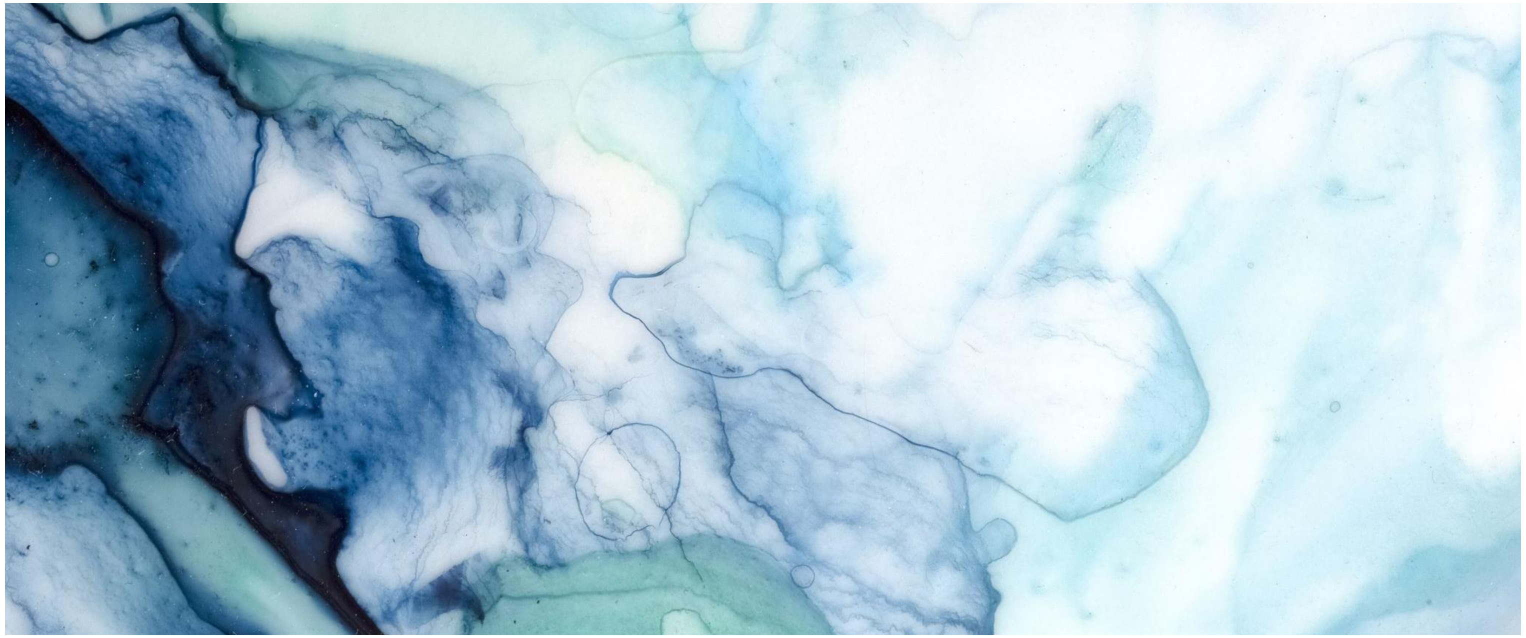


Public Private Partnerships

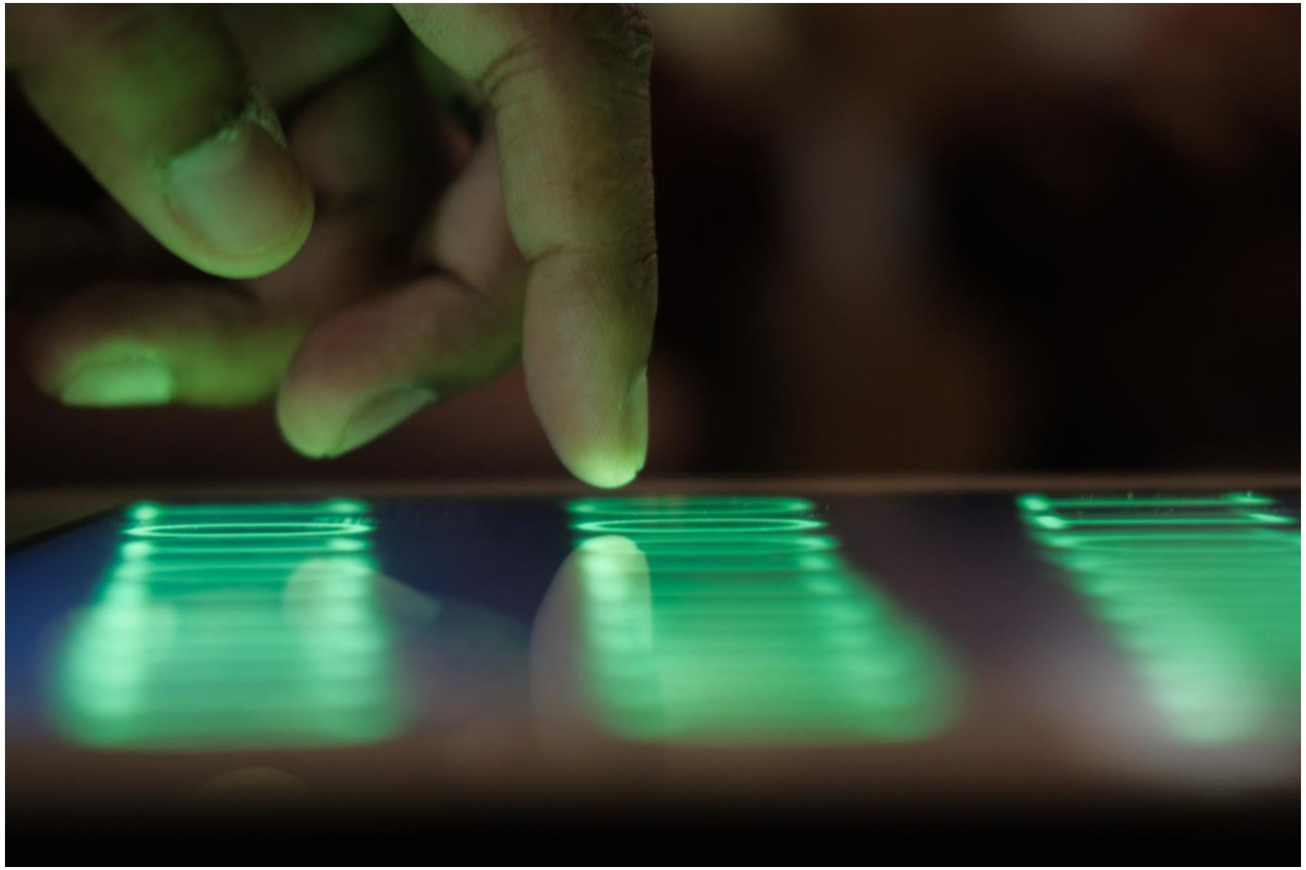
IMPORTANCE OF PPP/S IN CYBERSECURITY

LORRI JANSSEN-ANESSI
DIR, EXT CYBER ASSESSMENTS
BLUEVOYANT

- Introduction
- The Problem
- Solutions (*Public-Private Partnerships*)
- Challenges

The PROBLEM

Cyberattacks are more common than ever



Threat actors only need to find **one weakness** to exploit,
while cyber defenders must attempt to safeguard **everything**, ensuring not even one weakness is exposed.

