

UNDERSTANDING CYBER RISK

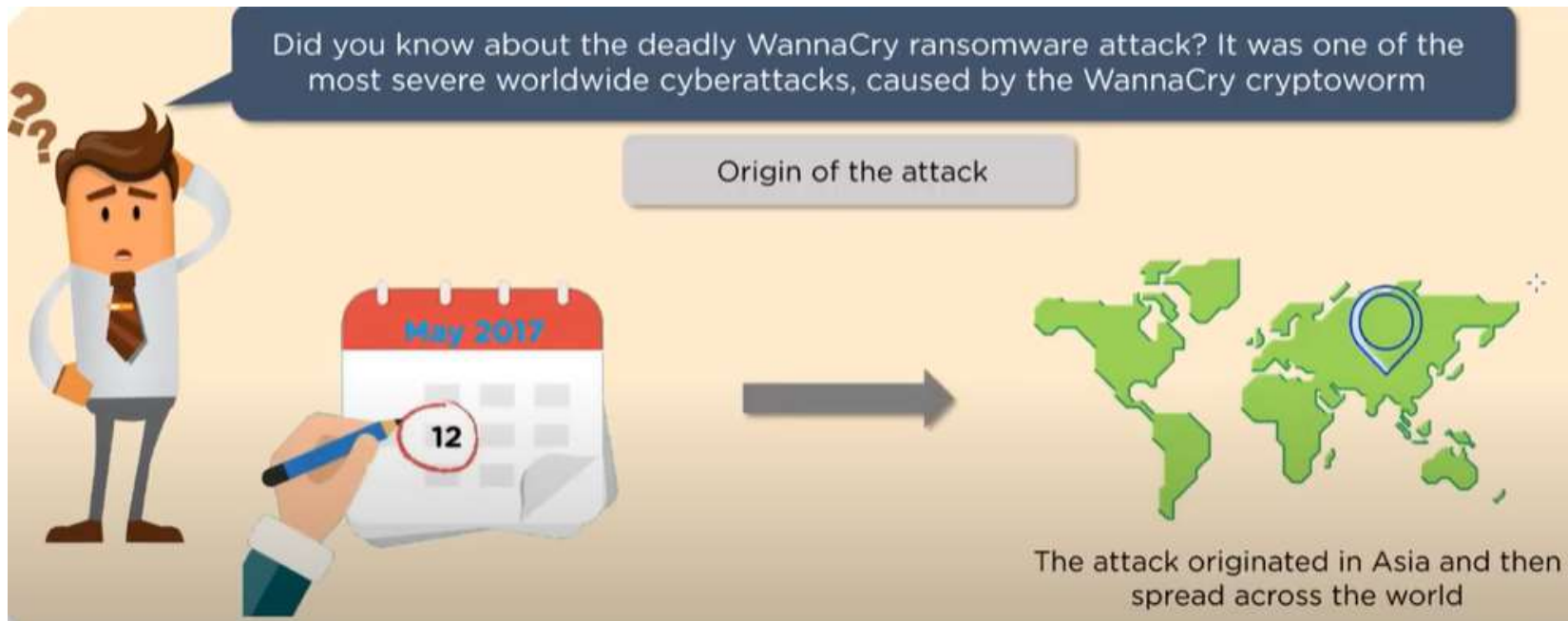
-The most disruptive risk of next decade

Presented by :
Harsh Jaitak

POLL 1: HAVE YOU EVER WORKED ON CYBER INSURANCE PRODUCTS?

