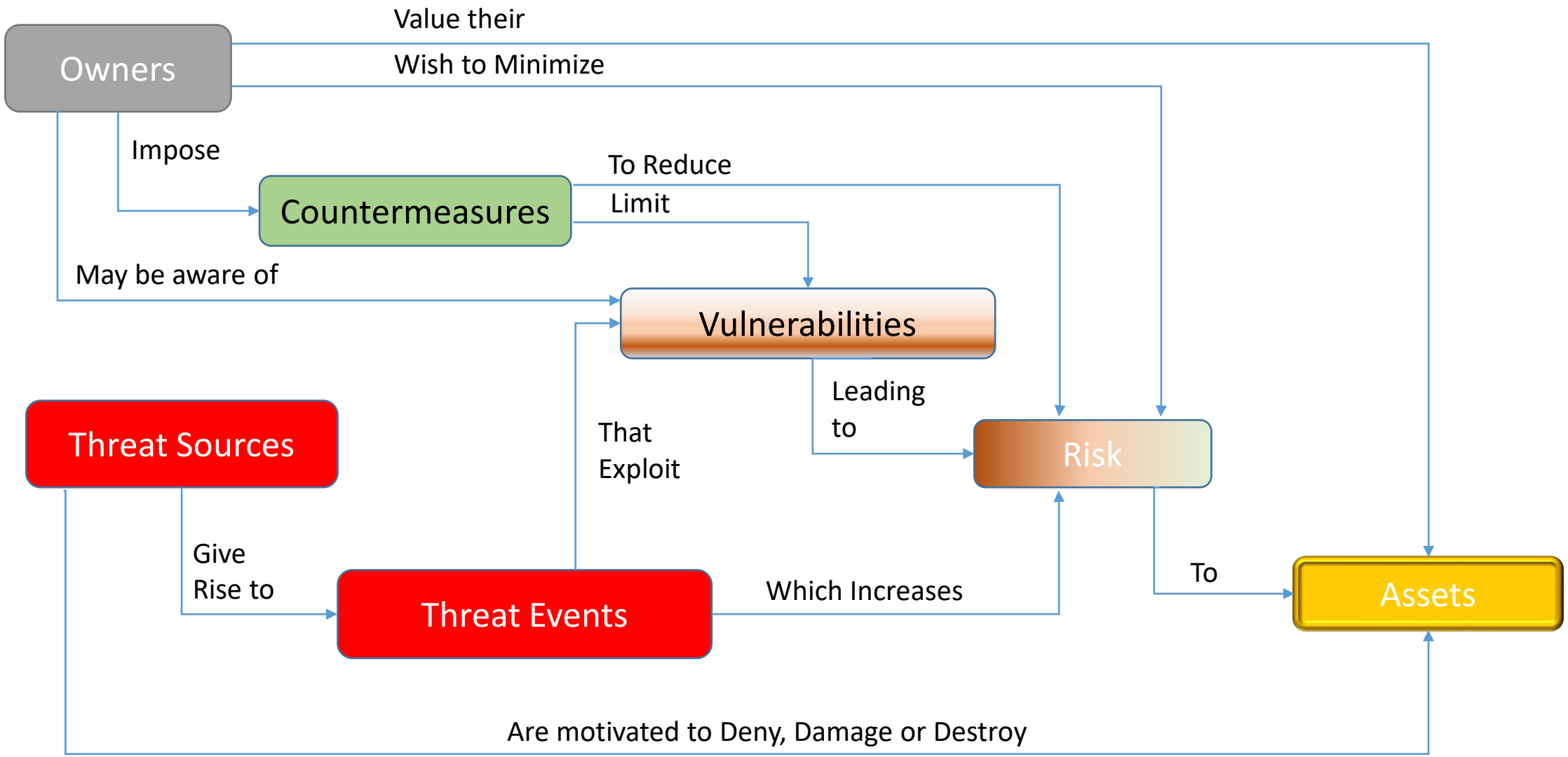
CYBERSECURITY FUNDAMENTALS & HYGIENE

#BeCyberSmart

What Cybersecurity Does (In a Nutshell)



