INSIDER THREATS

AI IS RAISING THE STAKES …

HERE'S WHAT YOU CAN DO ABOUT IT

Heather Egan, Orrick
Joe Bonavolonta, Sentinel (Former FBI Senior Executive)
Mike Prado, Department Of Homeland Security
Scot Lippenholz, CrowdStrike

October 24, 2024

orrick

Agenda

- Overview of the Insider Threat Landscape
- Real World Examples – Spotlight on Chollima
- How AI Is Raising the Stakes
- Detection and Investigation
- Tips for Risk Mitigation
- Export Control, Immigration Laws, and Anti-Discrimination Law Considerations
- Overview of DHS and Available Resources

orrick

Overview of the Insider Threat Landscape

Source: Cyber Security & Infrastructure Security Agency

Six Main Types of Insider Threats

Malicious

Negligent

Compromised (unaware - credentials accessed)

Disgruntled

Departing Insider

Third-Party (contractors/vendors)

FBI Typology of *Intentional* Insider Threats

- **Intentional** insider threat
  - Theft – mishandling information, unauthorized disclosure, espionage
  - Manipulation – fraud, sabotage
  - Violence – workplace violence, terrorist activity

- Motivations: **MICE:** Money, Ideology, Coercion, Ego
  - 75% of all insiders are categorized as disenfranchised and angry over a particular issue
  - Examples: John Hanson (FBI), Aldrich Ames (CIA), Edward Snowdon (NSA), Jack Teixeira (Massachusetts Air National Guard)

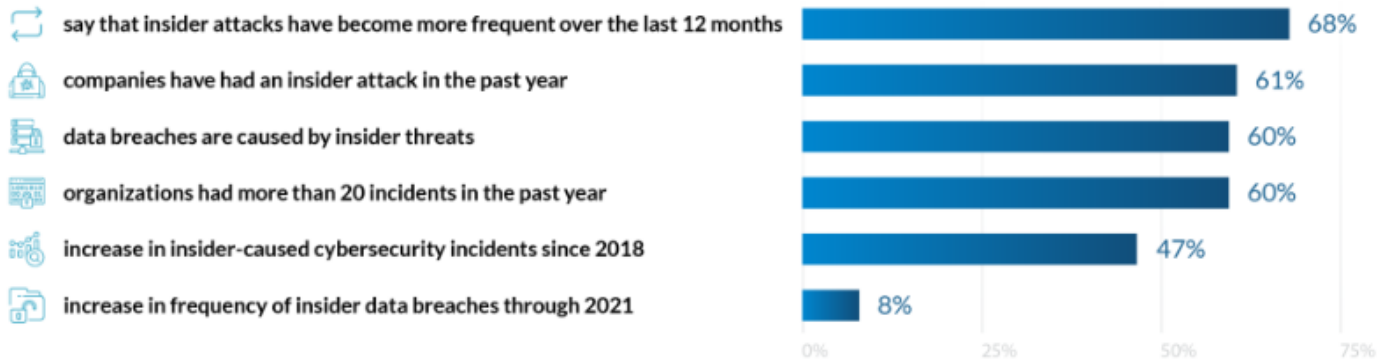
Insider Threat Indicators

Source: https://www.linkedin.com/pulse/insider-threat-internal-sabotage-cpp-ciam-fsyl-risc

A Few Stats:

1 Insider Threat Frequency of Attacks

Sources: Goldstein, CyberSecurity, ObservelT, Shey, Bitglass, IBM

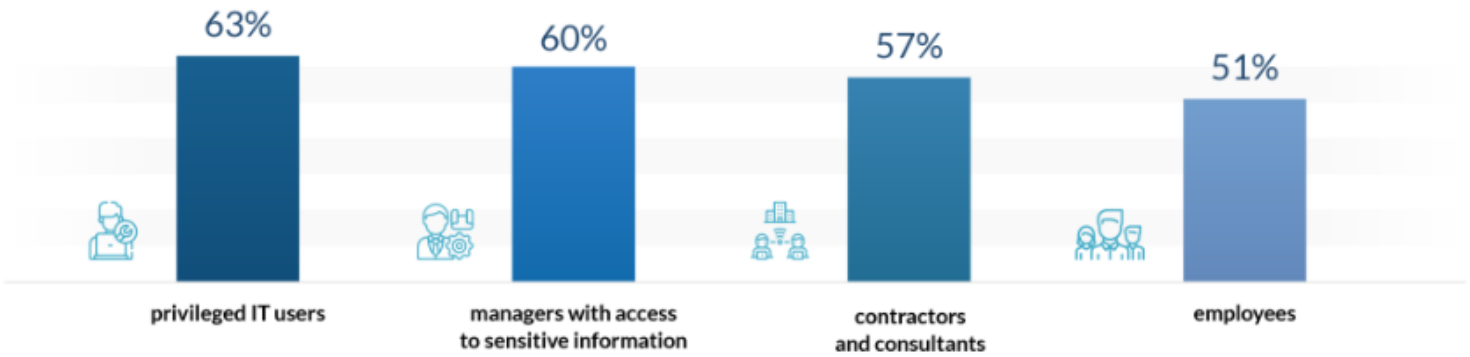


2 Top Motivations for Insider Attacks

Source: Fortinet

3 Top Insider Threat Actors

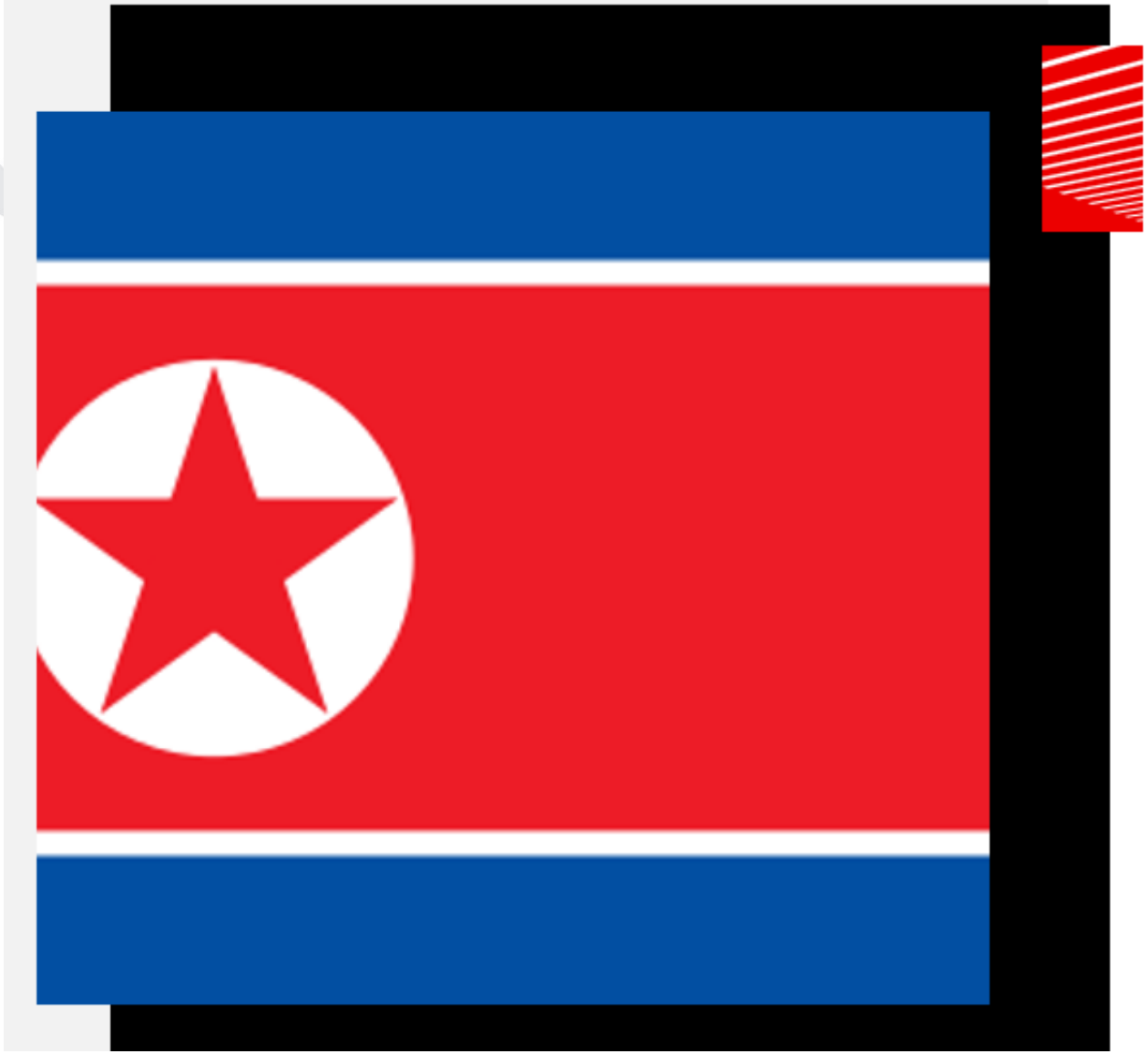
Source: Cybersecurity Insers, Bitglass



Source:
https://financesonline.com/insider-threat-statistics/

How AI is Raising the Stakes