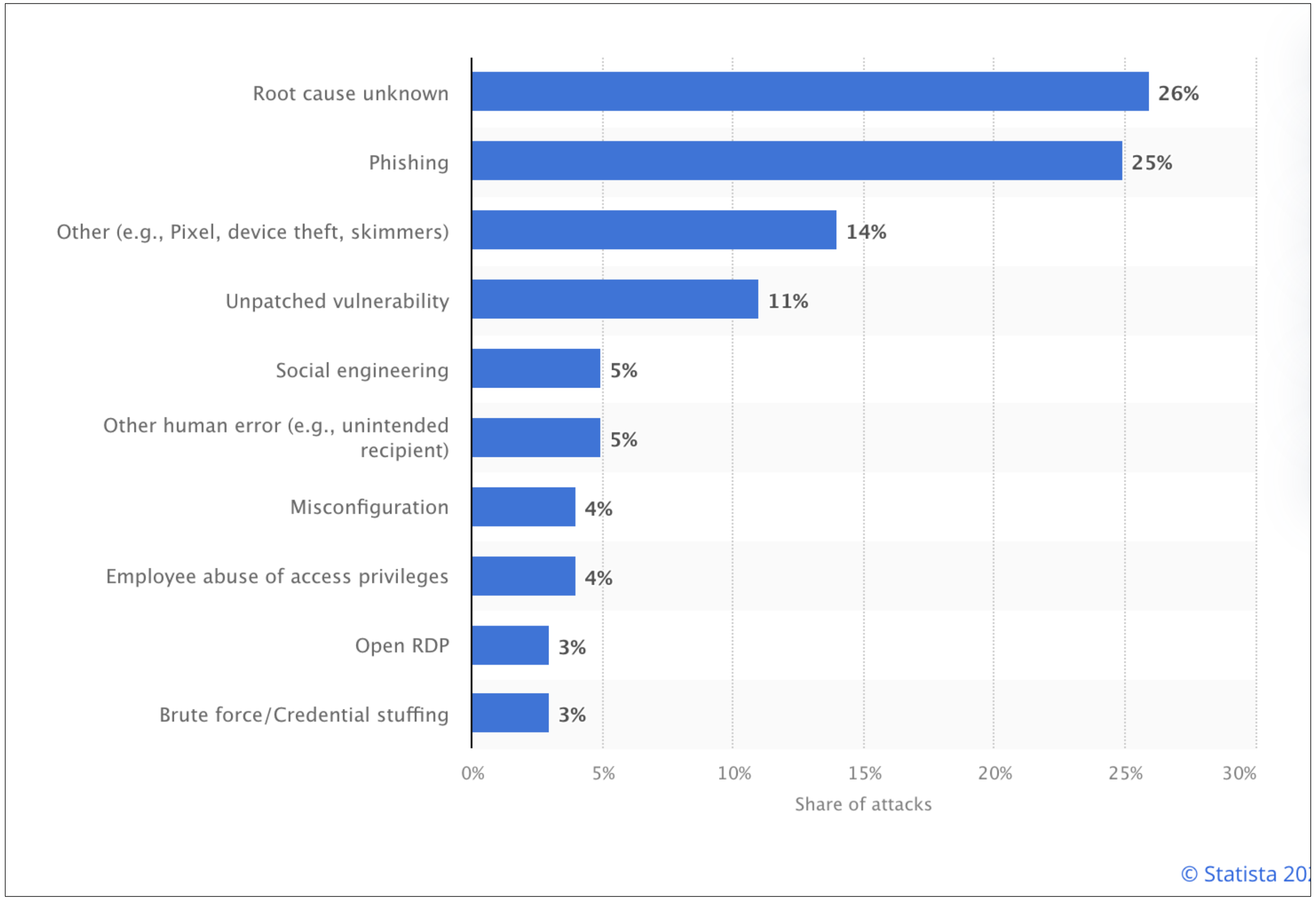
Most Common Types of Cyber Threats

PHISHING →

DEVICE THEFT →

UNPATCHED VULNERABILITY →

Root Causes of Attacks



© Statista 20

The 7 Stages of a Cyber Attack

https://www.weforum.org/videos/these-are-7-stages-of-a-cyberattack-used-by-hackers

Critical Cybersecurity Issues

Cyberattacks are happening more frequently and are increasingly costly and damaging

Cybersecurity professionals are in a continuous battle to prevent attacks and defend their infrastructure

In order to thwart cyber attacks companies need a lot of data and information

Recent incidents, such as Solarwinds and Log4Shell, showed the efficacy of public-private cooperation in response to large-scale incidents

Supply chain attacks, ransomware, and ubiquitous phishing campaigns occur daily

Security teams are overloaded by time-consuming manual processes, against constantly new novel attacks, with little to no time to be proactive

The SOLUTION (*at least some of them*)

Short-term Solutions

Patching to the most current and non-vulnerable version of software, hardware, operating systems, etc

Basic Cyber Hygiene implementations

Increase hiring for Cybersecurity jobs *

Expand cooperation with global allies

Build on current PPP organizations to increase information sharing and collaboration

(In the US, some estimates suggest ~ 597,000 cybersecurity openings, while the existing workforce can only fill 2/3 of cybersecurity jobs.)

Strategic Solutions

- Public-Private Partnerships expansion
- Solutions born in tech companies can help remove barriers and streamline data-sharing across government agencies
- Governments bring crucial knowledge and context to help make sense of the threats and data — and can help elevate the topic to the highest-level agendas.
- Along with promoting knowledge and information sharing, collaboration between public and private sector entities is necessary to develop tomorrow’s cybersecurity workforce

Current PPP Cyber-focused Organizations

NIST CYBERSECURITY FRAMEWORK

MITRE ENGENUITY™

JOINT CYBER DEFENSE COLLABORATIVE

WORLD ECONOMIC FORUM

NIAP

NATO OTAN

NATO Communications and Information Agency NCI AGENCY

CYBER THREAT ALLIANCE

Successful PPP Examples

- **Log4J** - a vulnerability that put at risk up to 93% of cloud environments, threatening the spread of private data and information — the entire world benefited from private-public partnerships working together to stop a bad situation from getting worse