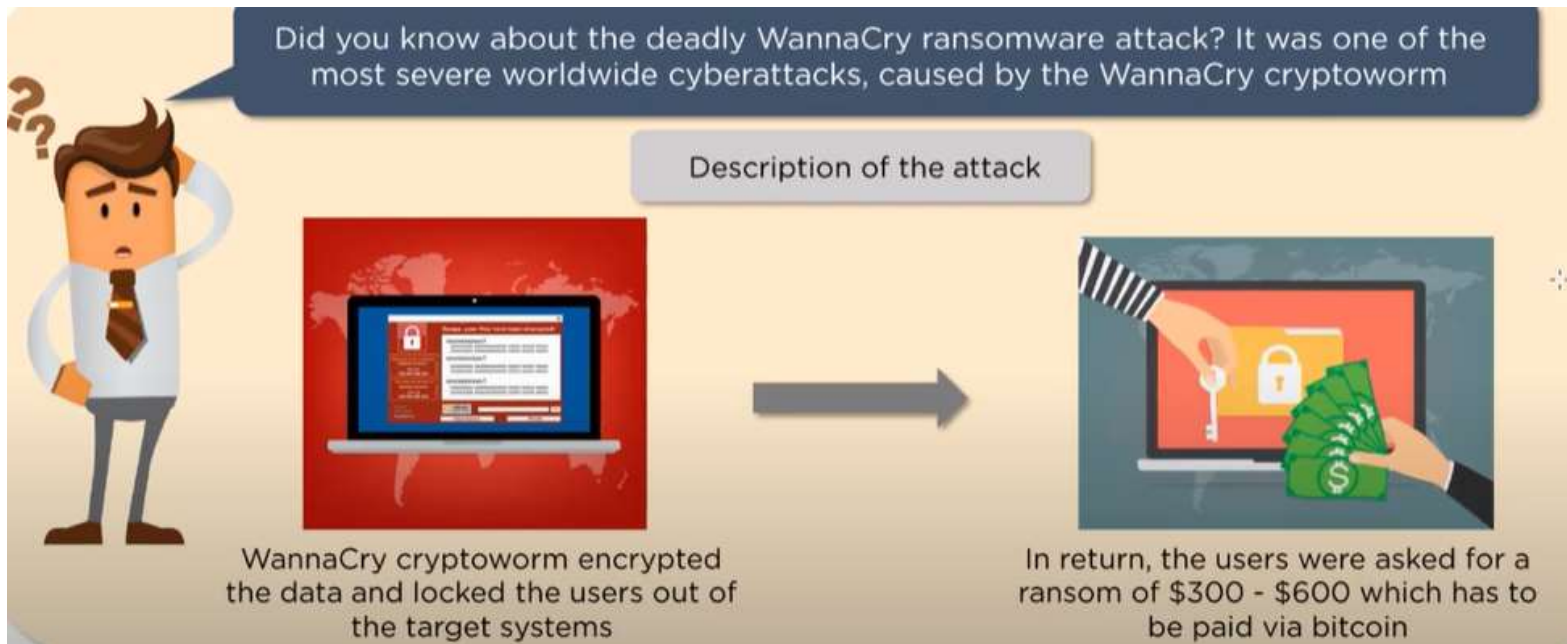
- Yes
 - No
-

RISE OF CYBERCRIME



More than 230,000 computers were affected across 150 countries

RISE OF CYBERCRIME



Both private and government organizations were hit. Nissan and Renault had to put their business on hold.

RISE OF CYBERCRIME



Personal Identifiable information stolen.

TYPE OF CYBERATTACKS

Malware
Attack

Denial Of
Service
Attack

Social
Engineering
Attack

SQL
Injection
Attack

Man in the
middle
attack

Password
Attack

POLL 3: WHICH OF THE FOLLOWING DO YOU KNOW LEAST ABOUT?

- Malware Attack
 - Denial of Service Attack
 - Social Engineering Attack
 - SQL Injection Attack
 - Man in the middle attack
 - Password Attack
-

MALWARE ATTACK

Malware refers to malicious software, viruses, ransomware, and worms. Trojan virus is also a form of malware that disguises itself as a legitimate software



MALWARE ATTACK

It gets into a system when the user clicks on suspicious links or downloads attachments or uses an infected pen drive. It then obtains all the information from the client's system



User opens links or uses a corrupted pen drive



User's system gets corrupted



SOCIAL ENGINEERING ATTACK

It is the art of manipulating people so that they end up giving their confidential information. It is broken down into 3 categories:



Phishing Attack

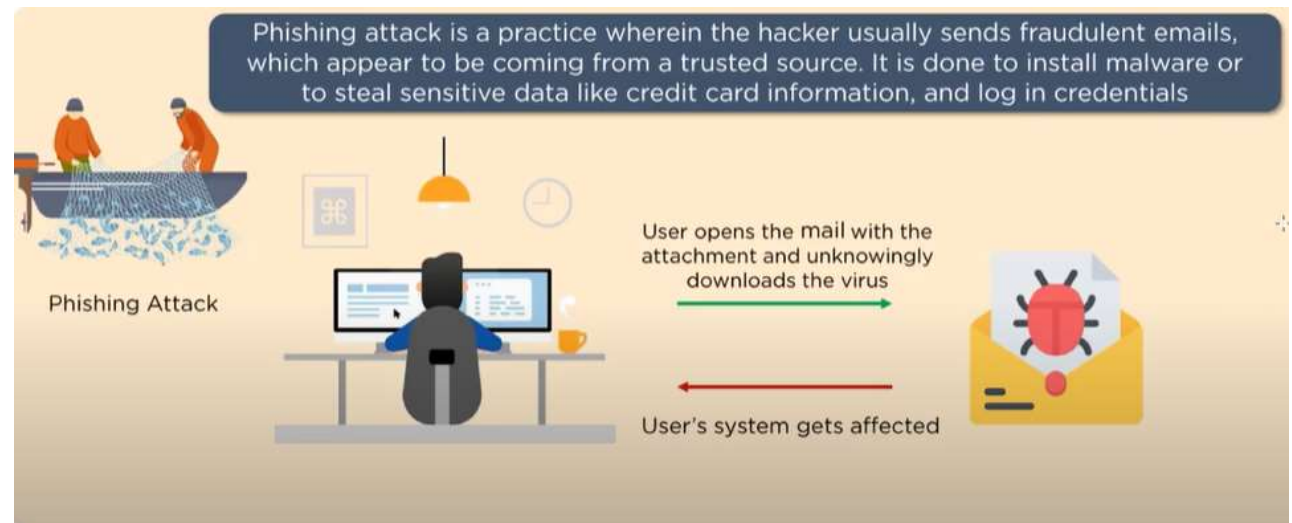


Spear Phishing Attack



Whaling Phishing Attack

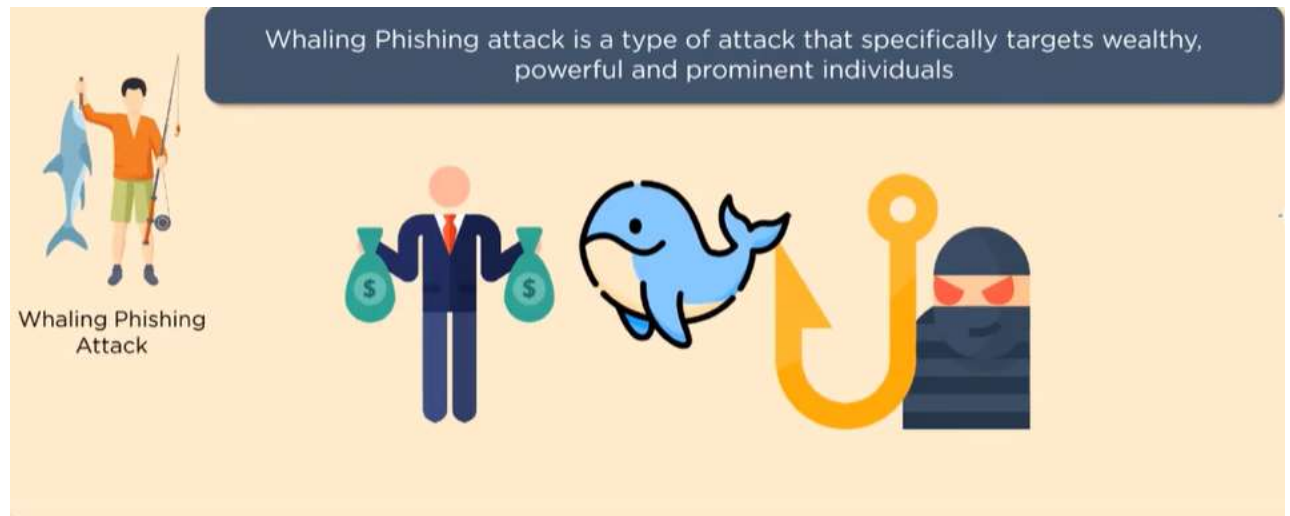
PHISHING ATTACK



SPEAR PHISHING ATTACK



WHALING PHISHING ATTACK



MAN IN THE MIDDLE ATTACK

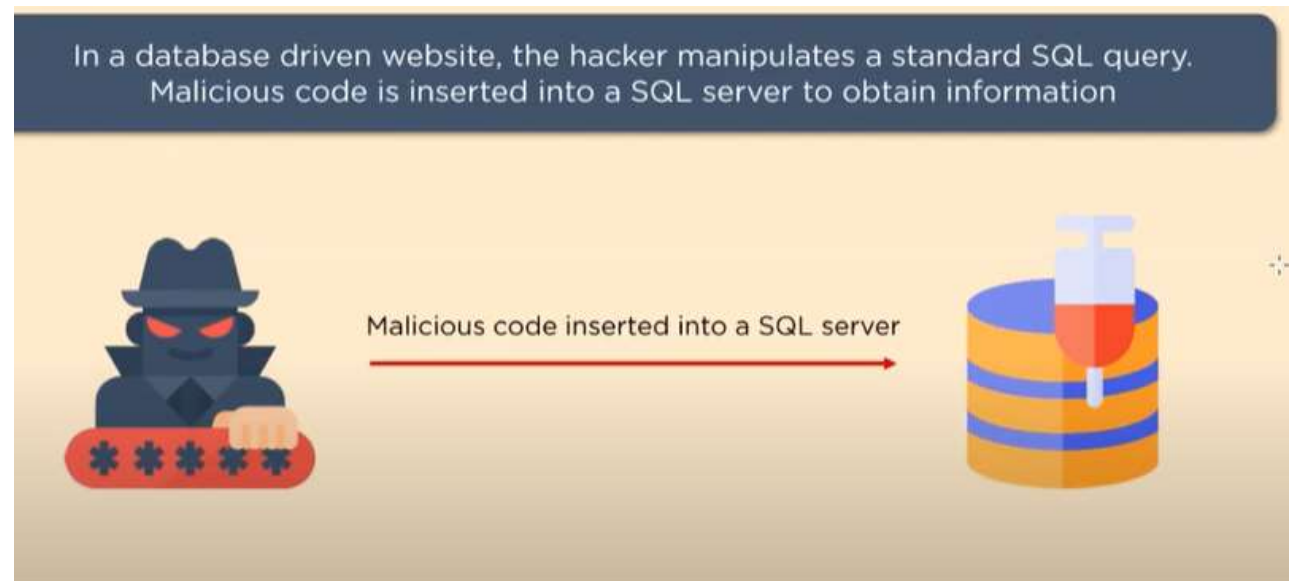