THE ROAD TO CYBERSECURITY

INFOSEC

85%
of breaches involved a human element

99.9%
of discovered mobile malware are hosted by third-party app stores

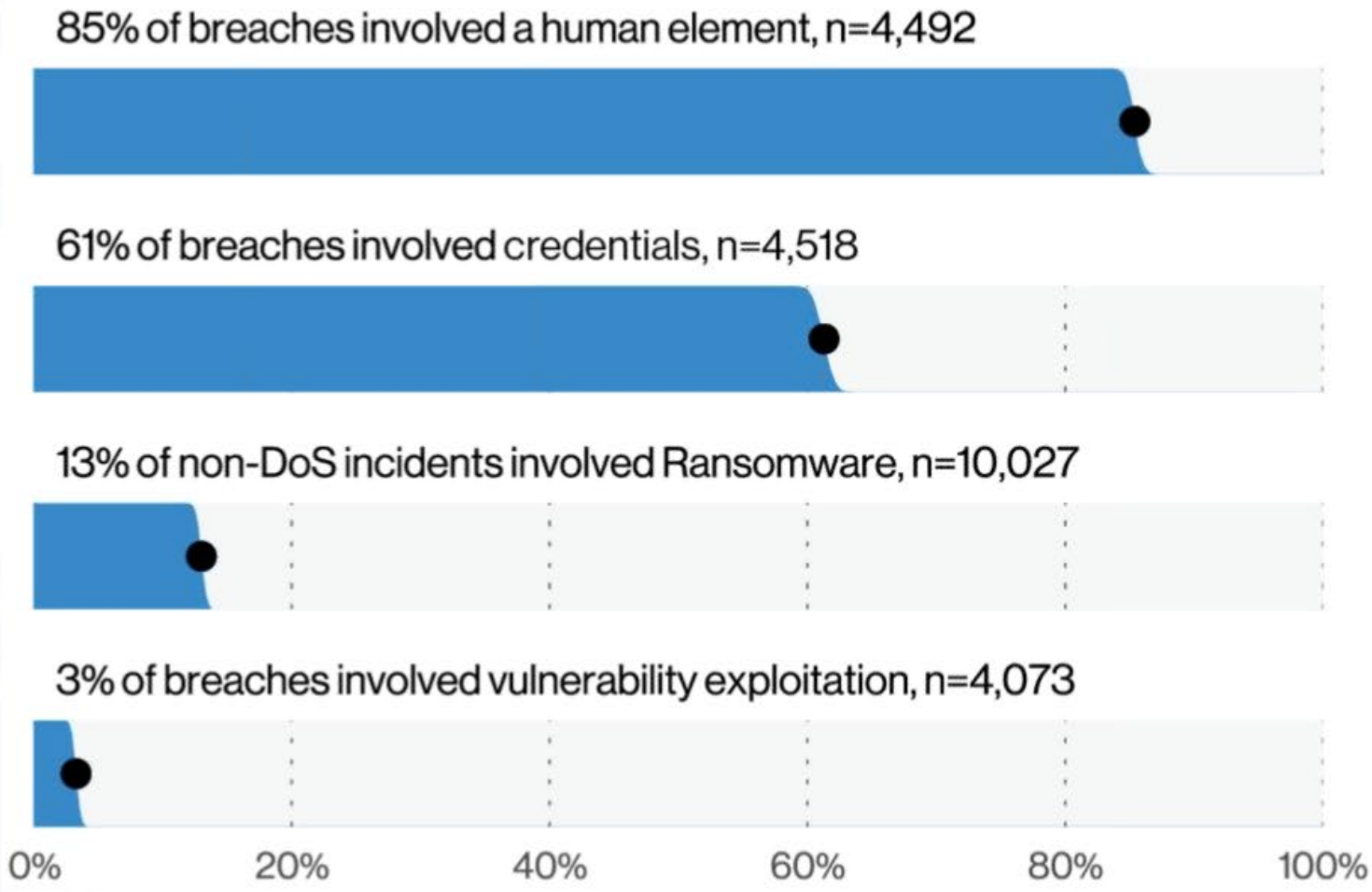
By 2017, Ransomware damage costs exceeded
$5 billion

60%
of data breaches are caused by insider threats (Goldstein, 2020)