https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us



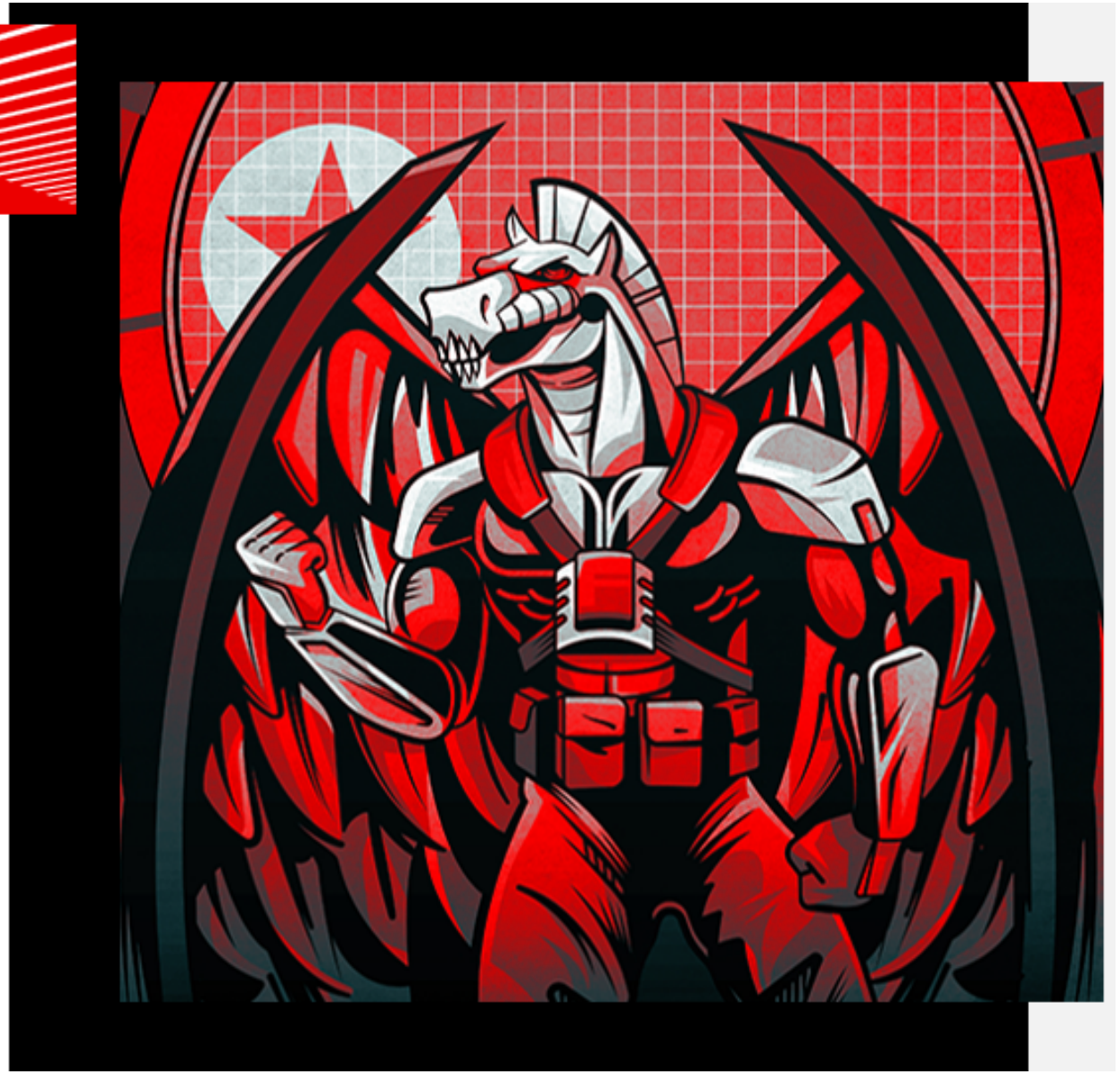
Overview of Famous Chollima

- North Korean State-sponsored & active since at least 2018
- Primarily conducts operations to illicitly obtain freelance or full-time equivalent (FTE) work to funnel money to the DPRK
- Has deployed the custom malware families BeaverTail and InvisibleFerret as well as remote monitoring and management (RMM) tools to victim hosts

