none"><li>• Same as community cloud, plus:</li><li>• Data may be stored in unknown locations and may not be easily retrievable.</li></ul>
Hybrid cloud	<ul style="list-style-type: none"><li>• A composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)</li></ul>	<ul style="list-style-type: none"><li>• Aggregate risk of merging different deployment models</li><li>• Classification and labeling of data will be beneficial to the security manager to ensure that data are assigned to the correct cloud type.</li></ul>

# Cloud Computing Benefits

Some security benefits of the cloud

- **Market drive**—Because security is a top priority for most cloud customers, cloud providers have a strong driver for increasing and improving their security practices.
- **Scalability**—Cloud technology allows for the rapid reallocation of resources, such as those for filtering, traffic shaping, authentication and encryption, to defensive measures.
- **Cost-effective**—All types of security measures are cheaper when implemented on a large scale. The concentration of resources provides for cheaper physical perimeter and physical access control and easier and cheaper application of many security-related processes.
- **Timely and effective updates**—Updates can be rolled out rapidly across a homogeneous platform.
- **Audit and evidence**—Cloud computing can provide forensic images of virtual machines, which results in less downtime for forensic investigations.

## Cloud Computing Risks

- **Loss of governance**—The client usually relinquishes some level of control to the cloud provider, which may affect security, especially if the SLAs leave a gap in security defenses.
- **Lock-in**—It can be difficult for a client to migrate from one provider to another, which creates a dependency on a particular cloud provider for service provision.
- **Isolation failure**—One characteristic of cloud computing is shared resources. Although not commonplace, the failure of mechanisms that separate storage, memory, routing and reputation between different tenants can create risk.
- **Compliance**—Migrating to the cloud may create a risk in the organization achieving certification if the cloud provider cannot provide compliance evidence.

## Cloud Computing Risks

- **Management interface compromise**—The customer management interface can pose an increased risk because it is accessed through the Internet and mediates access to larger sets of resources.
- **Data protection**—It may be difficult for clients to check the data handling procedures of the cloud provider.
- **Insecure or incomplete data deletion**—Because of the multiple tenancies and the reuse of hardware resources, there is a greater risk that data are not deleted completely, adequately, or in a timely manner.
- **Malicious insider**—Cloud architects have extremely high-risk roles. A malicious insider could cause a great degree of damage.

## Managing risks in the cloud

To manage risk in the cloud the following should be addressed:

- Contractual agreements:
- Access controls
- Certification and third-party audits:
- Compliance requirements
- Availability, reliability, and resilience
- Back-up and recovery
- Decommissioning

## Consumerization of IT

Consumerization of IT is the reorientation of technologies and services designed around the individual end user. Examples include:

- Smart devices such as smartphones and tablets
- Bring Your Own Device (BYOD) strategies
- New, freely available applications and services

# Consumerization of IT

## PROS

- Shifts costs to user
- Worker satisfaction
- More frequent hardware upgrades
- Cutting-edge technology with the latest features and capabilities

## CONS

- IT loss of control
- Security risk
- Acceptable Use Policy difficult to enforce
- Unclear compliance and ownership of data

# Blockchain



Bad News





# What is Blockchain



Blockchain technology enables distributed public ledgers that hold irreversible data in a secure encrypted way to ensure that transactions cannot be altered.

# Blockchain use cases



Cross Border Payments



Digital Rights Management



Land Registry



Voting

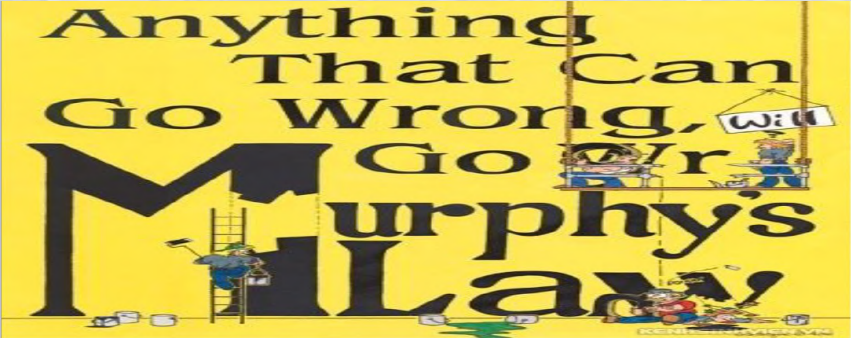


Identity



Internet of Things

# Blockchain Risks



Emerging  
Tech



Regulation



Software  
Vulnerability

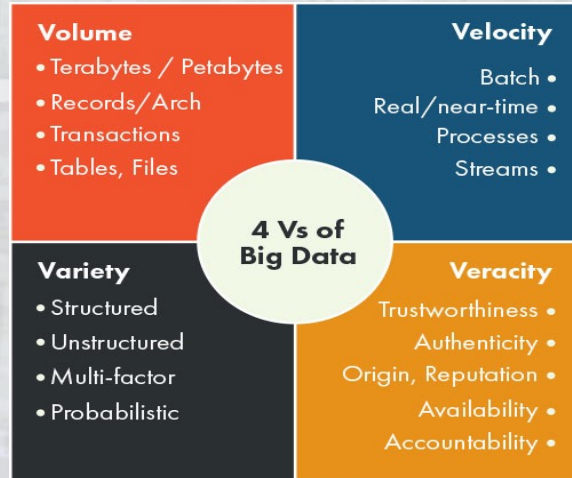


Unmet  
Expectations



Blockchain  
Hacks

# Big Data and Analytics



Big data is high-volume, high-velocity and high variety information assets that demand cost effective, innovative forms of information processing for enhanced insight and decision making

***Data and analytics** is the management of data for all uses (operational and analytical) and the analysis of data to drive business processes and improve business outcomes through more effective decision making and enhanced customer experiences.*

[Gartner](#)

# Getting Business Value from Data Analytics

Business has fundamentally changed with lots of systems in place integrating to each other

With innovation going on, you have to balance the risks introduced with the innovations in place.

Data is raw material that becomes valuable through the use of analytics.

Organizations have to use Data-driven decision making

We use technology, processes and people to ensure that we harness the power of data analytics.

# Artificial Intelligence

## Definition

- AI is a broad term that refers to the science of simulating human intelligence in machines with the goal of enabling them to think like us and mimic our actions.

## Benefits in cybersecurity

- Threat Detection
- Malware Detection
- Anomaly Detection
- Phishing Detection
- User Authentication
- Automated Response
- Vulnerability Management
- Security Analytics
- Threat Intelligence
- Security Automation

## Abuse of AI

- Social engineering schemes:
- Password hacking:
- Deepfakes:
- Data poisoning

# Prevention of cyber attacks

Organizational risk assessment

Cybersecurity framework, strategy and policies

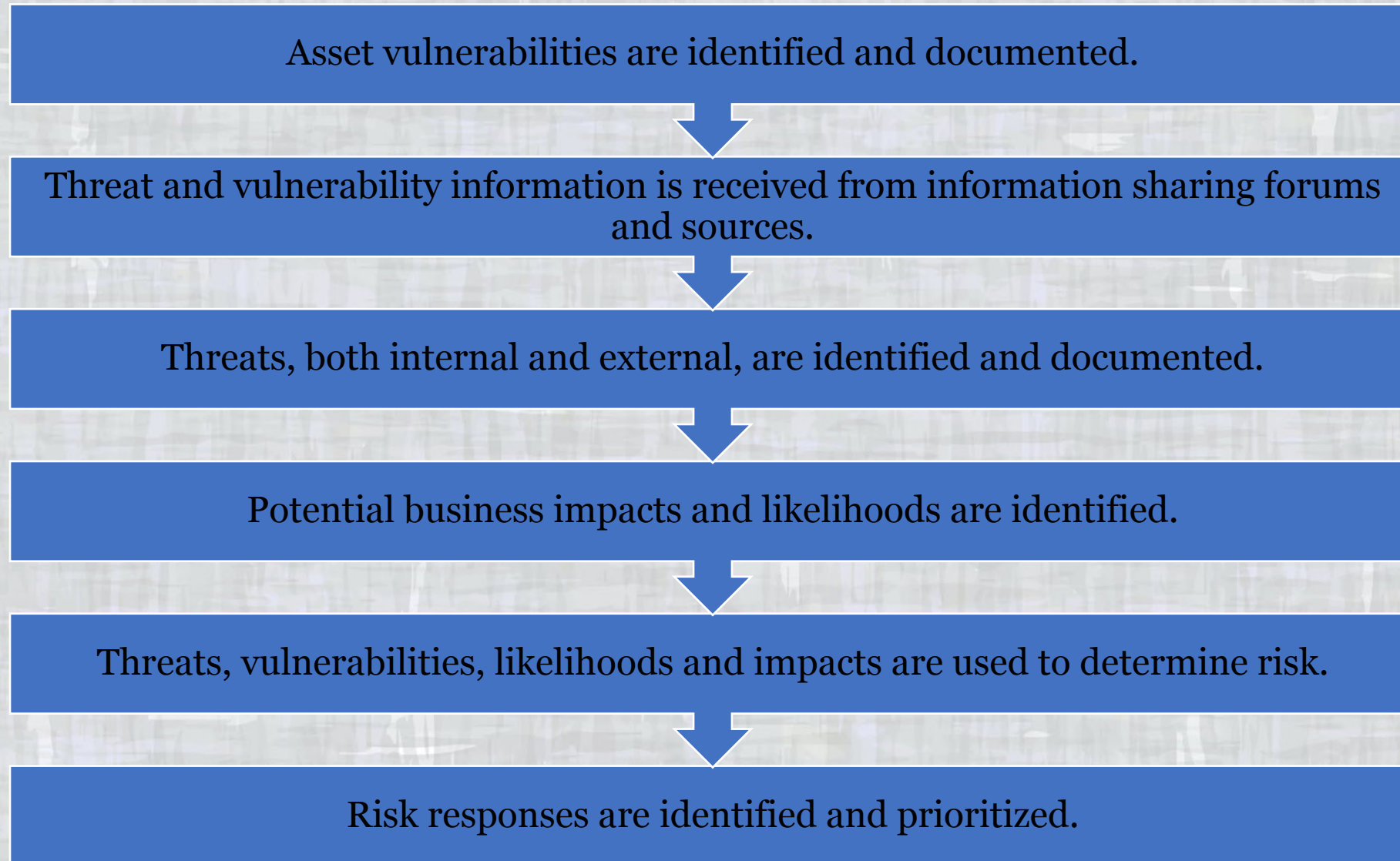
Investment in human resources and tools to combat cyber threats

Cybersecurity incident management

Organization wide information security awareness and training

Regular and independent compliance audits

## Organizational risk assessment





# CYBERSECURITY INVESTMENT

## 1. INTRUSION DETECTION AND PREVENTION SYSTEMS

IDS and IPS tools help protect the wired and wireless networks against several security threat types. These technologies, like several other categories of network security tools, are being deployed with greater frequency as networks grow in size and complexity.

Both IDS and IPS solutions detect threat activity in the form of malware, spyware, viruses, worms and other attack types, as well as threats posed by policy violations. IDS tools passively monitor and detect suspicious activity; IPS tools perform active, in-line monitoring and can prevent attacks by known and unknown sources.

## 2. ANTI-MALWARE

Anti-malware network tools help administrators identify, block and remove malware. Malware is always on the lookout for network vulnerabilities. Best practices call for a multipronged defense that might also include IP blacklisting, data loss prevention (DLP) tools, anti-virus and anti-spyware software, web browsing policies, egress filtering, and outbound-traffic proxies.

## 3. MOBILE DEVICE MANAGEMENT

MDM software enhances network security through remote monitoring and control of security configurations, policy enforcement and patch pushes to mobile devices. Further, these systems can remotely lock lost, stolen or compromised mobile devices and, if needed, wipe all stored data.

## **4. NETWORK ACCESS CONTROL**

NAC products enforce security policy by granting only security policy-compliant devices access to network assets. They handle access authentication and authorization functions and can even control the data that specific users access, based on their ability to recognize users, their devices and their network roles.