98%
of cyber attacks rely on social engineering

https://www.dataprivacyandsecurityinsider.com/2021/05/verizon-2021-data-breach-investigations-report-released/
https://purplesec.us/resources/cyber-security-statistics/
https://financesonline.com/insider-threat-statistics/

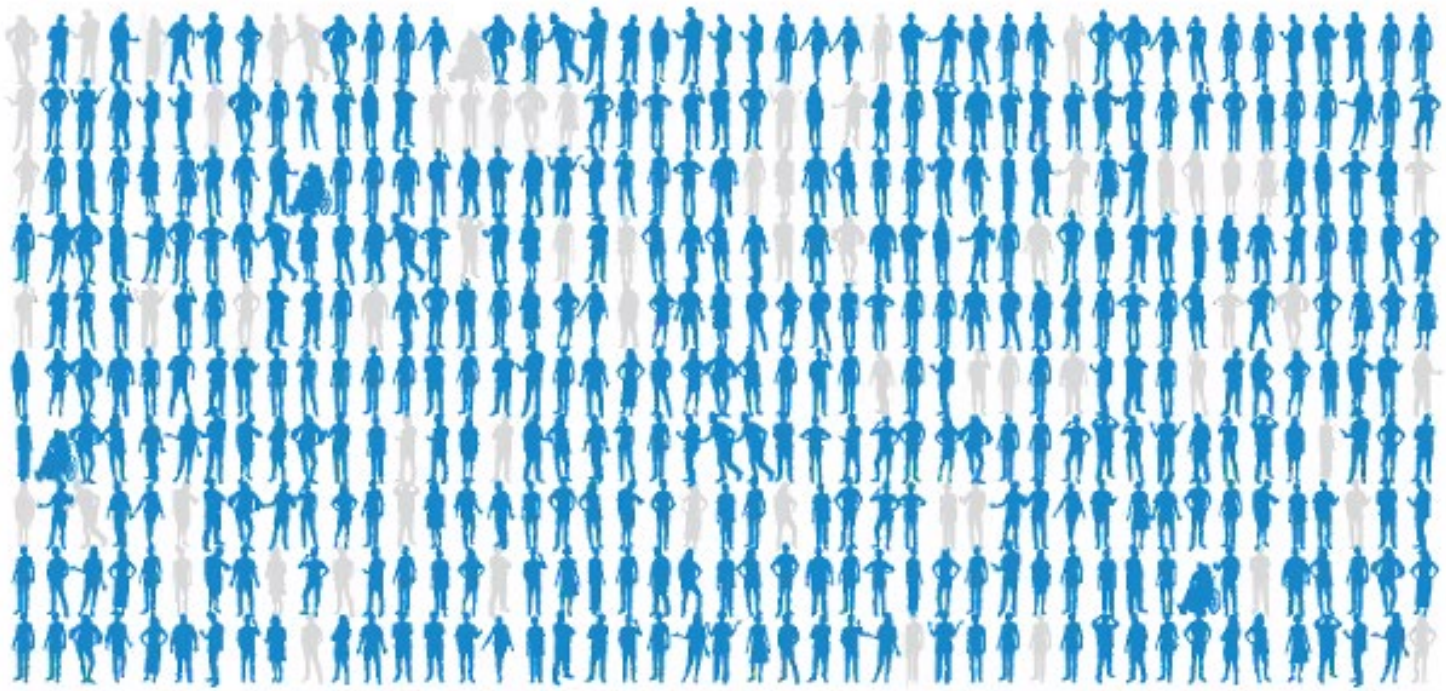
People Are Being Attacked at Unprecedented Levels



DBIR
2021 Data Breach Investigations Report

Human Risk?