Source: CrowdStrike

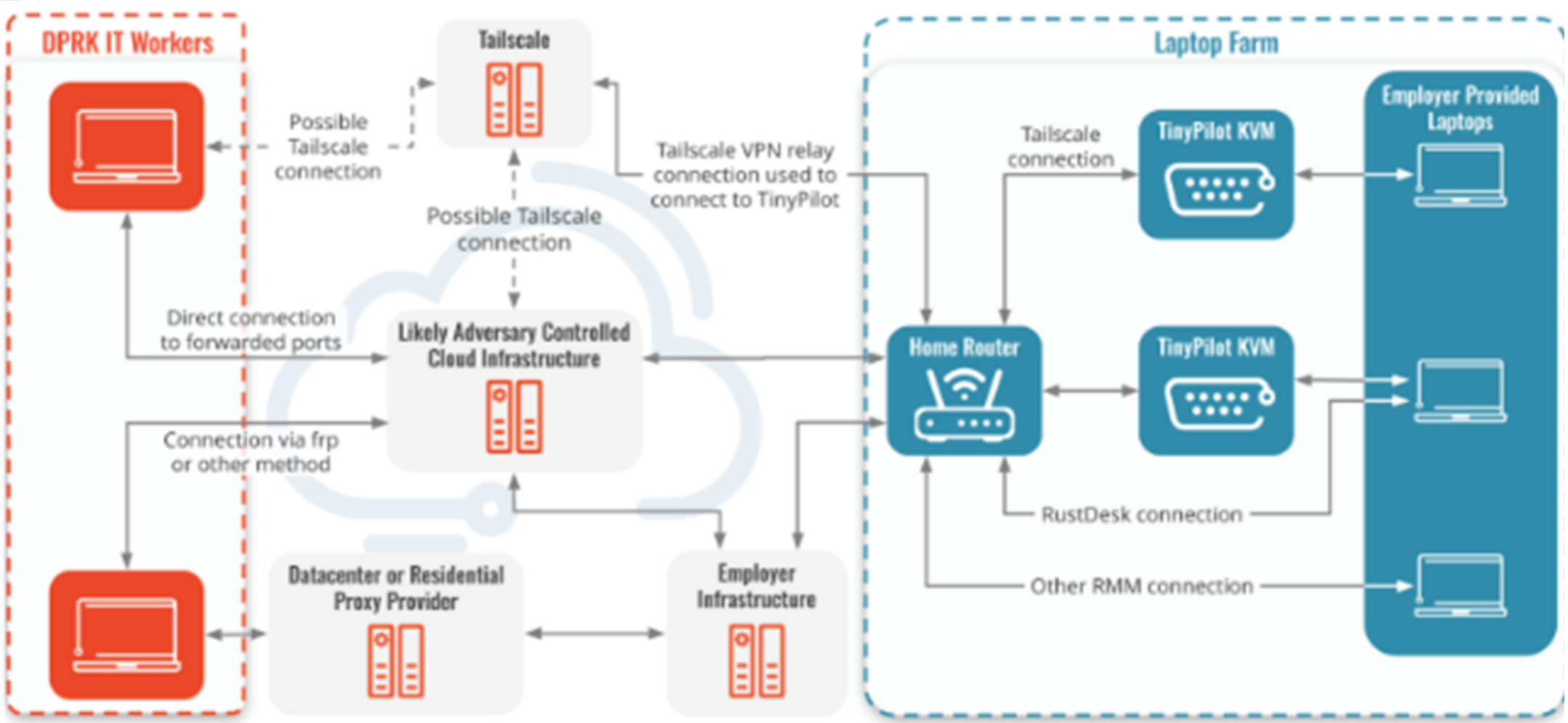
Overview of Famous Chollima

- CrowdStrike Intel assesses that FAMOUS CHOLLIMA likely conducts operations on behalf of North Korea's Munitions Industry Department (MID), which funds and oversees the DPRK's missile and nuclear weapons program
- Appear to be financially motivated, as most of their activity involves small-value