## **5. NEXT-GENERATION FIREWALLS**

This technology expands on traditional stateful inspection to provide next-generation network security services, including application visibility and control and web security essentials. Next-generation firewalls also improve on standard firewall capabilities through application-awareness features.

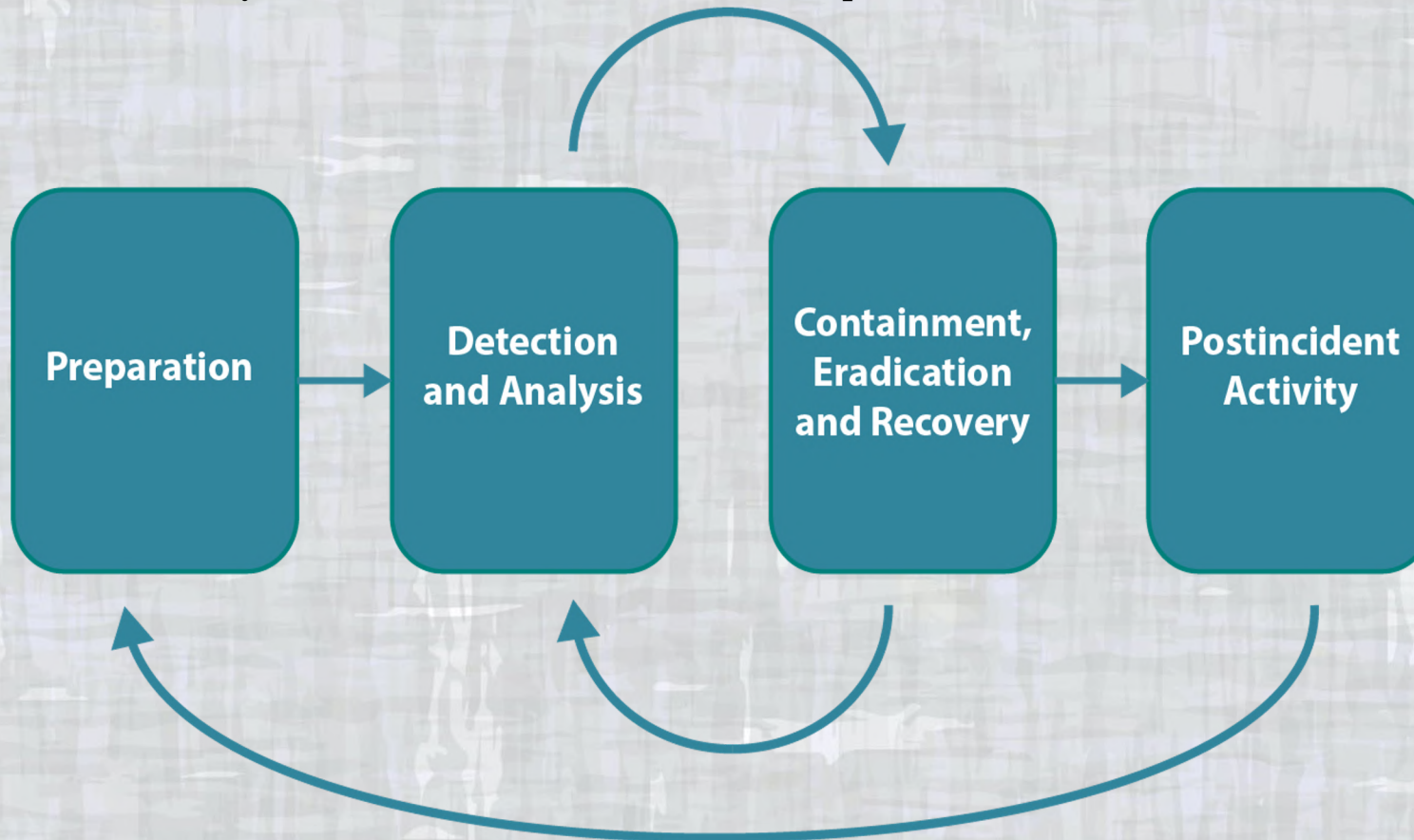
## **6. AUTHENTICATION AND AUTHORIZATION**

Traditional directory-based services, such as Active Directory, authenticate users and grant access based on authorization rules. Newer identity-based security technologies manage authentication and authorization through such methods as digital certificates and public key infrastructure solutions.

# INCIDENT RESPONSE PHASES

Incident response is a formal program that prepares an entity for an incident. Incident response phases are shown in below. Incident response generally includes:

1. Preparation to establish roles, responsibilities and plans for how an incident will be handled
2. Detection and Analysis capabilities to identify incidents as early as possible and effectively assess the nature of the incident
3. Containment capability if identifying an adversary is required
4. Eradication and Recovery procedures to contain the incident, reduce losses and return operations to normal
5. Postincident Analysis to determine corrective actions to prevent similar incidents in the future



# TRAINING AND AWARENESS

The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

All users are informed and trained.

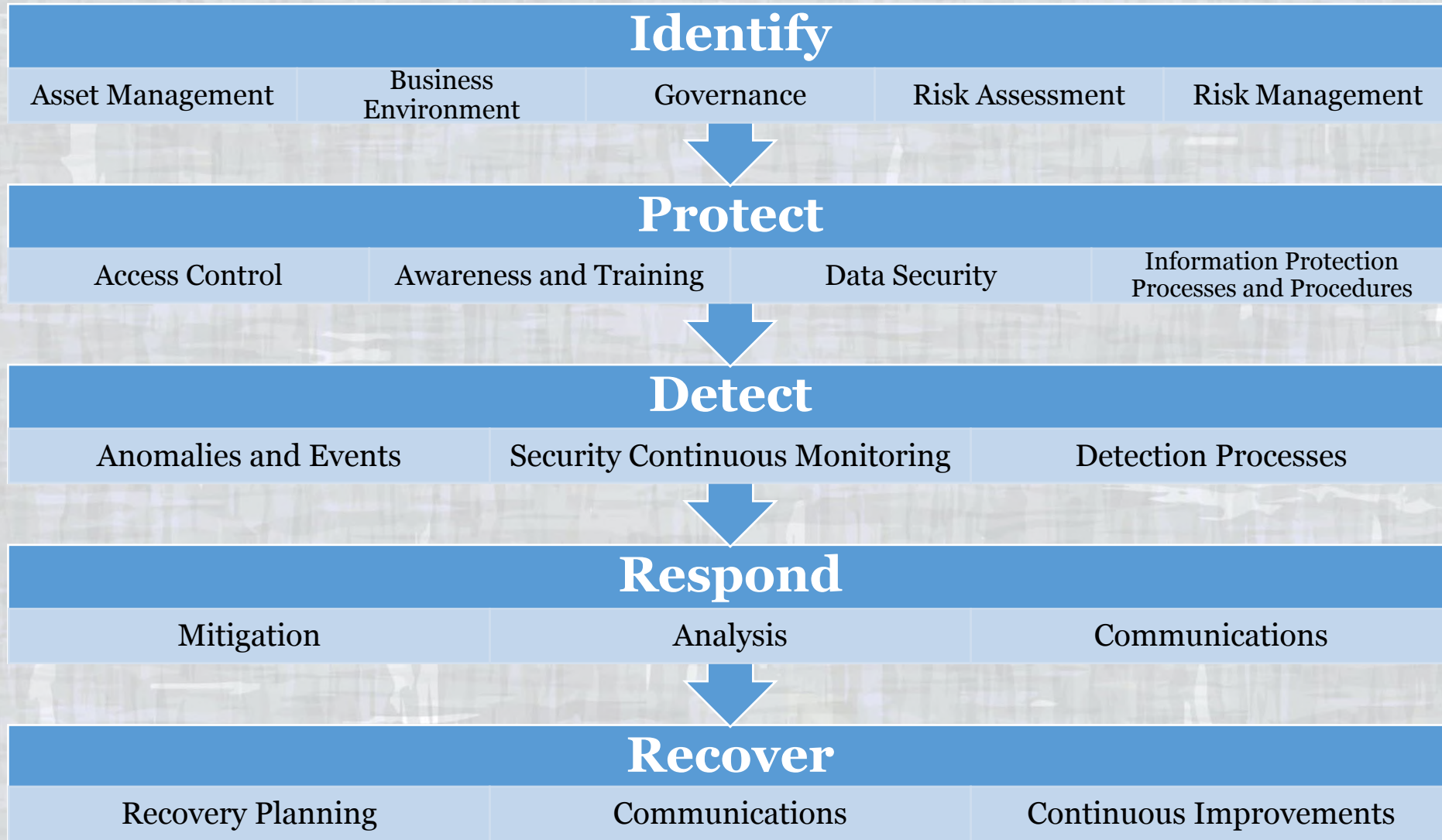
Privileged users understand roles and responsibilities.

Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities.

Senior executives understand roles and responsibilities.

Physical and information security personnel understand roles and responsibilities.

# CYBERSECURITY BEST PRACTICES



## Loss of Revenue

- This loss can be caused by an outside party who obtains sensitive financial information, using it to withdraw funds from an organization. It can also occur when a business e-commerce site becomes compromised-inoperable, valuable income is lost when consumers are unable to use the site.

## Data breaches

- Confidential data can be lost through cybercrime such as customer balances, customer names, transactions of customers, employee details and so on.

## Reputational Damage

- Financial institutions heavily rely on trust and if there is any publicized cybercrime, then it is likely to reduce the ability of the organization to attract new customers or even retain old ones as they lose public confidence.

## Regulatory fines

- Regulators are more stringent on organizations who don't protect themselves from cybercrime and in cases of breaches, they are likely to penalize such institutions

# GOVERNANCE, RISK MANAGEMENT & COMPLIANCE



## RISK MANAGEMENT

The process by which an organization manages risk to acceptable levels

## GOVERNANCE

- Provide strategic direction
- Ensure that objectives are achieved
- Ascertain whether risk is being managed appropriately
- Verify that organizational resources are used appropriately

## COMPLIANCE

The act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations.



# CYBERSECURITY ROLES



## BOARD OF DIRECTORS

---

Identify key assets and verify that protection levels and priorities are appropriate

## EXECUTIVE COMMITTEE

---

Set the tone for cybersecurity management and ensure that necessary functions, resources and infrastructure are available and properly utilized

## SECURITY MANAGEMENT

---

Develop security and risk mitigation strategies, implement security programs and manage incidents and remediation

## CYBERSECURITY PRACTITIONERS

---

Design, implement and manage processes and technical controls and respond to events and incidents