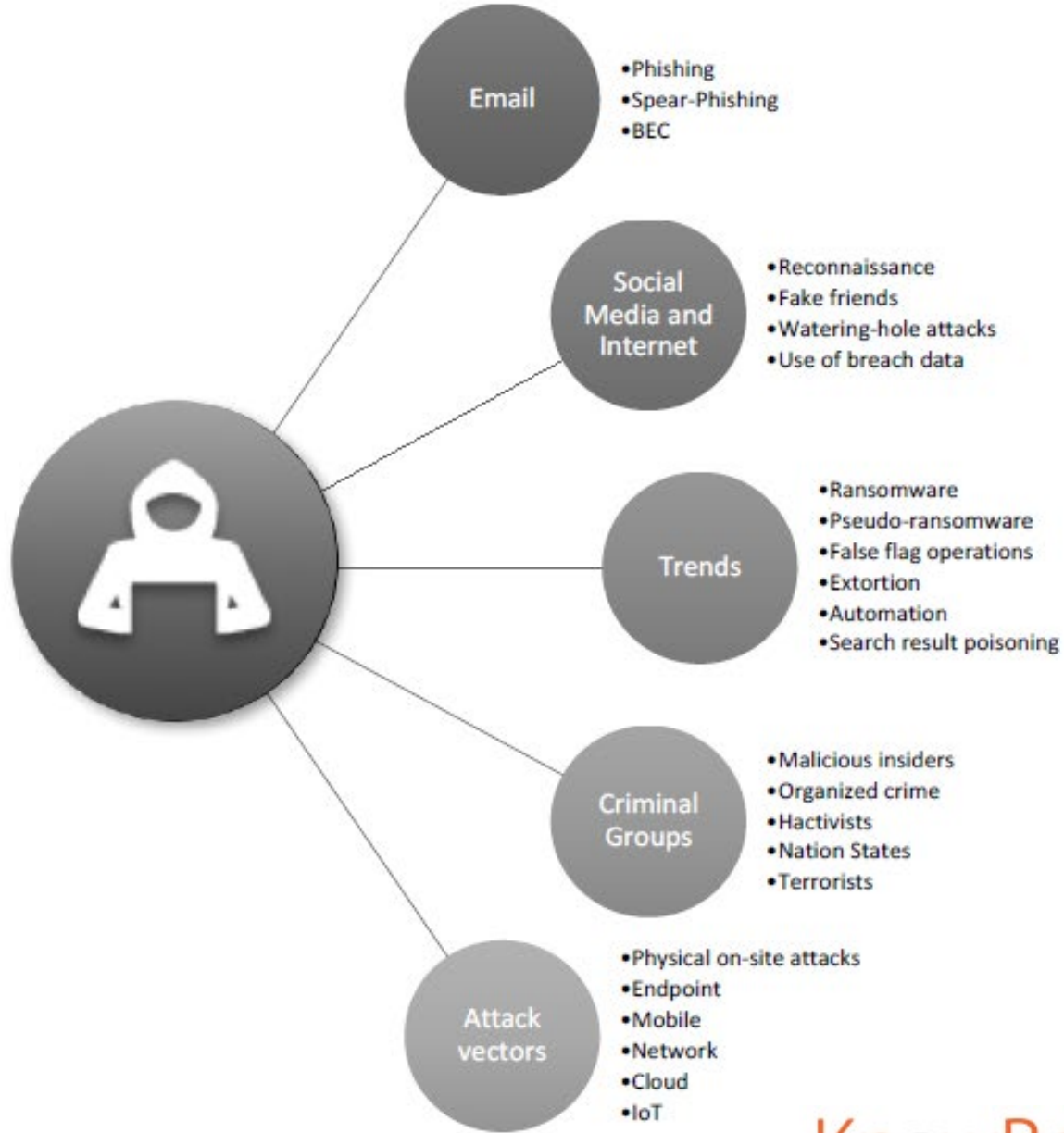
85% of breaches involved the human element.



Each person represents 10 breaches.

And only 3% involved vulnerability exploitation

Attackers go for the low-hanging fruit: *humans*



KnowBe4
Human error. Conquered.

WHY DO WE CARE?
WHAT ARE THE CONSEQUENCES?

- Institutional Risk
  - When bad actors successfully obtain user credentials for some systems, they not only gain access to the accounts that use the credentials, but they can potentially access high-value institutional data such as social security numbers, banking information (such as direct deposit), health information, research, student data, etc.
  - Internet or financial services companies can blacklist institutions, resulting in reputational damage.
  - When an institution is blacklisted, its ability to communicate with members of the community (prospective students, student athletes, faculty and staff; alumni, partners, friends, etc.) is diminished.
  - We use the valuable time of staff members (IT, legal, HR and financial departments) to address the issues caused by phishing and by blacklisting, rather than applying their skills to more productive work.