cryptocurrency theft, credit card fraud, or receipt of illicit salaries via employment as a software developer
- However, they have been seen exfiltrating data and source code from certain technology companies



Source: CrowdStrike

How Does This Happen At Scale?



Source: CrowdStrike

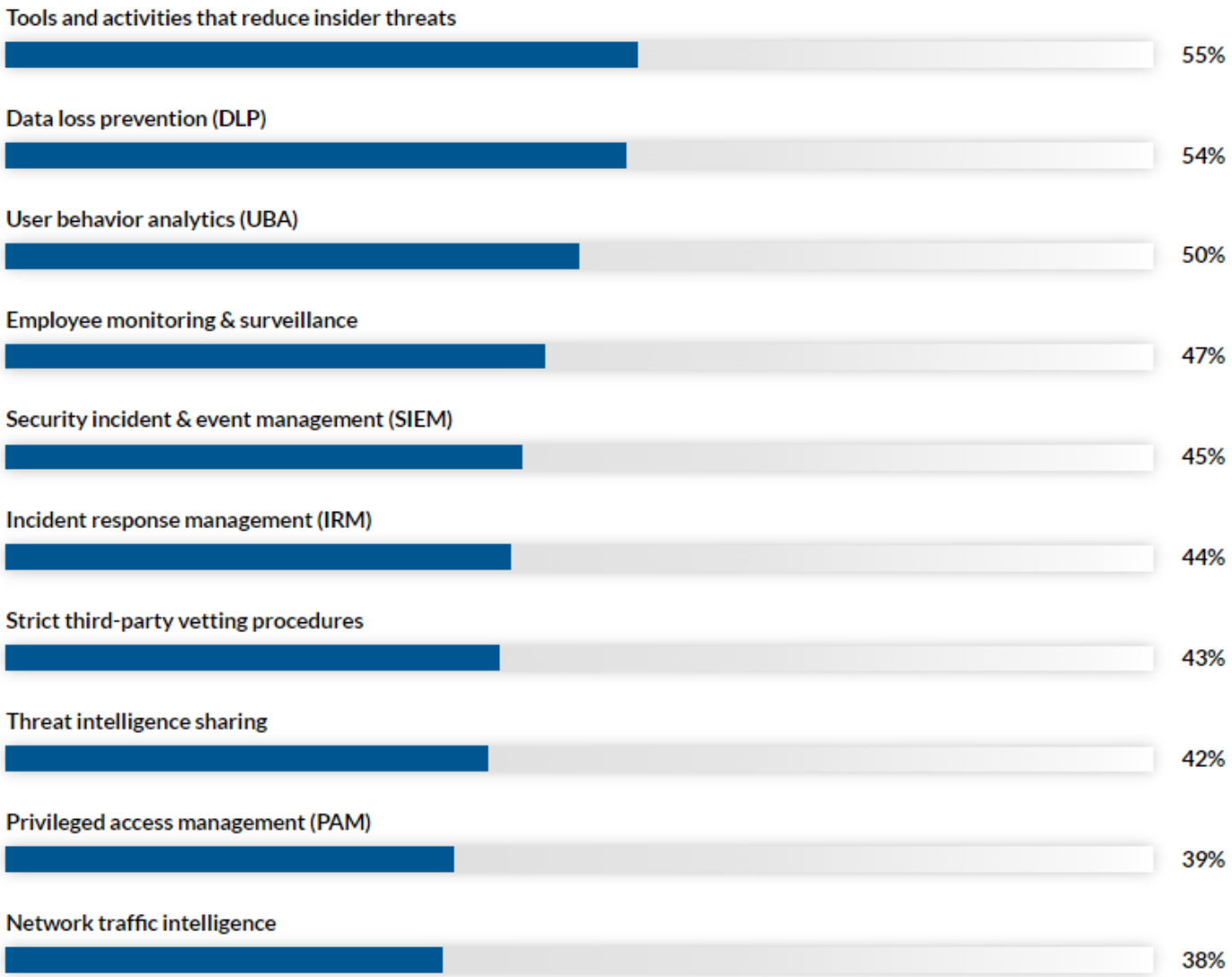
Fake Remote Workers: Detection and Investigation