DENIAL OF SERVICE ATTACK

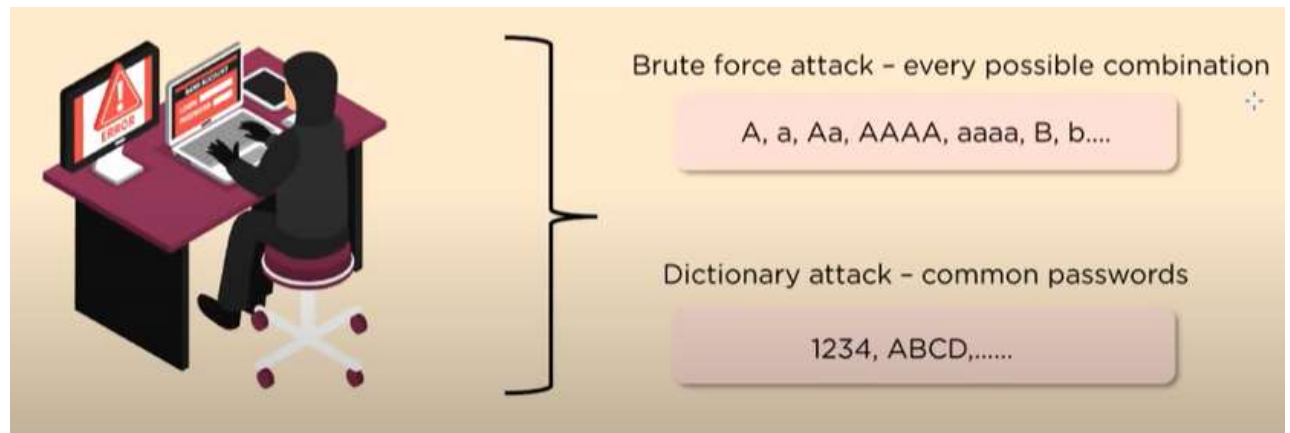
A Denial of Service attacks' motive is to flood systems and networks with traffic to exhaust its resources and bandwidth. By doing so, it is unable to cater to legitimate service requests