MOVIE TIME!

HP HAS PRODUCED A DIGITAL SERIES CALLED “THE WOLF”, A CAMPAIGN DESIGNED TO RAISE AWARENESS OF CYBERSECURITY IN THE WORKPLACE.

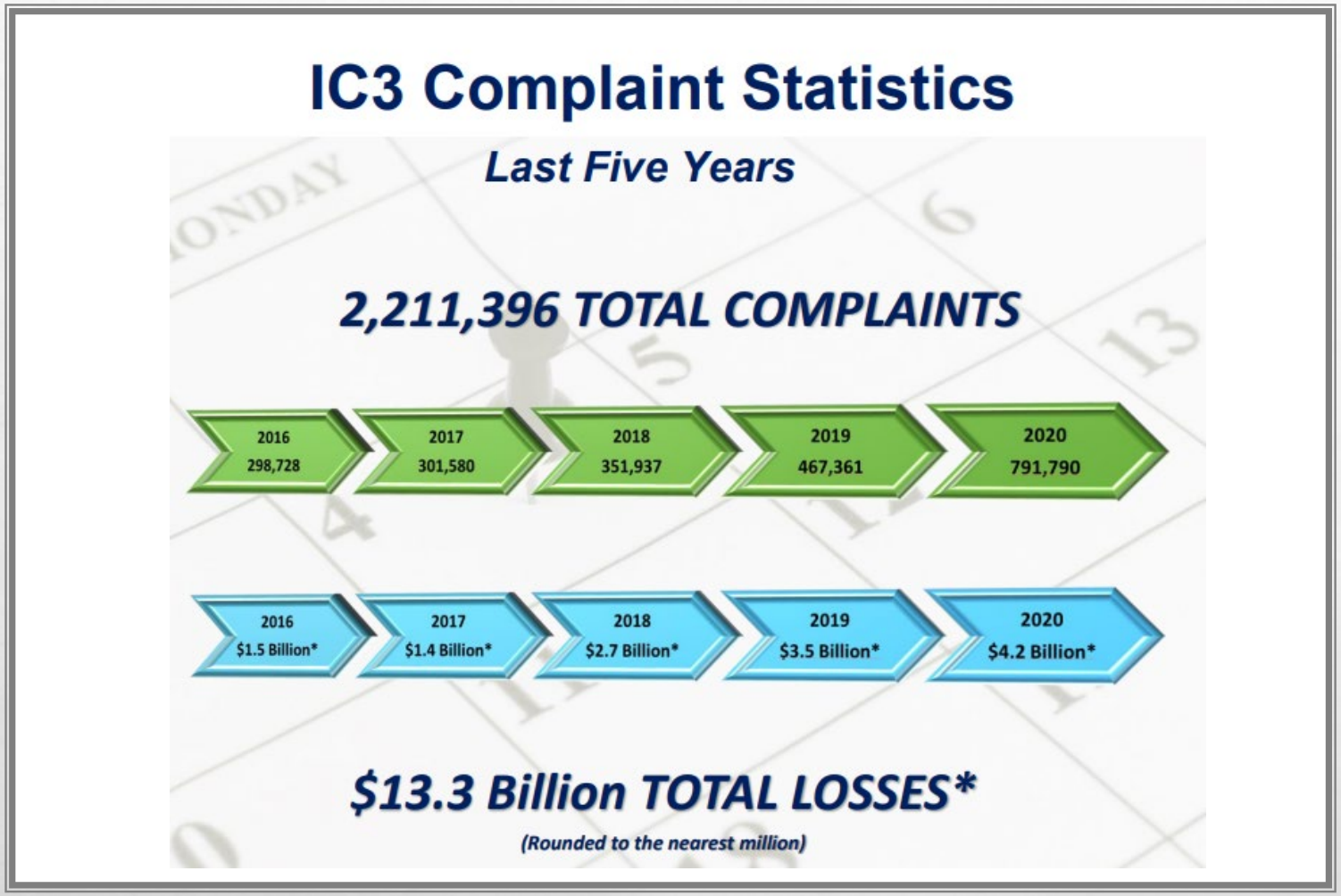
- HTTPS://CLIOS.COM/AWARDS/WINNER/BRANDED-CONTENT/HP/THE-WOLF-THE-HUNT-CONTINUES-50583