- What TTPs to look for?
  - Remote Access tools needed such as AnyDesk, RustDesk, JumpDesktop Connect, Visual Studio Dev Tunnels
  - Tools to prevent computer from sleeping Dontsleep.exe, Keepingyouawake.app
  - Chrome extension for cookie editing, screen blurring
  - Faceswap AI apps
- Special Considerations for Investigating Insiders
  - Consult legal and HR to consider next steps
  - Take communications out of band
  - Take home field advantage -- Slow is fast, the TA has already been working there a while
  - Prepare operationally and collect evidence before containing devices and accounts

Tips for Mitigating Risk of Insider Threats Generally

- Develop robust insider threat plans, policies, and procedures
  - Legal, HR, Finance, and Operations need to be included in these plans
- Robus Hiring/screening and monitoring processes of employees, vendors, and contractors
- Strong identity and access management (IAM) controls
- Risk assessment and asset classification
- Security procedures and policies
- Incident response plan
- Detective controls based on behavioral analytics

% of Companies Using Tools to Reduce Insider Threats



Source: IBM, 2020

Designed by FinancesOnline

Tips for Mitigating Risk of Fake Remote Workers

- Rigorous applicant screening processes for remote workers
- Use of advanced verification tools and background checks
- Employee training on recognizing and reporting suspicious activities
- Consider enhanced monitoring and logging on all activities
- Ensure strict IAM limits designed to prevent sabotage, theft, or espionage, including with positions like full stack application developers
- Ensure appropriate logging of all activities and periodic review to identify anomalies
- When provisioning laptops, lock down USB, restrict use of KVM, and consider implications of use of certain Apple products versus others
- Consider requiring the remote employee to present in-person for at least one company event and confirm the person who shows up matches the screenshots/photos taken during the screening process

Tips for Remote Worker Applicant Screening

- Train the front-line interview team about these scams and what to look for, and train your HR screening team, including those confirming I-9 documentation by video on the following:
  - Ensure references from prior companies are contacted through email at the actual company email -- if the employee claims their references no longer work at the company and cannot provide a reference from someone who still works there, *this is a red flag*
  - Conduct on-screen video interviews of the candidate and be sure to take a screen shot of the interviewee so you can then compare the screen shot to (1) the person who presents for the I-9 check, and (2) the person who shows up for work (e.g., at orientation and again on first day) – if you cannot validate with certainty that the pictures match, *this is a red flag*
  - During the I-9 check by video, ensure there is sufficient lighting, and the candidate is facing forward, up close to the camera – if they cannot do this, *this is a red flag*
  - Perform a website search, including LinkedIn and any public social media profiles matching the name, address and work history – if data is missing *this is a red flag*
  - If any photos are provided by the candidate, run them through an AI image detector to see if they are more likely to be AI-generated or real, and also perform a Google image reverse lookup – if the results come back questionable, *this is a red flag*