# LIKELIHOOD & IMPACT

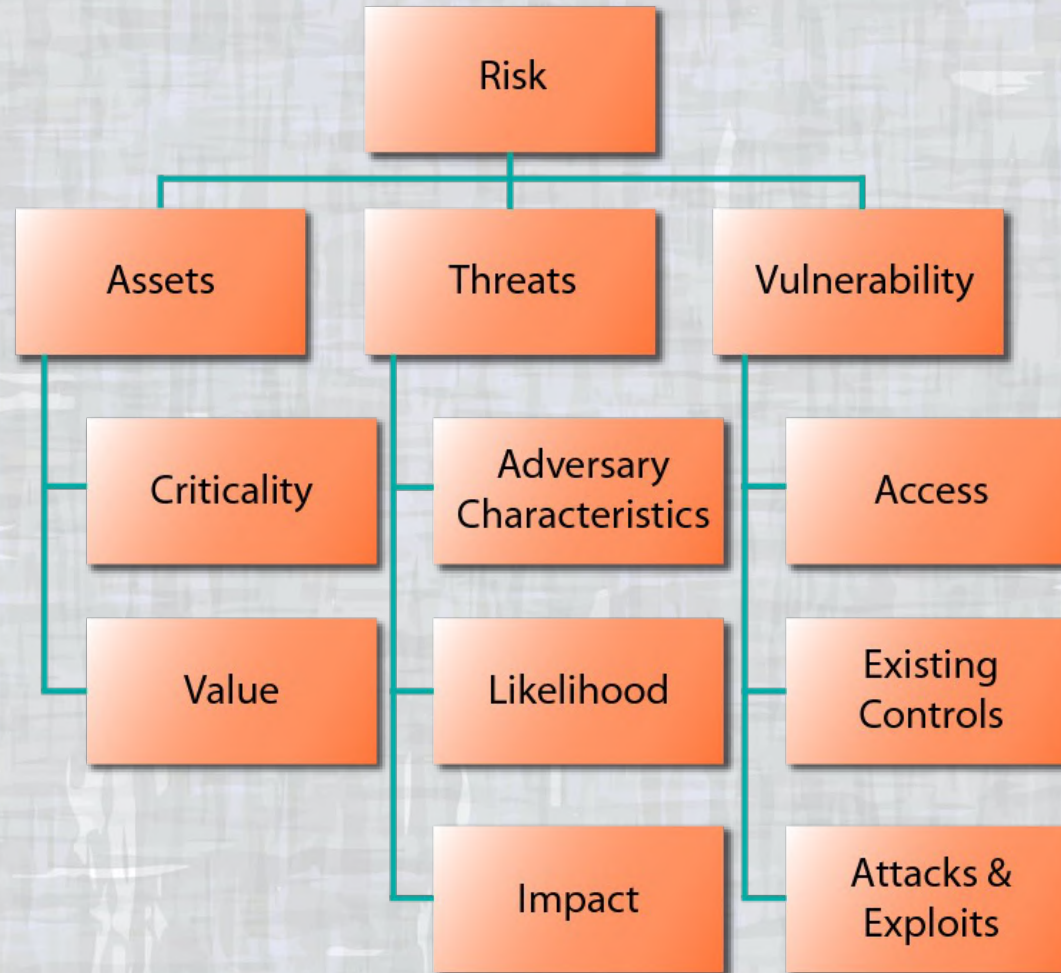


# Risk assessment

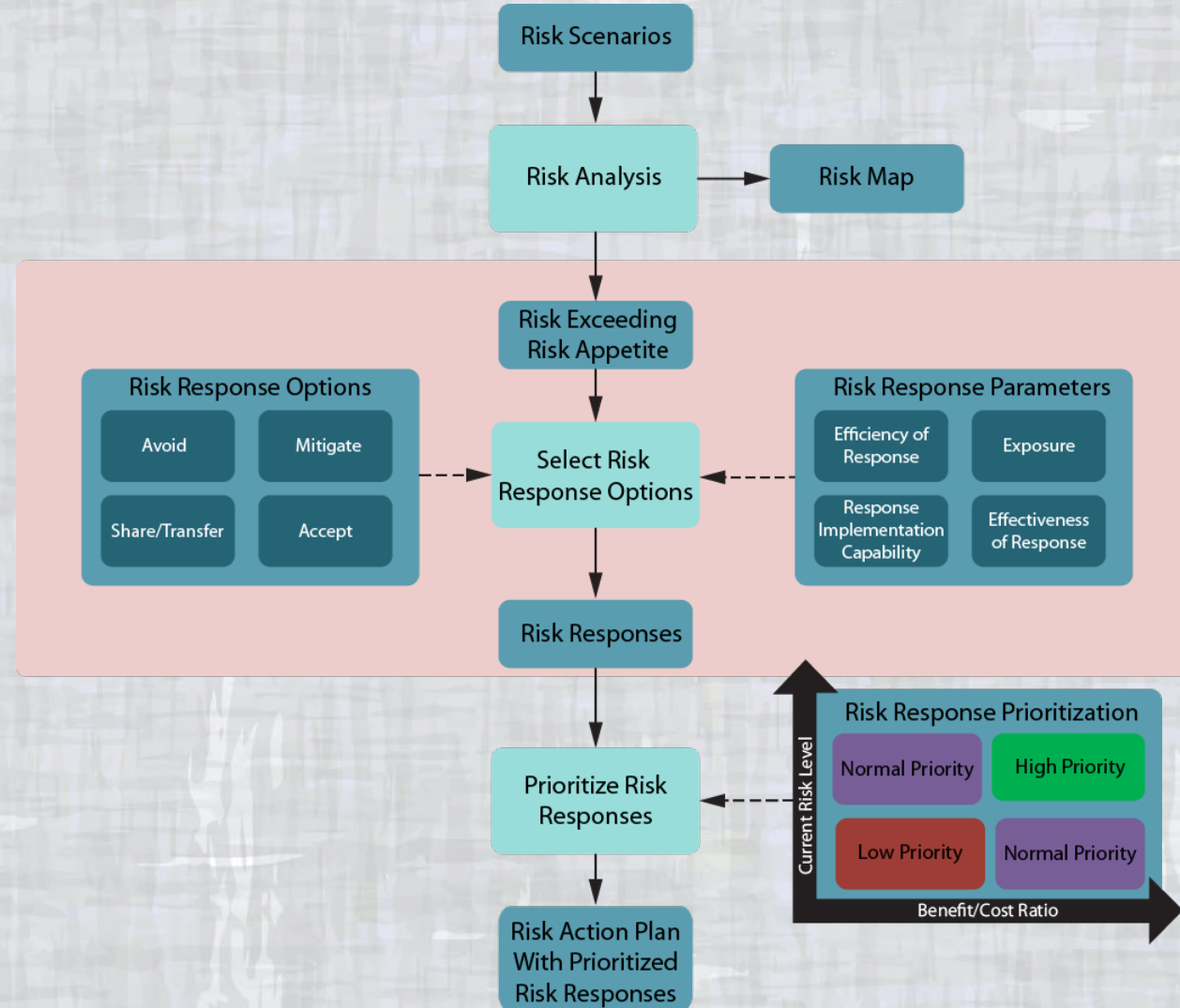
**Risk assessment**—a process used to identify and evaluate risk and its potential effects. It involves three inputs:

- **Asset assessment**
- **Threat assessment**
- **Vulnerability assessment**

# RISK ATTRIBUTES



# RISK MANAGEMENT



# RISK ASSESSMENT ORIENTATIONS

ORIENTATION	DESCRIPTION
Asset	Important assets are defined first, and then potential threats to those assets are analyzed. Vulnerabilities are identified that may be exploited to access the asset.
Threat	Potential threats are determined first, and then threat scenarios are developed. Based on the scenarios, vulnerabilities and assets of interest to the adversary are determined in relation to the threat.
Vulnerability	Vulnerabilities and deficiencies are identified first, then the exposed assets and potential threat events are determined.

# RISK RESPONSE STRATEGY

## Risk Reduction

- Implementation of controls or countermeasures to reduce likelihood or impact of risk to acceptable levels

## Risk Avoidance

- Avoid risk by not participating in an activity or business

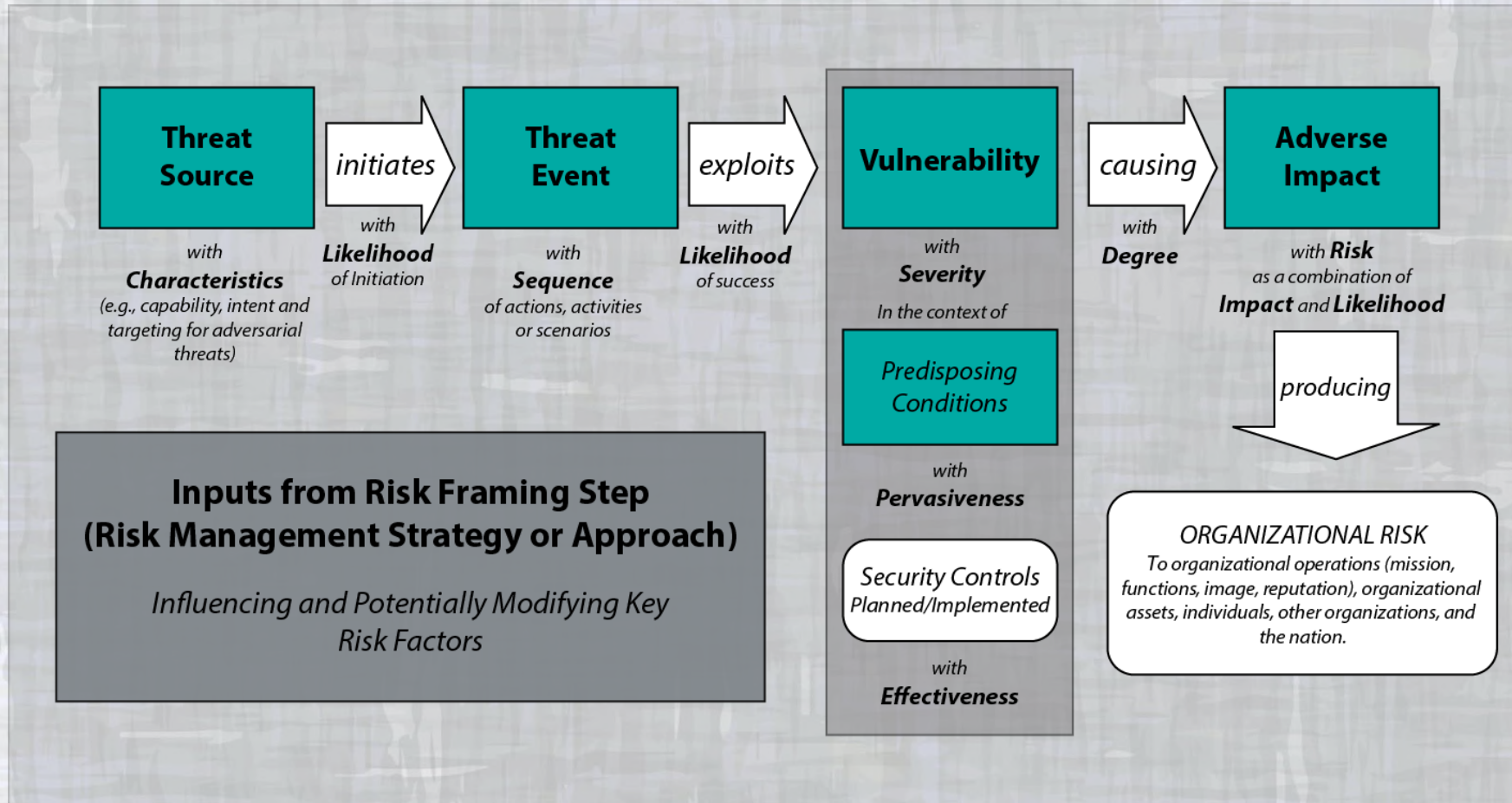
## Risk Transfer or Sharing

- Transfer risk to third party (e.g., insurance) or share with a third party via contractual agreement

## Risk Acceptance

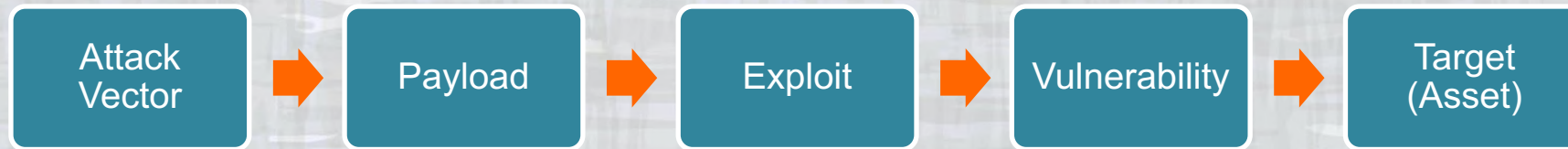
- Assume the risk and absorb losses if risk is within tolerance or the cost of mitigation exceeds potential loss