TAKE AWAYS

- SMART PHONES LOCK DEVICES WHEN WALKING AWAY? UTHSC HAS IMPLEMENTED A 10-MINUTE INACTIVITY LOCK SCREEN
- NURSE LEAVING HER DESK, MAY NOT HAPPEN OFTEN THESE DAYS DEPENDING ON OFFICE SIZE, BUT NEXT TIME YOU GO TO THE DOCTOR OR ANY HEALTHCARE FACILITY, WHAT INFORMATION DO THEY ASK YOU TO SAY OUT LOUD TO VERIFY YOU ARE WHO YOU SAY YOU ARE?
- “OLD PC” – REITERATES THE NEED TO KEEP OS AND APPS UP-TO-DATE
- “SORRY DAVE – IT’S NOT PERSONAL” – MOST OF THE TIME, THESE ATTACKS AREN’T PERSONAL, THEY ARE A BUSINESS TRANSACTION FOR THE BAD ACTORS.

KEY ELEMENTS TO GOOD CYBER HYGIENE

- STRONG ACCESS CONTROLS
  - PASSWORDS/PASS PHRASES
  - BIOMETRICS
  - KEY CARDS
  - PHYSICAL SECURITY
- KEEP AN INVENTORY OF HARDWARE AND SOFTWARE
- BACK UP YOUR DATA / ENCRYPT YOUR DATA
- USE MULTI-FACTOR AUTHENTICATION
- UPDATE SOFTWARE / KEEP IT PATCHED
- KNOW HOW TO SPOT PHISHES AND OTHER SOCIAL ENGINEERING TACTICS
- ENSURE ANTIVIRUS AND ANTIMALWARE SOFTWARE IS PROPERLY INSTALLED



FBI'S INTERNET CRIME COMPLAINT CENTER (IC3)

- RECOVERY ASSET TEAM (RAT) FUNCTIONS AS A LIAISON BETWEEN LAW ENFORCEMENT AND FINANCIAL INTUITIONS

Success in 2020

Incidents: 1,303

Losses: $462,967,963.72

Frozen: $380,211,432.04

Success Rate: 82%

WORKING REMOTE

The pandemic brought challenges and opportunities.

Cybersecurity became more about protecting data instead of a perimeter.

This era didn't become just "work from home" but literally "work from anywhere (with internet connectivity)".

CYBERSECURITY CHALLENGES IN WORKING REMOTELY

- Remote workers often practice poor cybersecurity hygiene.
  - 1 out of 3 employees believe they can get away with riskier security behaviors
  - Almost 40% say their cybersecurity behavior at home is different from when they are at the office
  - Half who claim different behavior said they did so because they felt like they weren't being watched by IT
- Remote workers rely on email and messaging tools which are prone to phishes
- Remote work enables social engineering
  - Frequent interruptions and notifications
  - Basic human traits like curiosity, anxiety and urgency

Tessian – "Have Employees Picked up Bad Security Behaviors?"

A NEW LOOK AT ENDPOINT SECURITY

- **HP CREATED A NEW PRODUCTION EXPLAINING THE PITFALLS OF WORKING FROM HOME.**

- HP WOLF SECURITY: A NEW BREED OF ENDPOINT SECURITY | SECURITY | HP

Final Thoughts

Good cyber hygiene starts with the basics that we mention time and time again:

- Recognize you are a target
- Know how to spot a phishing scam
  - Be careful where you click
- Strong passwords and other access control initiatives
  - Use MFA whenever possible
- Keep systems and apps up-to-date
- Know your classification of data and keep it safe
  - Encrypt your data / drive / machine
- Backup regularly
- Anti-virus / anti-malware protection

CONTACT INFORMATION

Chris Madeksho – Cybersecurity Analyst

mmadeksh@uthsc.edu

901.448.1579

Office of Cybersecurity

itsecurity@uthsc.edu

901.448.1860

https://uthsc.edu/its/cybersecurity/

Questions?