Imagenz

Cybersecurity in the New Normal

Ash Ang

Managing Information Security Risk

Organizations need to prove they are secure and compliant to key stakeholders like their customers, regulators or their board. Simply put, we help provide that proof. Imagenz security services helps our customers to achieve that in using our approach of Secure, Test, Aware and Protect i.e. **S.T.A.P** approaches since 2016. Customers ranges from NASDAQ listed company, MNC's, GLC's, Non-profit organizations to SME's

Secure

Consulting As A Service with our proven framework to achieve ISO 27001 & ISO 27701 certification

Test

VAPT Test & Network Vulnerability Assessment

Aware

Online Security Training & customize cyber security awareness training

Protect

Enterprise grade cybersecurity and defense solution to protect your information assets

STELLAR CYBER

RIDGE SECURITY

CloudGuard

Harmony

Quantum

CHECK POINT

Imagenz

Overview

- New demand on companies
- Sanction risk and cybersecurity
- Cyber Kill Chain
- Commonly used cyber attack in data breach
- How much security is enough?
- Ransomware to pay or not to pay?

Speaker

Ash Ang
Principal Consultant

- Certified Ethical Hacker
- Certified ISO/IEC 27001 Lead auditor
- Certified Information Security Manager
- ISO/IEC 27001 internal auditor trainer
- Experience in IT Mgt & Services, IT infra, System Engineering, IT audit, Data governance in MNC
- Risk assessment with ISO/IEC 27001, ISO 27002, MAS TRM