# RISK MANAGEMENT STRATEGY

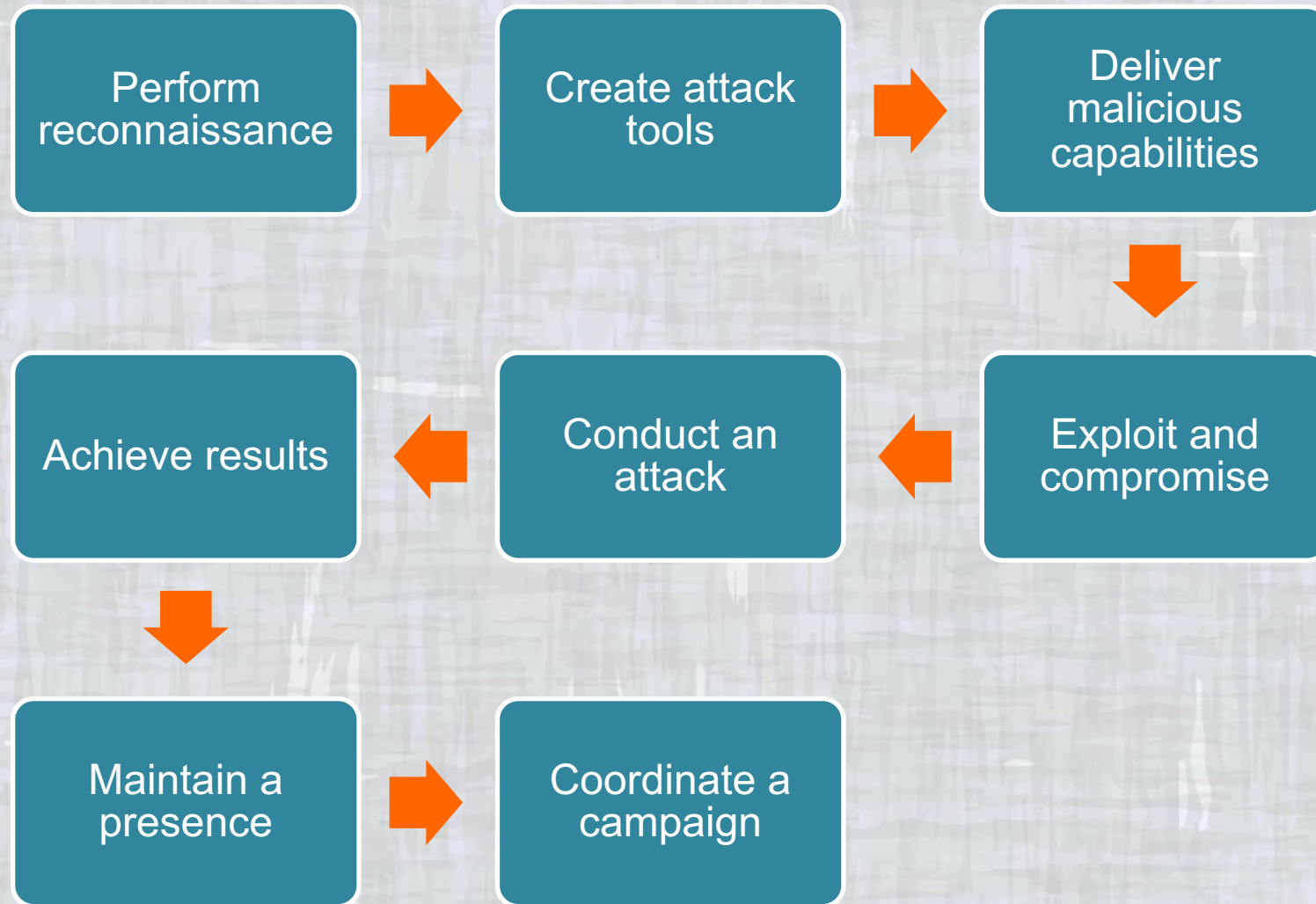




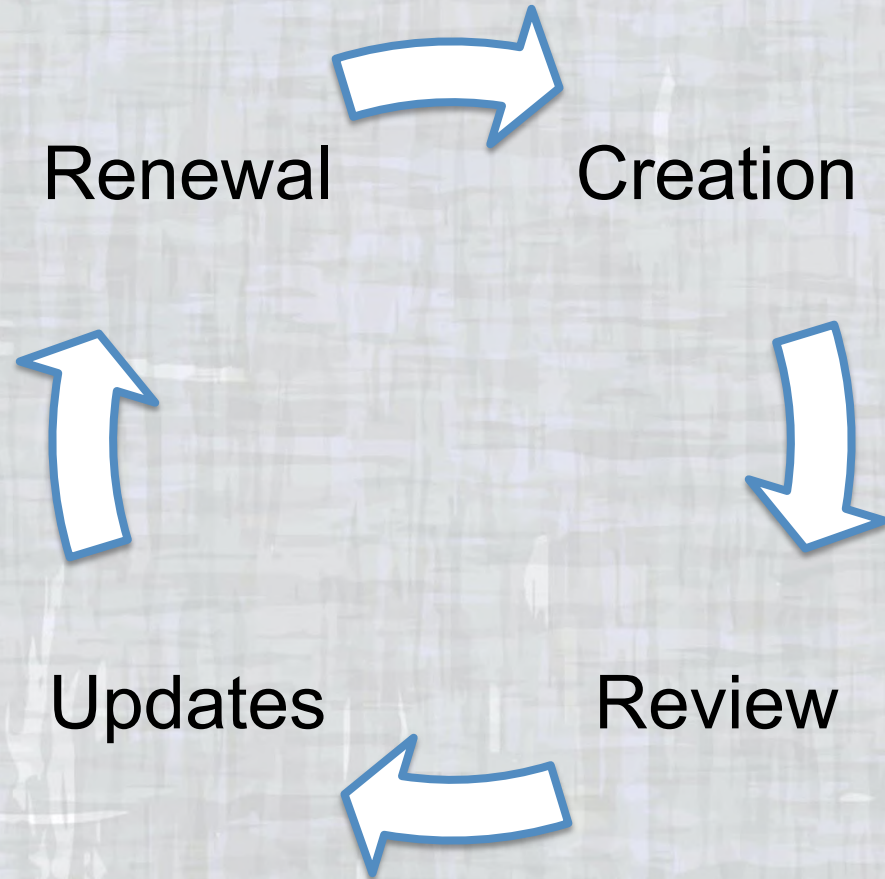
# ATTRIBUTES OF A CYBERATTACK



# GENERALIZED ATTACK PROCESS



# POLICY LIFE CYCLE



# POLICY FRAMEWORKS

Policy frameworks explain how compliance documents relate to one another.

---



# COBIT 2019 INFORMATION SECURITY POLICY SET

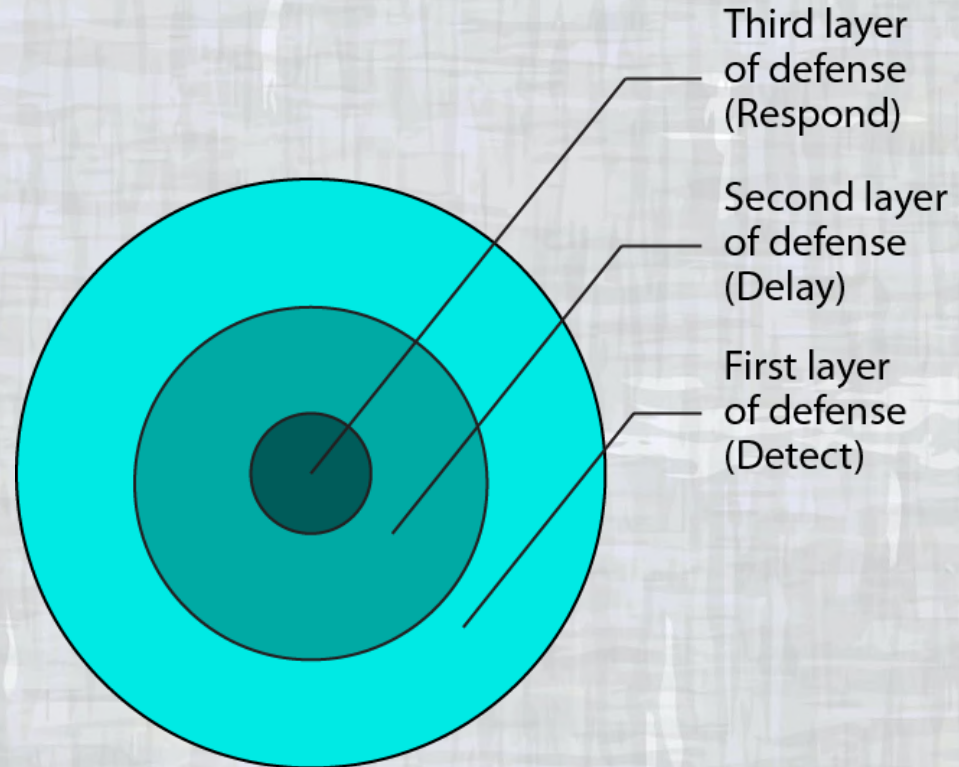


# DEFENSE IN DEPTH STRATEGIES

## CONCENTRIC RINGS

---

- Creates a series of nested layers that must be bypassed in order to complete an attack
- Each layer delays the attacker and provides opportunities to detect the attack



# DEFENSE IN DEPTH

When developing defense in depth implementations, consider the following questions:

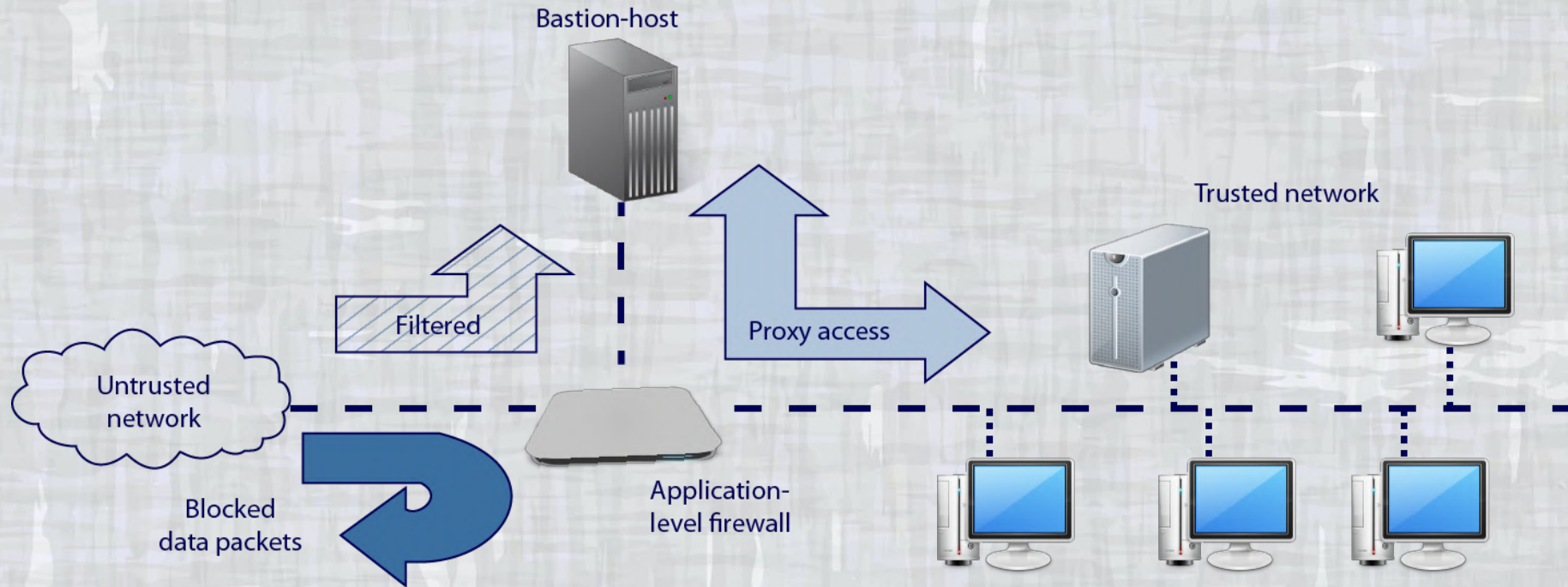
- What vulnerabilities are addressed by each layer or control?
- How does each layer mitigate the vulnerability?
- How does each control interact with or depend on the other controls?