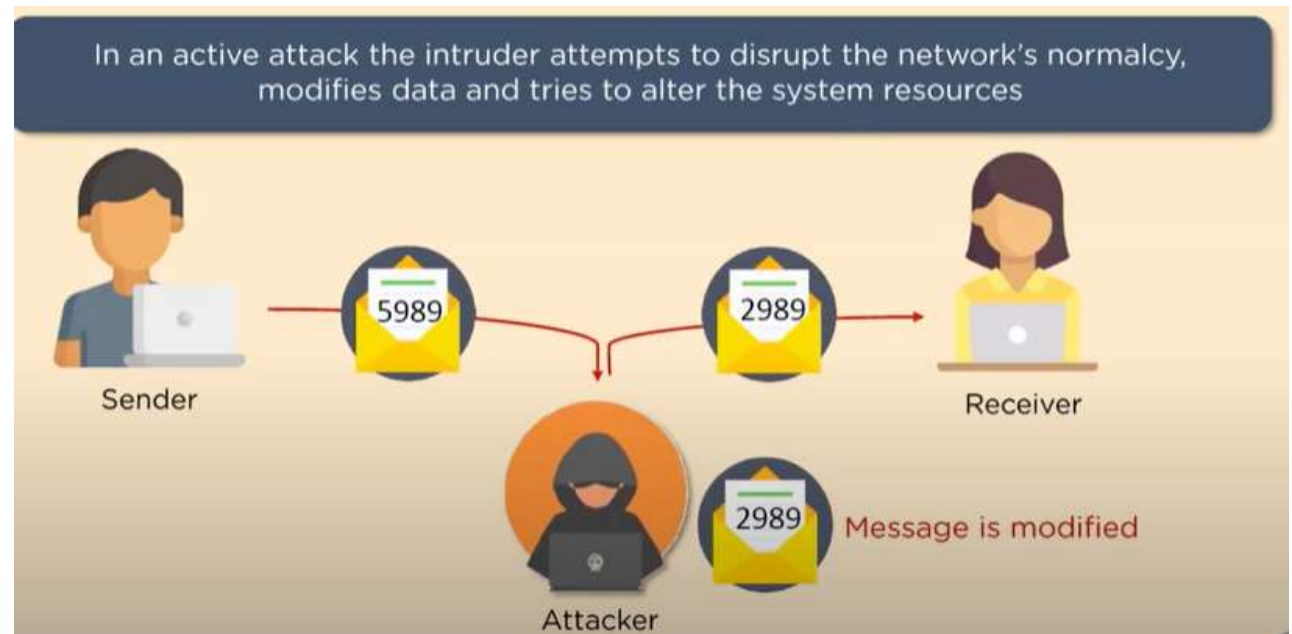
SQL INJECTION ATTACK



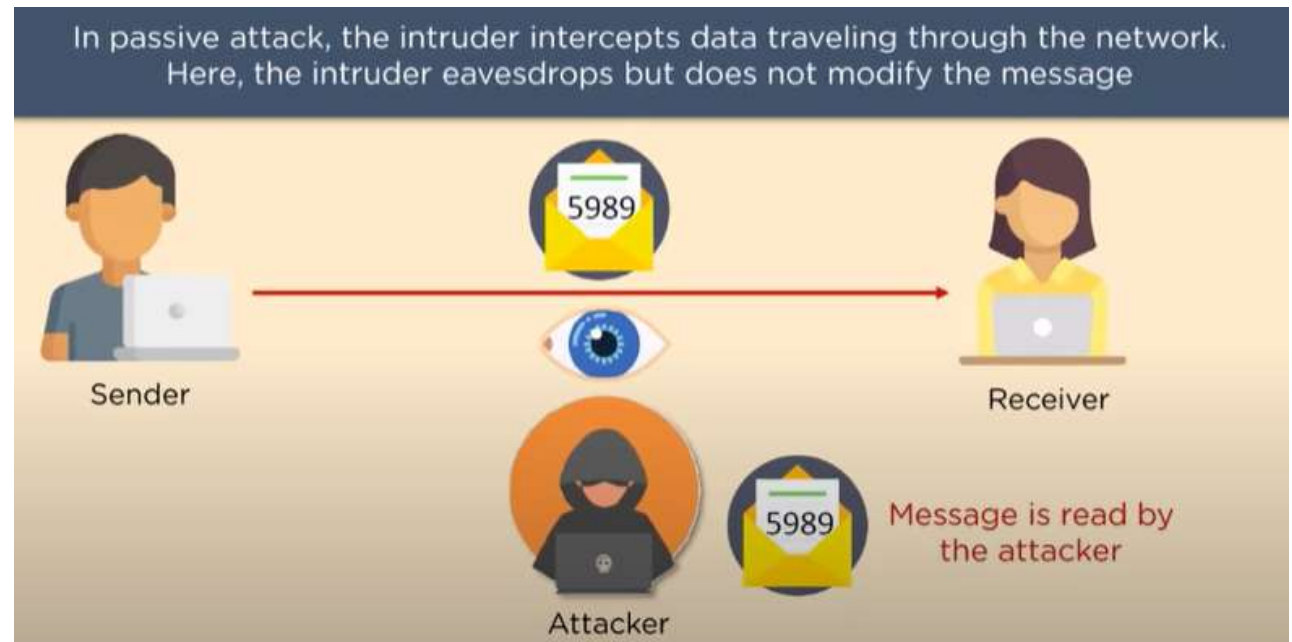
PASSWORD ATTACK



ACTIVE NETWORK ATTACK



PASSIVE NETWORK ATTACK



CYBER SECURITY

Cyber Security refers to the practice of protecting networks, programs, computer systems, and their components from unauthorized digital access and attacks



Cyberattack



Cyber Security

CYBER SECURITY AND INFORMATION SECURITY

Cyber Security and Information Security are different from one another

Information Security

Processes and tools deployed to protect sensitive information



Cyber Security

Set of techniques used to protect the integrity of networks



POLL 4: DO YOU KNOW THE VALUE OF YOUR DATA?

- Yes
 - No
-

POLL 5: DO YOU KNOW WHERE YOUR DATA IS ?

- Yes
- No

POLL 6: DO YOU KNOW WHO HAS THE ACCESS TO YOUR DATA ?

- Yes
 - No
-

POLL 7: DO YOU KNOW WHO IS PROTECTING THE DATA ?

- Yes
 - No
-

POLL 8: DO YOU KNOW HOW TO RESPOND IN CASE THE DATA IS COMPROMISED ?

- Yes
 - No
-

ANSWER THESE 5 KEY QUESTIONS



Do you know value of your data ?



Do you know where your data is?



Do you know who has access to this data?