Imagenz

Current environment putting new demand on companies

Can we learn faster and be smarter than the hackers

Digital Transformation & New Technology

Mobile collaboration /BYOD

Digital payment /Cloud SaaS

Ever Increasing Threats

WFH

Supply Chain Attack

Social Business blurring "social" identities

Sanction Risks

Potential Impact

Data or device theft

Malware infection
Loss of productivity

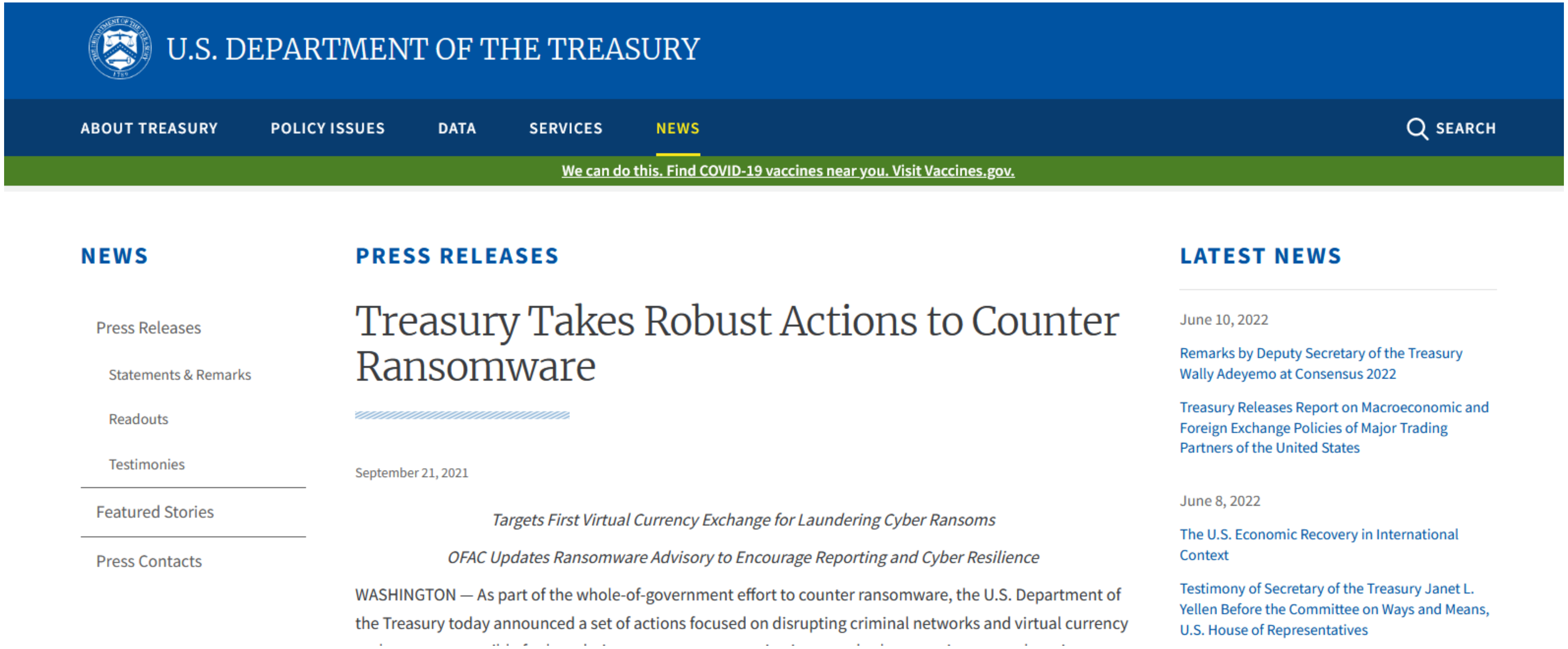
Regulatory fines
$$$$

Data Breach

Skilled Security Professionals

Imagenz

Ransomware Payment and Sanction Risk



PRESS RELEASES

Treasury Takes Robust Actions to Counter Ransomware

September 21, 2021

Targets First Virtual Currency Exchange for Laundering Cyber Ransoms

OFAC Updates Ransomware Advisory to Encourage Reporting and Cyber Resilience

WASHINGTON — As part of the whole-of-government effort to counter ransomware, the U.S. Department of the Treasury today announced a set of actions focused on disrupting criminal networks and virtual currency

LATEST NEWS

June 10, 2022

Remarks by Deputy Secretary of the Treasury Wally Adeyemo at Consensus 2022

Treasury Releases Report on Macroeconomic and Foreign Exchange Policies of Major Trading Partners of the United States

June 8, 2022

The U.S. Economic Recovery in International Context

Testimony of Secretary of the Treasury Janet L. Yellen Before the Committee on Ways and Means, U.S. House of Representatives

Ransomware Statistics 2021

$ 170k

Average Ransom Payout

11 secs

Ransomware Attack Every (Estimate)

$ 1.85 Million

Average Cost of Recovery

21 days

Average Downtime after Attack

$ 40 Million

Largest Ransom Payout

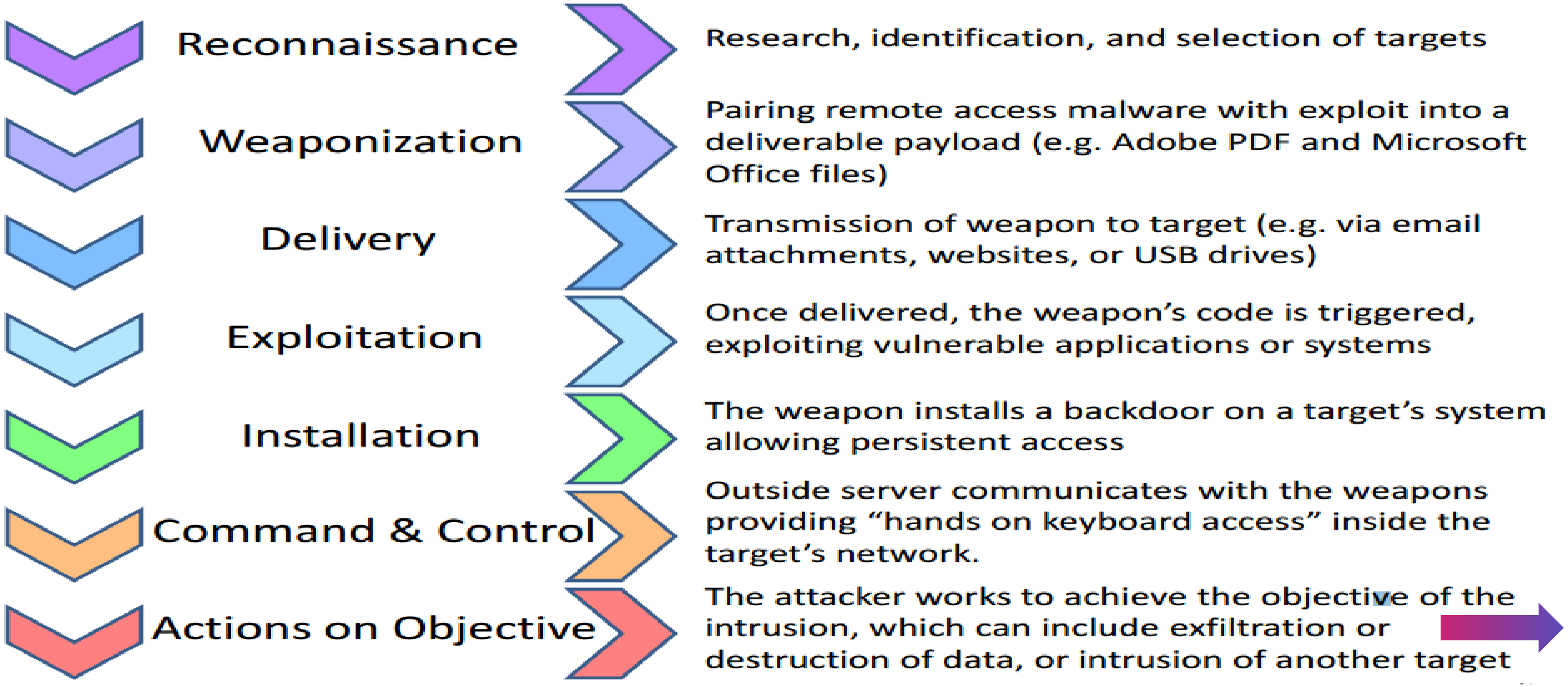
42%

Companies with Cyber insurance indicated it covered small part of damages

Source of information: https://www.varonis.com/blog/ransomware-statistics-2021

Imagenz

Cyber Kill Chain



Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon’s code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target’s system allowing persistent access
Command & Control	Outside server communicates with the weapons providing “hands on keyboard access” inside the target’s network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