# FIREWALL TECHNOLOGIES

- Packet Filters
- Stateful Inspection
- Application Proxy
- Next Generation Firewall

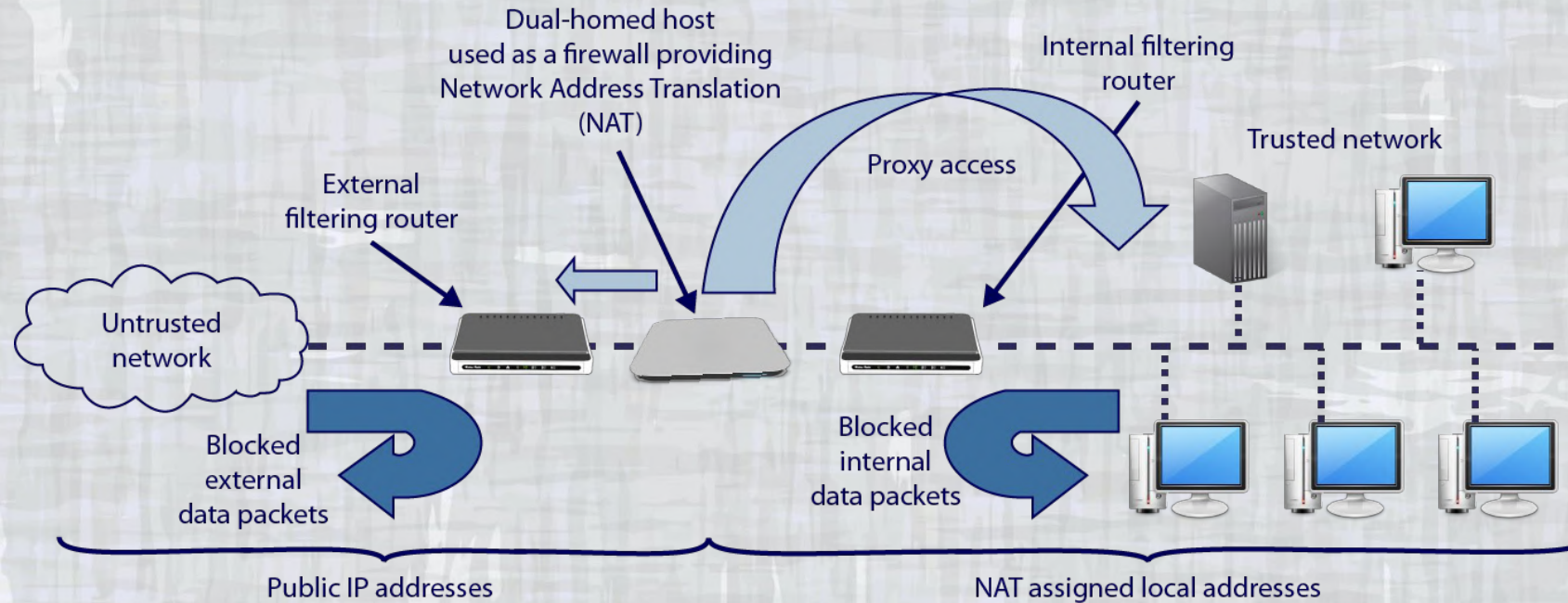


# SCREENED HOST FIREWALL



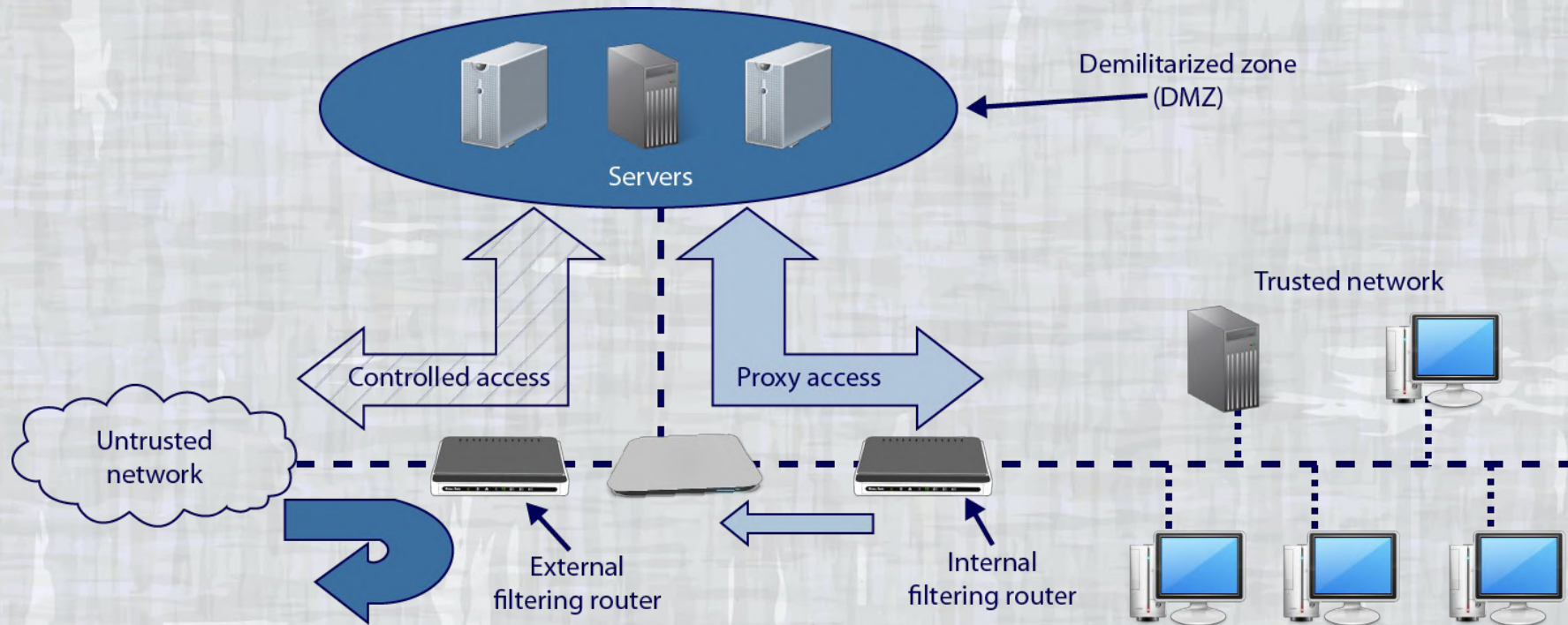
Source: <http://dc430.4shared.com/doc/Knqkp1ff/preview.html>

# DUAL-HOMED FIREWALL



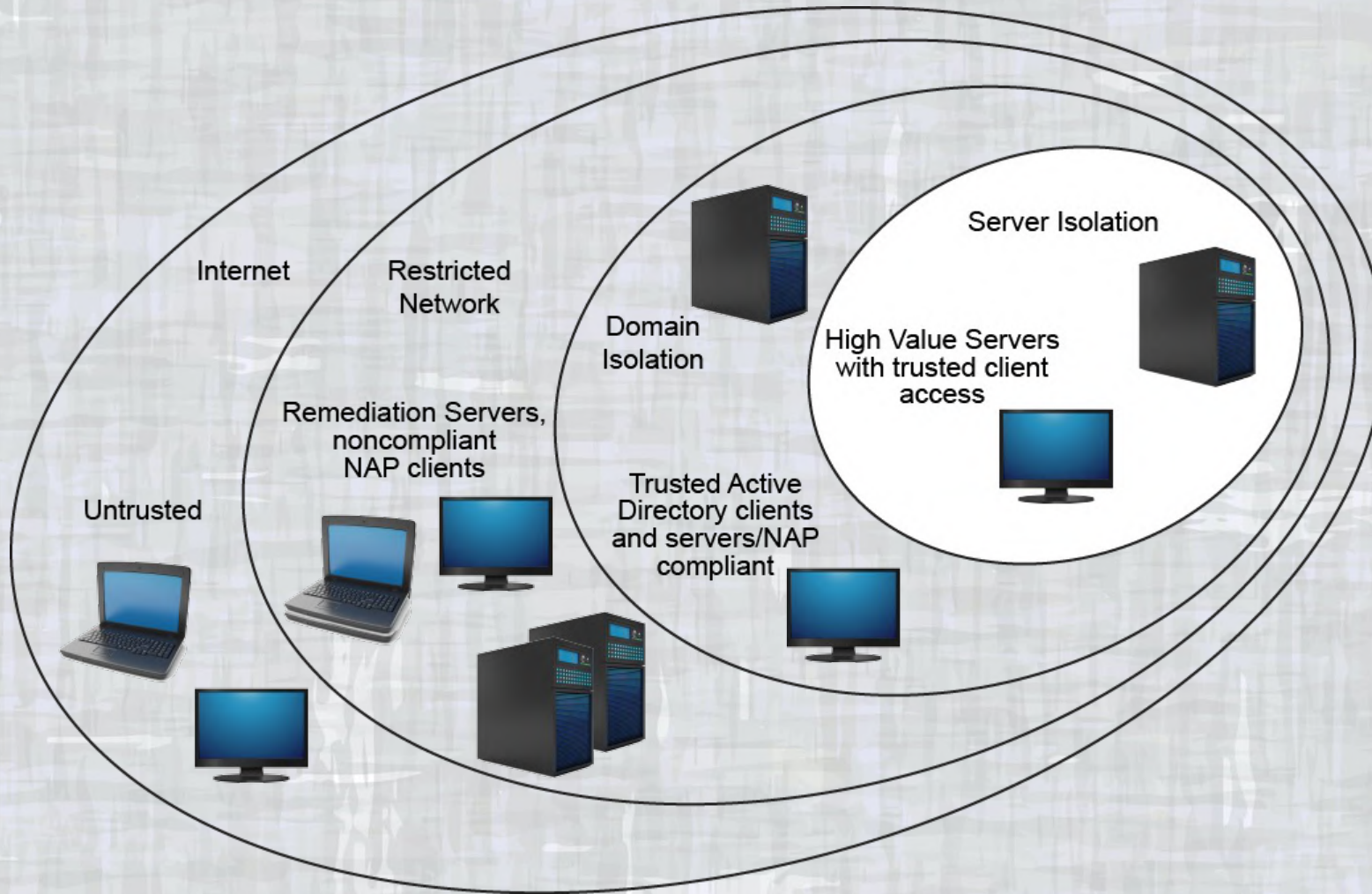
Source: <http://dc430.4shared.com/doc/Knqkp1ff/preview.html>

# DMZ / SCREENED SUBNET FIREWALL



Source: <http://dc430.4shared.com/doc/Knqkp1ff/preview.html>

# ISOLATION & SEGMENTATION



# Cryptography

## Cryptography is generally used to:

- Protect information stored on computers from unauthorized viewing and manipulation
- Protect data in transit over networks from unauthorized interception and manipulation
- Detect and identify accidental or intentional alterations of data
- Verify authenticity of a transaction or document

# KEY ELEMENTS OF ENCRYPTION

Key elements of encryption systems include:

- **Encryption algorithm** – A mathematically based function or calculation that encrypts or decrypts data
- **Encryption key** – A piece of information similar to a password that makes the encryption or decryption process unique
- **Key length** – A predetermined length for the key

# ENCRYPTION FACTORS

Effective encryption systems depend upon a variety of factors, including:

- Algorithm strength
- Secrecy and difficulty of compromising a key
- Nonexistence of backdoors by which an encrypted file can be decrypted without knowing the key
- Inability to decrypt parts of a cipher text message and prevent known plaintext attacks
- Properties of plaintext known by a perpetrator

# TYPES OF CRYPTOGRAPHIC SYSTEMS

## Symmetric Key Systems

- Use single, secret bidirectional keys that encrypt and decrypt
- Include DES, AES and Triple DES/DES3

## Asymmetric Key Systems

- Use pairs of unidirectional, complementary keys that only encrypt or decrypt
- One key is secret; the other is publicly known
- Include RSA, ECC