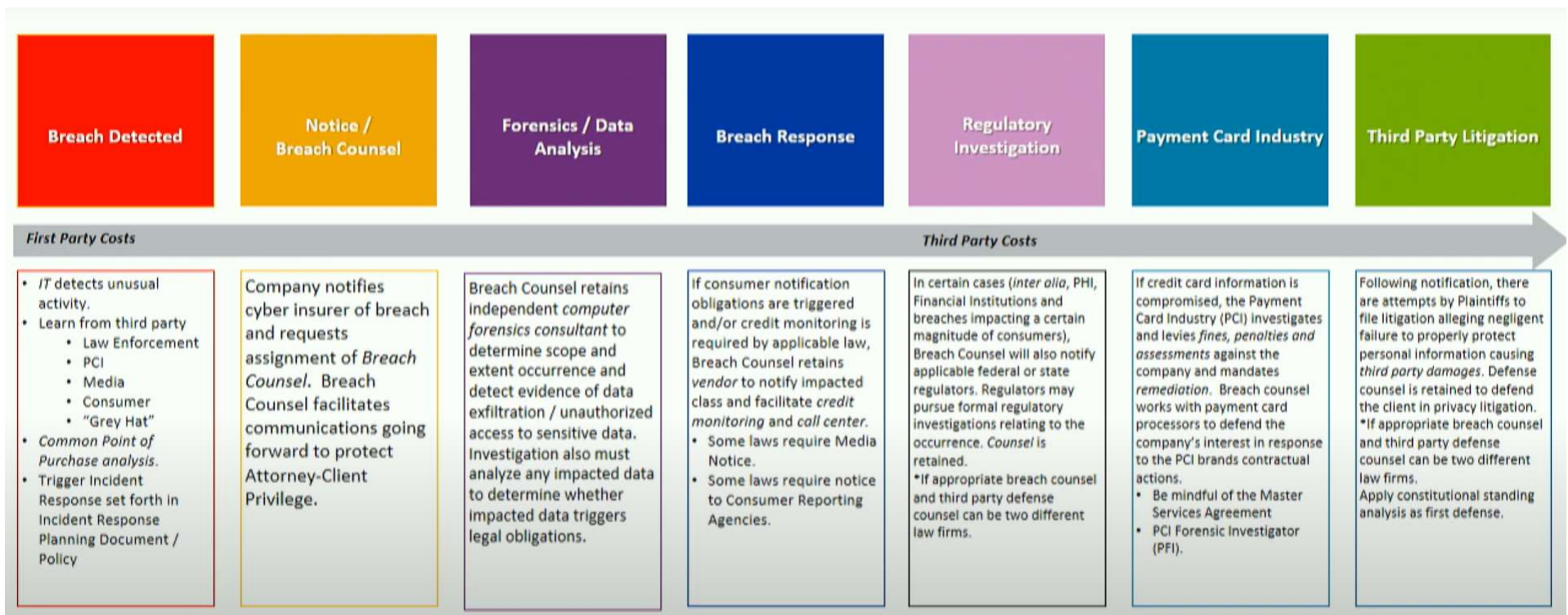


Do you know who is protecting the data ?



Do you know how to respond in case data is compromised ?

LIFECYCLE OF A DATA BREACH



POLL : HAVE YOU EVER HEARD OF NATPETYA ATTACK?

- Yes
 - No
-

STANDALONE CYBER POLICY COVERAGE

First Party

- Incident Response/ Crisis Management Costs
- Forensics / IT / Data Recovery / Systems Restoration / E-Discovery
- Legal
- Notification / Call-center
- Public Relations
- Business Interruption / Contingent Business Interruption
- Digital Extortion

Third Party

- Broad coverage for failure to protect data
- Vicarious liability coverage for vendors (Business Associates, Tech Providers (Saas, PaaS, etc)).
- Regulatory fines & penalties
- Civil & Class Action Defense

Other Benefits

- “Other Insurance” Clause may make professional liability policy primary
- Preserves Errors & Omissions policy limits for professional Liability claims rather than data breaches
- Cyber policies generally have lower deductibles
- “Primary / noncontributory” language is being added to some cyber policies to avoid coverage disputes

POSSIBLE EXPOSURE MEASURES



CRITERIA FOR EXPOSURE

Simplicity

Auditability

Strength of
relationship to
losses

Stability

Legal
Determinability

MAJOR COVERAGES



PRIVACY LIABILITY



NETWORK
SECURITY LIABILITY



CYBER EVENT
RESPONSE

FOCUS: PRIVACY LIABILITY COVERAGE

1

Losses : Damage,
Defense Costs and
Fines

2

Bad exposure
measures : Harm
Caused, Preventive
measures

3

Possible Measures :
Class Size or
related proxy

CLASS SIZE

01

Two types: Service providers(Employees) and Service receivers(Customers)

02

Customers uniquely identified and those not uniquely identified .

03

Employee vs customer class size

ACTUARIAL CHALLENGES



Data and standardization issues



No geographical Limitation



Network risk from External
Perspective



The Human element

ACTUARIAL CHALLENGES



Correlation of attacks



Actuarial Paradox



Cyber Catastrophe



Technology Evolution and Silent Coverage

QUESTIONS AND ANSWERS