280 days

Avg. Time to Identify and Contain

“If you know the enemy and know yourself (*what you have and what you need to defense*), you need not fear the result of a hundred battles. — Sun Tzu

Imagenz

Commonly used cyber attack in data breach

Ransomware Target: Enterprise companies & businesses	• Lock down access to vital data (avg. 170k USD payment) • Fee is demanded commonly in cryptocurrency
Phishing Target: Individual & businesses	• Hacker gain access to sensitive or confidential information
Denial of Service (DoS) Target: Sites or services hosted on high-profile web servers such as banks	• Make machine or network unavailable • Flood targeted machine or resource with requests

Protecting the Business

- Defense-in-depth
- Risks and vulnerabilities
- Proactive vs reactive security
- Legal compliance

280 days

Avg. Time to Identify
and Contain a data breach

How much Security is Enough?

- Maintain security while ensuring profitability
- Adopt risk-based approach to determine the security controls needed

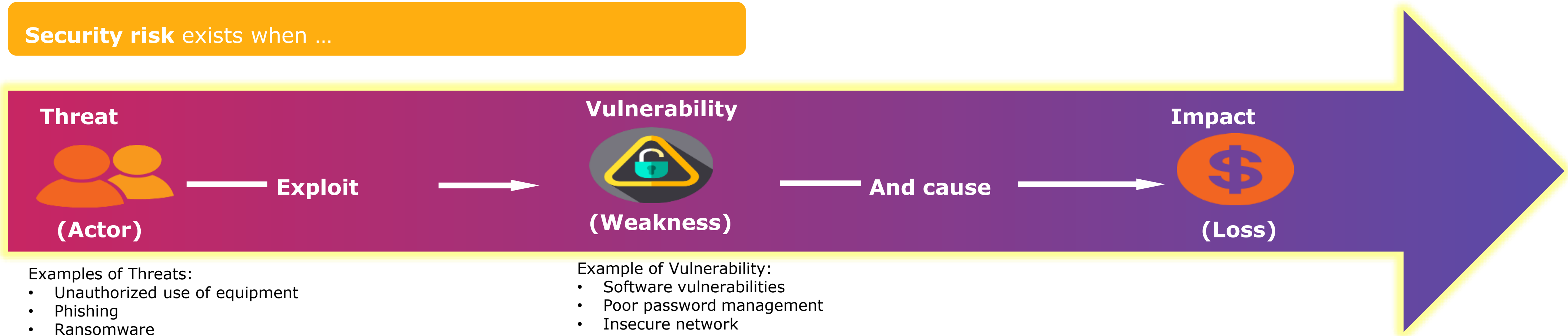
Imagenz

Think like a Security Expert – Continually monitor assets for the likelihood and severity of cyberattacks

Security Risk Management is the application of **control** to detect and block the threat, to detect and fix a vulnerability, or to respond to incidents (impacts) when all else fails.

Security risk exists when …

What will Happen if…..



Examples of Threats:

- Unauthorized use of equipment
- Phishing
- Ransomware
- Denial of Service Attack
- Data Breaches

Example of Vulnerability:

- Software vulnerabilities
- Poor password management
- Insecure network
- Lack of security testing
- Lack of security awareness
- Lack of established monitoring mechanism for security breaches

Questions to Ask

Threats
What are the losses if our most important assets were compromised? i.e. loss of confidentiality, integrity, data access

Actions
What actions would be required to mitigate and respond to a breach i.e. remediation, respond plan

Cost
How must would it cost to address problems associated with breaches?

3 steps to get secured!

1. Identify what information assets you own

(KNOW WHAT YOU HAVE)

   a. *How critical it is to protect it; Low, Medium, High Risk*
   b. *Risk level and Impact if lost or breached, measure in terms of dollars!*

2. Identify what the type of protection needed based on criticality and impact
(UPDATE YOUR DEFENSE)

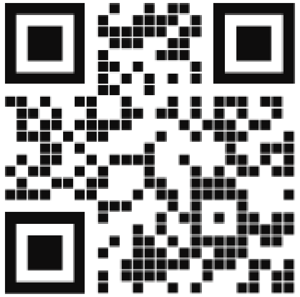
   a. *Defense in depth (network protection, endpoint protection, encryption, Web Application Firewalls)*
   b. *Monitoring (e.g. Endpoint Detection & Response)*

3. Awareness training for your team

Imagenz

Awareness Training Videos

Help to Subscribe, Share and Like us on Facebook, Youtube



THANK YOU!

Ash Ang

E: ash@imagenz.net

M: 91087809

https://imagenz.net