# Checksum

Uses a cryptographic hashing algorithm to create a message digest that verifies the integrity of the document

## COMMON MESSAGE DIGEST TYPES

SHA1

SHA2

MD2

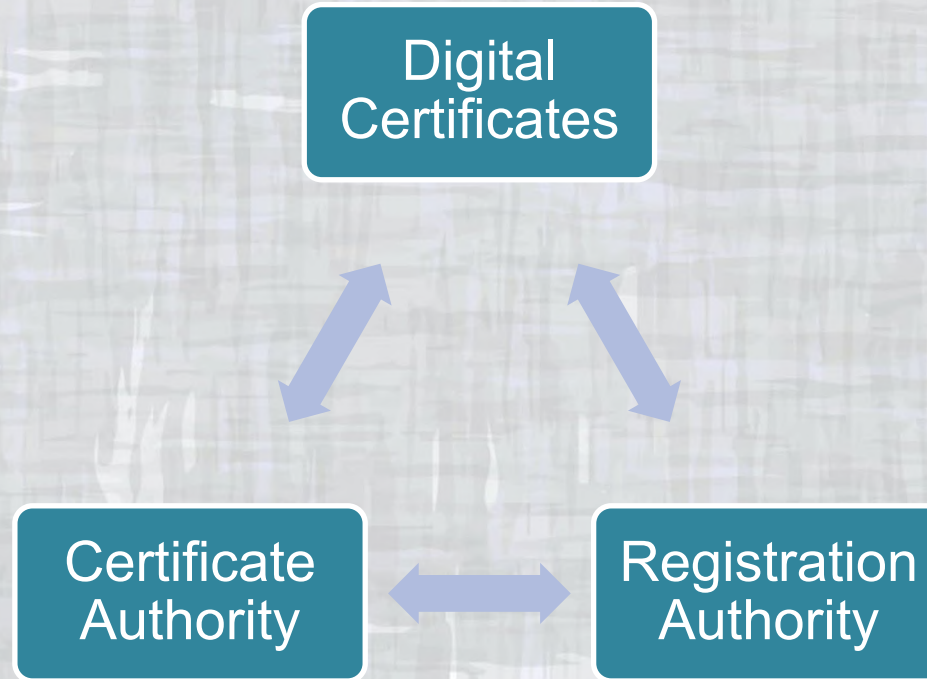
MD4

MD5

# PUBLIC KEY INFRASTRUCTURE (PKI)

Public key infrastructure allows a trusted third party to issue, maintain and revoke public key certificates.

## ELEMENTS OF PKI



# SECURE SOCKET LAYER (SSL) AND TRANSPORT LAYER SECURITY (TLS)

## SSL PHASES

Peer negotiation for algorithm support

```
graph TD; A[Peer negotiation for algorithm support] --> B[Public-key, encryption-based key exchange and certificate-based authentication]; B --> C[Symmetric cipher-based traffic encryption];
```

Public-key, encryption-based key exchange and certificate-based authentication

Symmetric cipher-based traffic encryption

# Vulnerability management

- A **vulnerability** is an exploitable weakness that results in a loss.
- They are continuously being discovered.
- Common discovery techniques include **vulnerability scans** and **penetration tests**.
- Organizations must understand **cybersecurity assets** and where they reside (physical and logical).
- Taking advantage of a vulnerability is called an **exploit**.

# COMMON TYPES OF VULNERABILITIES

TYPE	CAUSE	CYBERSECURITY EXAMPLES
Technical	Errors in design, implementation, placement or configuration	<ul style="list-style-type: none"><li>• Coding errors</li><li>• Inadequate passwords</li><li>• Open network ports</li><li>• Lack of monitoring</li></ul>
Process	Errors in operation	<ul style="list-style-type: none"><li>• Failure to monitor logs</li><li>• Failure to patch software</li></ul>
Organizational	Errors in management, decision-making, planning or ignorance	<ul style="list-style-type: none"><li>• Lack of policies</li><li>• Lack of awareness</li><li>• Failure to implement controls</li></ul>
Emergent	Interactions between, or changes in, environments	<ul style="list-style-type: none"><li>• Cross-organizational failures</li><li>• Interoperability errors</li><li>• Implementing new technology</li></ul>

# Penetration testing

Penetration testing uses common exploit methods to:

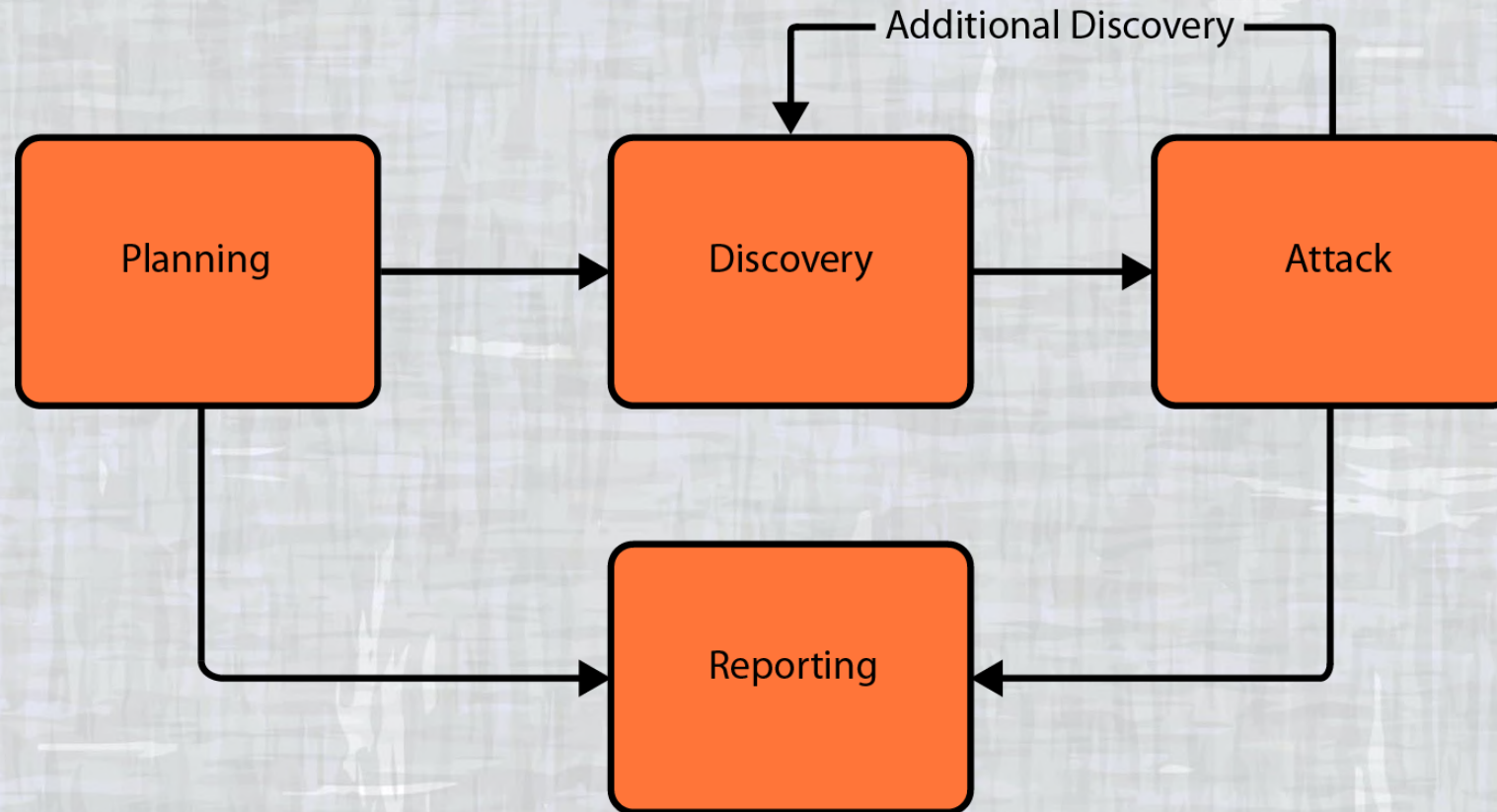
- Confirm exposures
- Assess the level of effectiveness and quality of existing security controls
- Identify how specific vulnerabilities expose IT resources and assets
- Ensure compliance

# Testing guidelines

## Before conducting a penetration test:

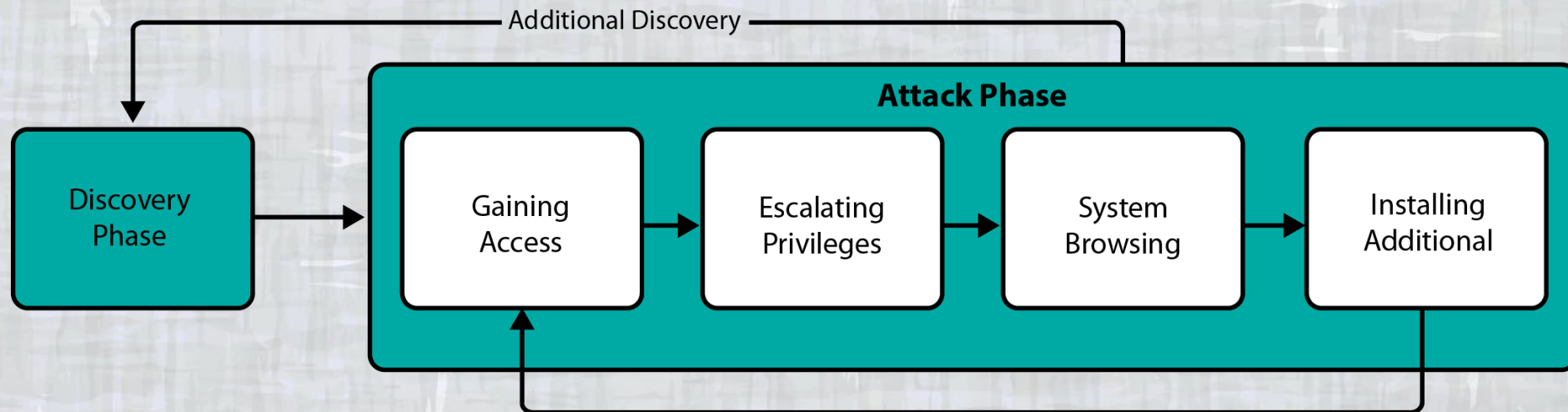
- Clearly define the scope of the test.
- Provide explicit, written permission authorizing testing.
- Implement “do no harm” procedures to ensure no assets are harmed (e.g., deletions, denial of service).
- Have communication and escalation plans.