- **SolarWinds** - The SolarWinds Orion attack was detected by the private sector, and the quick engagement of government reaffirms that a robust public-private sector partnership is fundamental to digital security

- **Ukraine** - the private sector worked with organizations both inside and outside of Ukraine to strengthen defensive cyber postures against nation-state cyber-attacks and other malicious activity

BENEFITS of PPP

- Neutral forum where private companies and government can share information expeditiously and privately without competitive advantages
- Enable sharing of data and information quickly and continuously
- US government has acted as a clearing place for accurate and timely information, where companies could turn to for up-to-date information
- Private companies and governments work together with mutual priorities and the right incentives
- Cyber actors are not limited by borders, and neither should governments or cyber defenders be
- Create new partnerships, work to demonstrate how to make the digital world safer and more resilient for everyone through collaboration
- Help Small and Medium Sized Businesses improve their cyber hygiene and Cybersecurity posture

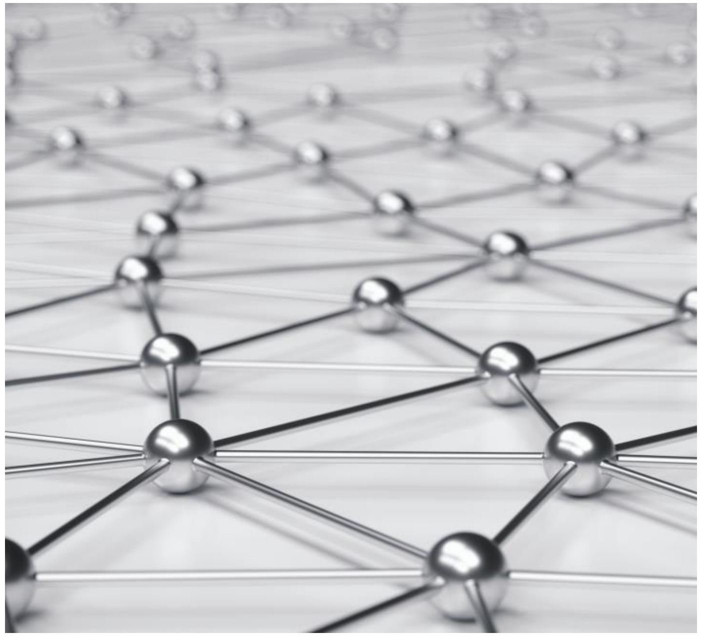
The CHALLENGES

Current CHALLENGES

- Unclear responsibilities
- Solutions constrained by existing standards, methodologies, and limited exposure to best practices under traditional approaches
- Companies suffer from inadequate internal resources and personnel to ensure progress and daily decision making in a timely manner
- Voluntary government regulation is unpopular
- Cyber attacks can originate domestically or internationally, with motives ranging from financial gain to state-sponsored, low-level warfare
- Threat actors continuously increase their capability resulting in increased ransomware, data theft, and zero-day exploitation activities
- There is no easy way to stop cyber attacksThere is no easy way to stop cyber attacks
- There are not enough workforce personnel to fill the current positions

No matter how strong partnerships are believed to be, there is always more work to be done when organizations work together to stay ahead of threat actors.

By strengthening these relationships, the entire cybersecurity community can become more resilient and effective at stopping cybercrime on a global scale.



QUESTIONS

ACRONYMS

JCDC: CISA sponsored, a place for defenders from the public and private sectors, including Splunk, that are united by common goals to proactively gather, analyze and share actionable cyber risk information.

CISA: US Cybersecurity and Infrastructure Security Agency

WEC - World Economic Forum: provide the opportunity to share knowledge and forge long-term commitments and global collaboration across business, civil society and government in pursuit of a shared goal

NIAP - National Information Assurance Partnership - Oversees Evaluations of Commercial IT Products for Use in National Security ***Systems***

CTA – Cyber Threat Alliance - The Cyber Threat Alliance (CTA) is a 501(c)(6) non-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity

ACRONYMS

MITRE ENGINUITY: Comprised of participant organizations from around the globe with highly sophisticated security teams, the Center builds on MITRE ATT&CK®, an important foundation for threat-informed defense used by security teams and vendors in their enterprise security operations.