# PHASES OF A PENETRATION TEST





# ATTACK PHASE



# SYSTEM HARDENING CONTROLS

- Authentication and authorization
- File system permissions
- Access privileges
- Logging and system monitoring
- System services

# VIRTUALIZATION

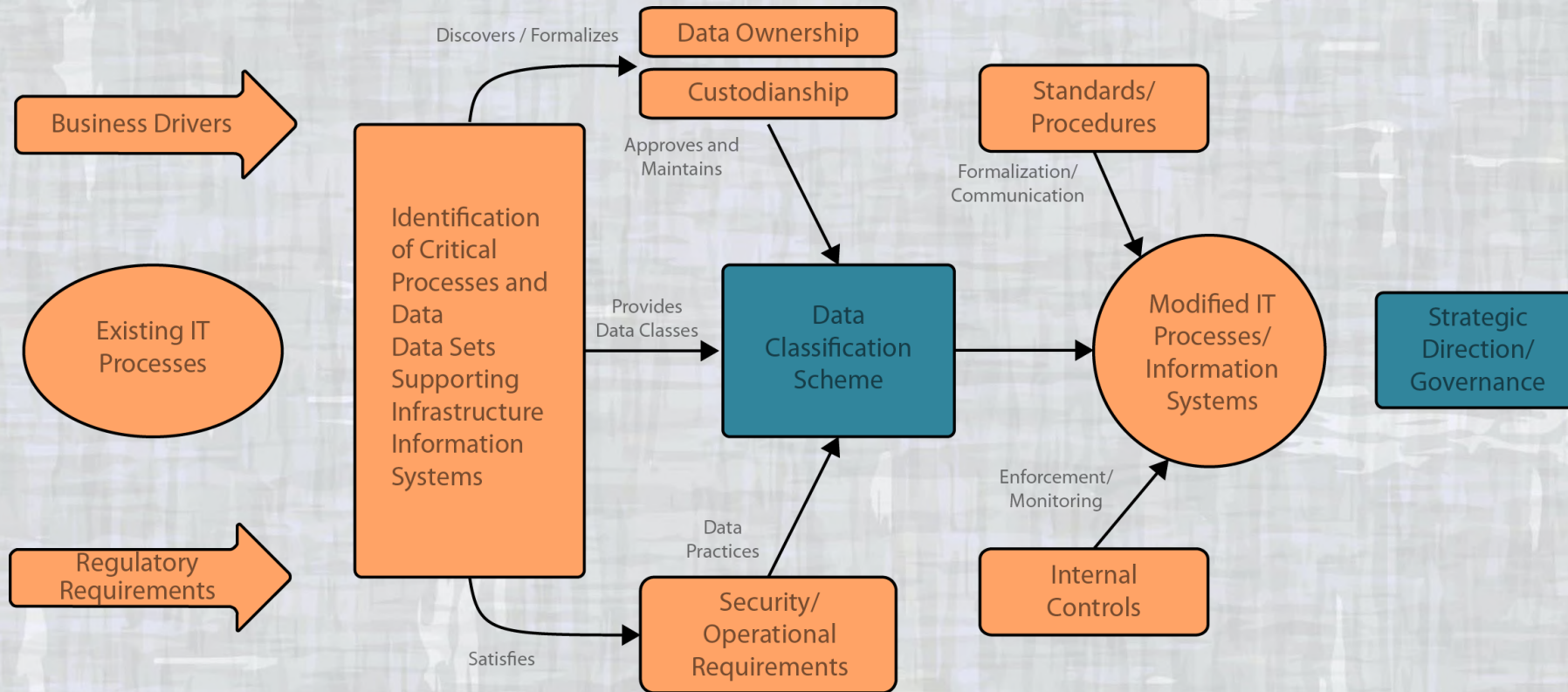
ADVANTAGES	DISADVANTAGES
Server hardware costs may decrease for server builds and maintenance.	Inadequate configuration of the host could create vulnerabilities that affect hosts and guests.
Multiple OSs can share processing capacity and storage space, reducing operating costs.	Exploits of vulnerabilities or a denial of service attack could affect all of the hosts guests.
The physical footprint of servers may decrease within the data center.	A compromise of the management console could grant guests unapproved administrative access.
A single host can have multiple versions of the same OS, or even different OSs.	Data could leak between guests if memory is not released and allocated properly by the host.
Creation of duplicate copies of guests in alternate locations can support business continuity efforts.	Insecure remote access protocols could result in exposure of administrative credentials.
A single machine can house a multitier network in an educational lab environment.	Performance issues of the host's own OS could impact each of the host's guests.

# Virtualization—OTHER Advantages

- Smaller organizations can set up logically separate, cost-effective development and test environments.
- A well built, single access control on the host can provide tighter control for the host's multiple guests.
- Application support personnel can have multiple versions of the same OS or even different OSs on a single host.



# DATA CLASSIFICATION PROCESS



# Data classification REQUIREMENTS

- Access and authentication
- Privacy
- Availability
- Ownership and distribution
- Integrity
- Data retention
- Auditability

# Data classification

- Keep levels to a minimum
- Keep level descriptions simple
- Define levels in policy
- Reclassify information as needed

# Database controls

- Authentication and authorization access
- Access controls limiting or controlling the type of data that can be accessed and what types of accesses are allowed (read-only, read-and-write or delete)
- Logging and other transactional monitoring
- Encryption and integrity controls
- Backups



# Difference between windows and linux events

Linux Events	Windows Events
Log files vary from distribution to distribution	Logs are generally similar across all windows systems
Logs are mostly located under /var/log/	Logs are located in the Event Viewer
<p>Logs are divided like so:</p> <p>Debian:</p> <ul style="list-style-type: none"><li>• <b>/var/log/auth.log</b> Logs of successful and failed authentications to your system can be found in this log file. It is also logged when a user invokes commands via sudo.</li><li>• <b>/var/log/messages</b> This file contains log entries of general system information, amongst others, you will also find the system upstart logs.</li><li>• <b>/var/log/syslog</b> This is one of the most important log files in general. Every Linux process is free to log to the syslog by implementing the syslog interface. It also logs the system upstart and executed cron-jobs.</li></ul>	<ul style="list-style-type: none"><li>• <b>Application</b> This entry will show the events of locally installed applications.</li><li>• <b>Security</b> Here you can see successful and failed login attempts.</li><li>• <b>System</b> This entry logs operating system internal events and errors.</li></ul>

# Difference between windows and linux events

Linux Events	Windows Events
<p><b>CentOS 7.2:</b></p> <ul style="list-style-type: none"><li>• <b>/var/log/secure</b> This log file is the equivalent to /var/log/auth.log in Debian systems. All kind of authentications are logged here.</li><li>• <b>/var/log/messages</b> There is no separation of /var/log/messages and /var/log/syslog in CentOS, all system logs of processes which implement the syslog interface can be found here.</li><li>• <b>/var/log/cron</b> Cron specific log files are not part of the syslog as in Debian. They can be found in the above mentioned file.</li></ul>	<p>There are other important entries like:</p> <ul style="list-style-type: none"><li>• Forwarded events</li><li>• Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational</li><li>• Microsoft-Windows-SMBServer/Security</li><li>• Microsoft-Windows-Sysmon/Operational</li></ul>
Events don't have IDs	Events have IDs called <b>Events IDs</b>

# Tools you can use to enhance events

- Sysmon for linux
- modifying /etc/profile - linux
- Sysmon for windows

Install the tools on windows and linux

# Windows Events

Event ID	What it means
4624	Successful account log on
4625	Failed account log on
4634	An account logged off
4648	A logon attempt was made with explicit credentials
4719	System audit policy was changed.
4964	A special group has been assigned to a new log on
1102	Audit log was cleared. This can relate to a potential attack
4720	A user account was created
4722	A user account was enabled

# Windows Events

4723	An attempt was made to change the password of an account
4725	A user account was disabled
4728	A user was added to a privileged global group
4732	A user was added to a privileged local group
4756	A user was added to a privileged universal group
4738	A user account was changed
4740	A user account was locked out
4767	A user account was unlocked
4735	A privileged local group was modified
4737	A privileged global group was modified

# Windows Events

4755	A privileged universal group was modified
4772	A Kerberos authentication ticket request failed
4777	The domain controller failed to validate the credentials of an account.
4782	Password hash an account was accessed
4616	System time was changed
4657	A registry value was changed
4697	An attempt was made to install a service
4698, 4699, 4700, 4701, 4702	Events related to Windows scheduled tasks being created, modified, deleted, enabled or disabled
4946	A rule was added to the Windows Firewall exception list
4947	A rule was modified in the Windows Firewall exception list

# Windows Events

4950	A setting was changed in Windows Firewall
4954	Group Policy settings for Windows Firewall has changed
5025	The Windows Firewall service has been stopped
5031	Windows Firewall blocked an application from accepting incoming traffic
5152, 5153	A network packet was blocked by Windows Filtering Platform
5155	Windows Filtering Platform blocked an application or service from listening on a port
5157	Windows Filtering Platform blocked a connection
5447	A Windows Filtering Platform filter was changed

# Event vs. incident

**An event is any change, error or interruption within an IT infrastructure such as a system crash, a disk error or a user forgetting their password.**

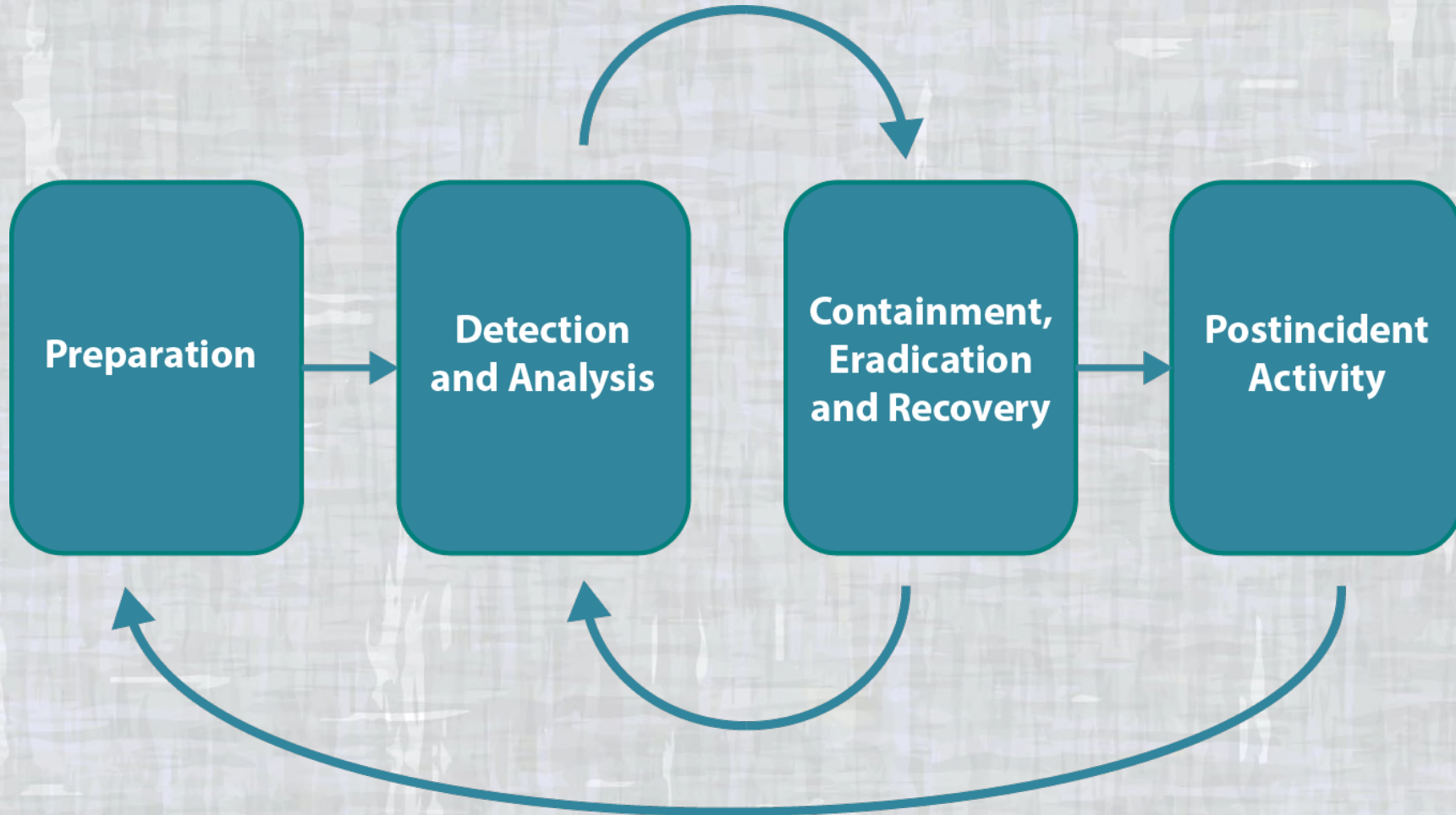
**An incident is any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service.**



# INCIDENT CATEGORIES

CATEGORY	NAME	DESCRIPTION	REPORTING TIME FRAME
CAT 1	Unauthorized access	Individual gains logical or physical access without permission to a network, system, application, data or other resource	Within 1 hour of discovery/detection
CAT 2	Denial of service (DoS)	An attack that successfully prevents or impairs normal authorized functionality of networks, systems or applications by exhausting resources	Within 2 hours of discovery/detection (if the successful attack is still ongoing)
CAT 3	Malicious code	Successful installation of malicious software (e.g., virus, worm, Trojan horse or other code-based malicious entity) that infects an operating system or application	Daily; within 1 hour of discovery/detection if widespread
CAT 4	Improper Usage	Authenticates identity of sender and receiver to ensure privacy of message contents (including attachments)	Weekly
CAT 5	Scans / probes / attempted access	Any activity that seeks to access or identify a computer, open ports, protocols, service or any combination of the above	Monthly
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity	N/A

# INCIDENT RESPONSE PHASES



# Preparing for an incident

- Establish approach to handling incidents
- Establish policy and warning banners to deter intruders and allow information collection
- Establish communication plan with stakeholders
- Develop incident reporting criteria
- Develop process to activate the incident management team
- Establish secure location to execute the incident response plan
- Ensure equipment needed is available

# Identifying an incident

- Assign ownership to an incident handler
- Verify reports or events qualifying as incidents
- Establish chain of custody
- Determine incident severity and escalate as necessary

# Containing an incident

- Activate incident management/response team and notify appropriate stakeholders
- Obtain agreement on actions taken that may affect availability
- Get IT representative and relevant virtual team members to implement containment procedures
- Obtain and preserve evidence
- Document actions
- Control and manage communication to the public

# Eradicating an incident

- Determine signs and cause of incidents
- Locate most recent version of backups or alternative solutions
- Remove root cause
- Improve defenses by implementing protection techniques
- Perform vulnerability analysis

# Recovering from an incident

- Restore operations to normal
- Verify that actions taken on restored systems were successful
- Get system owners to test the system
- Help system owners declare normal operation

# Lessons learned

- Write incident report
- Analyze issues encountered during incident response efforts
- Propose improvements
- Present report to relevant stakeholders



# Incident investigations

- Have a goal of identifying the perpetrator of an attack or unauthorized use or access
- May be conducted for criminal activity, violations of contracts or violations of policy
- May be performed in-house, by a third-party consultant, by law enforcement, regulators or a combination

# Evidence preservation

- Evidence includes log files, file time stamps, contents of memory, etc.
- The first step is to create a copy of the system.
- **Chain of custody** is a term that refers to documenting how evidence is handled and maintained, including its ownership, transfer and modification.

# Legal issues

Evidence collection and storage

Chain of custody for evidence

Searching or monitoring communications

Interviews or interrogations

Licensing requirements

Law enforcement involvement

Labor, union and privacy regulation

# FORENSICS CHAIN OF EVENTS



# Forensics key elements

- Data protection
- Data acquisition
- Imaging
- Extraction
- Ingestion or normalization
- Interrogation
- Reporting
- Network traffic analysis
- Log file analysis
- Timelines

# Anti-Forensics

- Securely deleting data
- Overwriting metadata
- Preventing data creation
- Encrypting data
- Encrypting network protocols
- Hiding data in slack or unallocated space
- Hiding data or files within another file (steganography)

# What is a disaster?

**Disasters** are disruptions that cause critical information resources to be inoperative for a period of time, adversely impacting organizational operations.



# BUSINESS CONTINUITY PLANS





# BUSINESS IMPACT ANALYSES

Business Impact Analysis provides the basis for



Business Continuity Planning, which determines



Recovery Time Objectives  
Recovery Point Objectives  
Maximum Tolerable Outages  
Service Delivery Objectives

# Cybersecurity risk

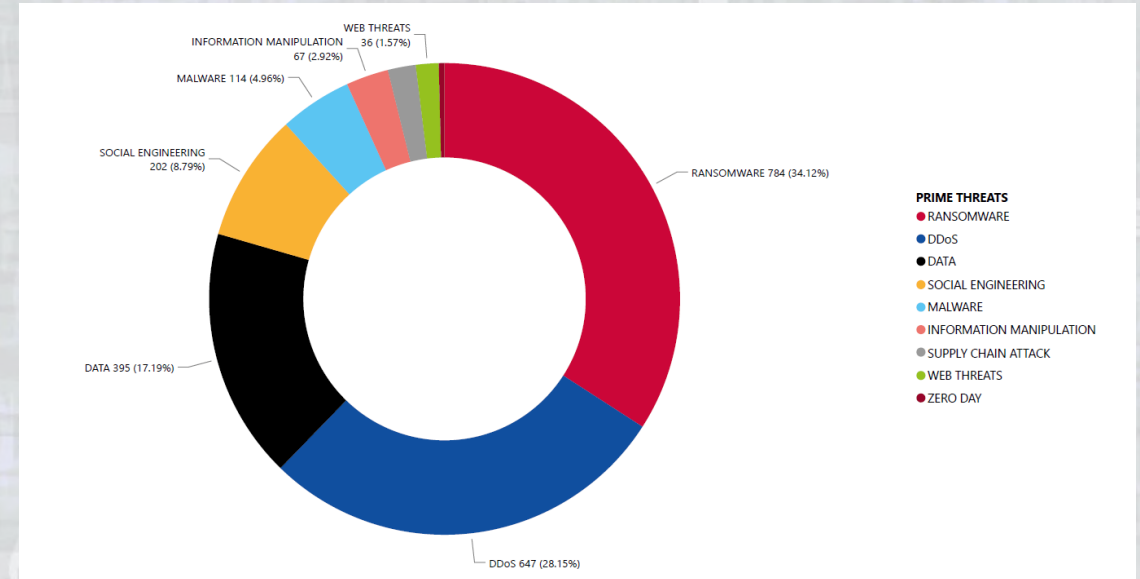
Increasing dependence on digital technologies makes organizations more susceptible to cybersecurity risk.



# Threat landscape

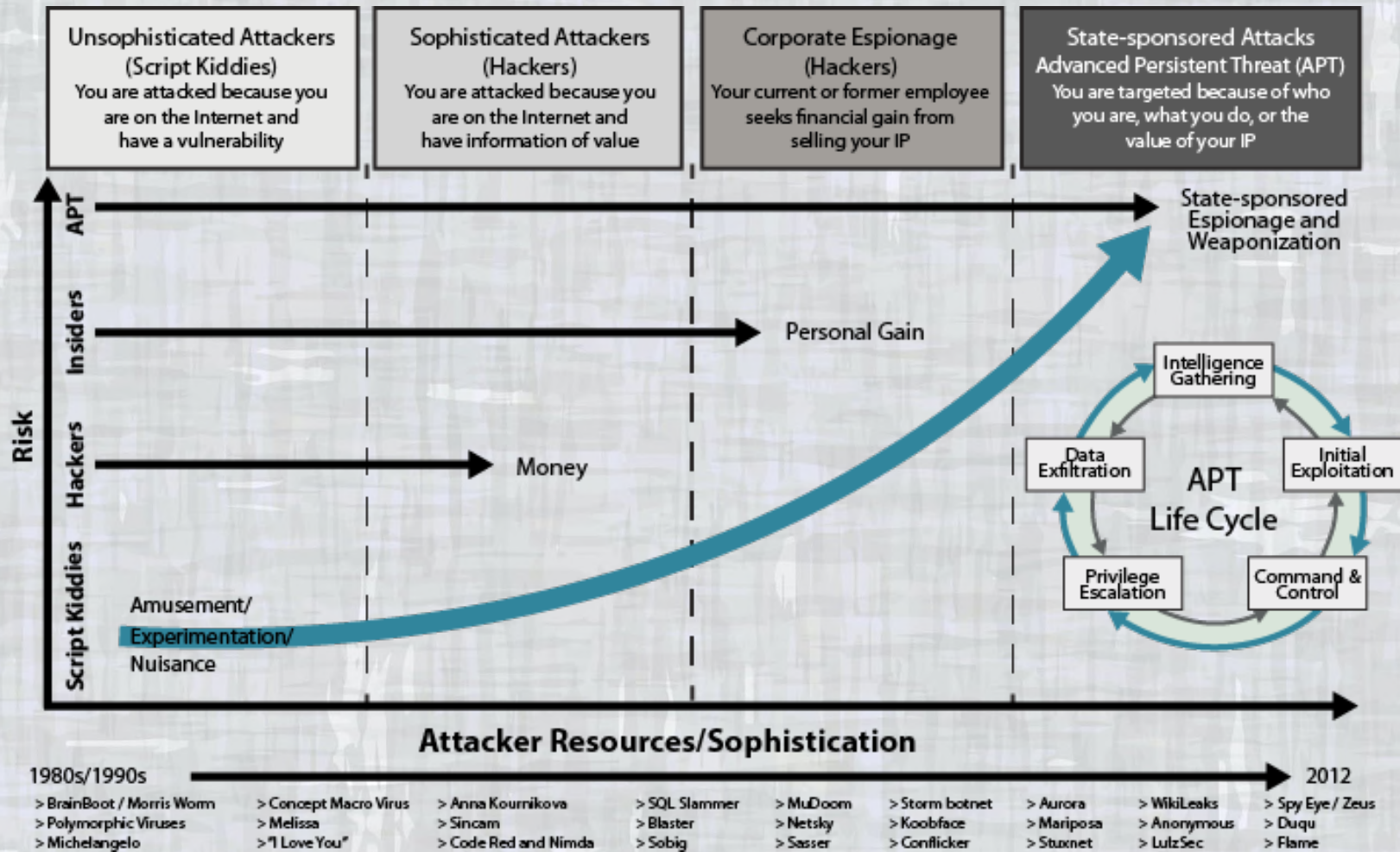
- **Collection of threats**
- **Constantly changing**
- **Evolves as new technologies are developed and attacks become more sophisticated**

# RECENT TRENDS IN CYBERSECURITY



Source: ENISA Threat Landscape 2023

# EVOLUTION OF THE THREAT LANDSCAPE



# What is an apt?

An **APT** is targeted threat that is composed of various complex attack vectors and can remain undetected for an extended period of time.

In addition, APTs have the following characteristics:

- Unprecedented degree of planning, resources employed and techniques used
- Often follow a particular *modus operandi*

# APT SOURCES OF THREAT

THREAT	WHAT THEY SEEK	BUSINESS IMPACT
Intelligence agencies	Political, defense or commercial trade secrets	Loss of trade secrets or commercial, competitive advantage
Criminal groups	Money transfers, extortion opportunities, personal identify information or secrets for potential onward sale	Financial loss, large-scale customer data breach or loss of trade secrets
Terrorist groups	Production of widespread terror through death, destruction and disruption	Loss of production and services, stock market irregularities, and potential risk to human life
Activist groups	Confidential information or disruption of services	Major data breach or loss of service
Armed forces	Intelligence or positioning to support future attacks on critical national infrastructure	Serious damage to facilities in the event of a military conflict

# STAGES OF AN APT ATTACK





# Salaam Technology

## Service offering:

### Salaam Assurance

- An independent audit on IT governance, access to programs and data, computer operations and interfaces.

### Salaam Cybersecurity Testing (VAPT)

- A security review through vulnerability assessment and penetration testing to identify the threats to an organization whether internal or external.
- We simulate the actions of a malicious intruder to your systems to ensure that all loopholes are sealed.

### Salaam 24/7 (Managed Security Services)

- We provide 24/7 continuous monitoring to your network for fraud and cyber attacks.
- With our expertise in incident response, we are sure to provide the best in class service as we hunt the malicious actors, detect attacks and respond to them before they escalate.

### Salaam Analytics

- We have the expertise in analysing complex data to aid in decision making. We use daily, weekly and monthly analytical monitoring to determine patterns so that you can tell us what you are doing well, determining how we can do it better and recognizing problems before they can result in material damage.

### Salaam Awareness

- We provide training and awareness on various emerging areas on IT such as Cybersecurity and Anti Money Laundering.
- We have partnered with the leading providers of this platform such as KnowBe4 among others

# Contact/Questions



Raymond Bett

M-PESA, Whatsapp,  
Truecaller, +254 720 983 411

[raymond.bett@salaam.ke](mailto:raymond.bett@salaam.ke)

[www.salaam.ke](http://www.salaam.ke)