Tips for Tooling – Detecting Fake Remote Workers

Technical Controls

- RBAC for Devops systems
- Application and admin controls in AWS, M365, Azure, GWS etc.
- Inventory RMM tools. Block and alert on any unexpected
- Check for use of proxy services, and infrastructure like AWS and Azure to connect to systems
- Unusual IP address patterns, risky sign-ins, impossible travel
- Falcon queries for Raspberry Pi neighbors and HID devices
- USB device control and Data Protection

Source: CrowdStrike

Export Control, Immigration, and Employment Laws

On one hand:

- The **Immigration and Nationality Act** makes it illegal for employers to make hiring or recruiting decisions based on an applicant's citizenship, immigration status or national origin. Among other things, it also bars companies from treating workers differently based on these characteristics in verifying their eligibility to work.

On the other:

- **U.S. export control laws and regulations** restrict an employer's ability to release certain technical information and source code without U.S. government authorization to some people who are not U.S. citizens, lawful permanent residents, refugees or asylees.

What Can Employers Do About it?

- U.S. Department of Justice, Civil Rights Division Employer Fact Sheet "How to Avoid Immigration-Related Discrimination when Complying with U.S. Export Control Laws" https://www.justice.gov/crt/media/1287536/dl?inline=

- Orrick Article "How to Avoid Immigration-Related Discrimination When Complying with U.S. Export Control Laws in Hiring and Employment Verification" https://www.orrick.com/en/Insights/2023/05/How-to-Avoid-Immigration-Related-Discrimination-When-Complying-with-US-Export-Control-Laws

Action Plans

- Steps to take if fraud is suspected or detected
- Collaboration with law enforcement and cybersecurity experts
- Export control obligation management
- Immigration and employment law compliance
- Communication strategies to manage potential fallout

HOMELAND SECURITY INVESTIGATIONS

HSI

HSI INVESTIGATES, DISRUPTS, AND DISMANTLES TERRORIST, TRANSNATIONAL, AND OTHER CRIMINAL ORGANIZATIONS THAT THREATEN OR SEEK TO EXPLOIT THE CUSTOMS AND IMMIGRATION LAWS OF THE UNITED STATES.

WHO WE ARE

HSI IS THE PRINCIPAL INVESTIGATIVE ARM OF THE U.S. DEPARTMENT OF HOMELAND SECURITY, RESPONSIBLE FOR INVESTIGATING TRANSNATIONAL CRIME AND THREATS, SPECIFICALLY THOSE CRIMINAL ORGANIZATIONS THAT EXPLOIT THE GLOBAL INFRASTRUCTURE THROUGH WHICH INTERNATIONAL TRADE, TRAVEL, AND FINANCE MOVE.

OUR MISSION

HONOR | SERVICE | INTEGRITY

Insider Threats - By The Numbers

- **76% of organizations** have reported an increase in insider threat activity over the past five years
- In 2023, **71% of companies** experienced 21 to 40 insider security incidents, an increase of 67% from 2022
- Insider threats are responsible for **60% of data breaches**
- Avg cost to organizations of resolving insider-related incidents per year: **$16.2 million USD**, an increase of 40% from previous years
- Avg cost to organizations of malicious insider attacks: **$4.99 million USD** per incident

(Sources: https://www.stationx.net/insider-threat-statistics/
https://www.securonix.com/press_release/2024-insider-threat-report/)
https://www.idwatchdog.com/insider-threats-and-data-breaches
https://www.ibm.com/topics/insider-threats

Contacting Law Enforcement

- Getting law enforcement involved can help organizations
  - Marshal resources
  - Provide context on the attackers
  - Facilitate recovery and ultimately lead to effective disruption of cybercrime organizations
- If an organization is unsure of who to contact, there is a saying that "a call to one is a call to all". Reach out to whatever local, state, or federal entity that has the resources to respond.

Cyber Crimes Center Operation

Designed to significantly disrupt adversaries that exploit the internet to subvert U.S. laws and threaten the economic integrity, public safety, and national security of the United States.

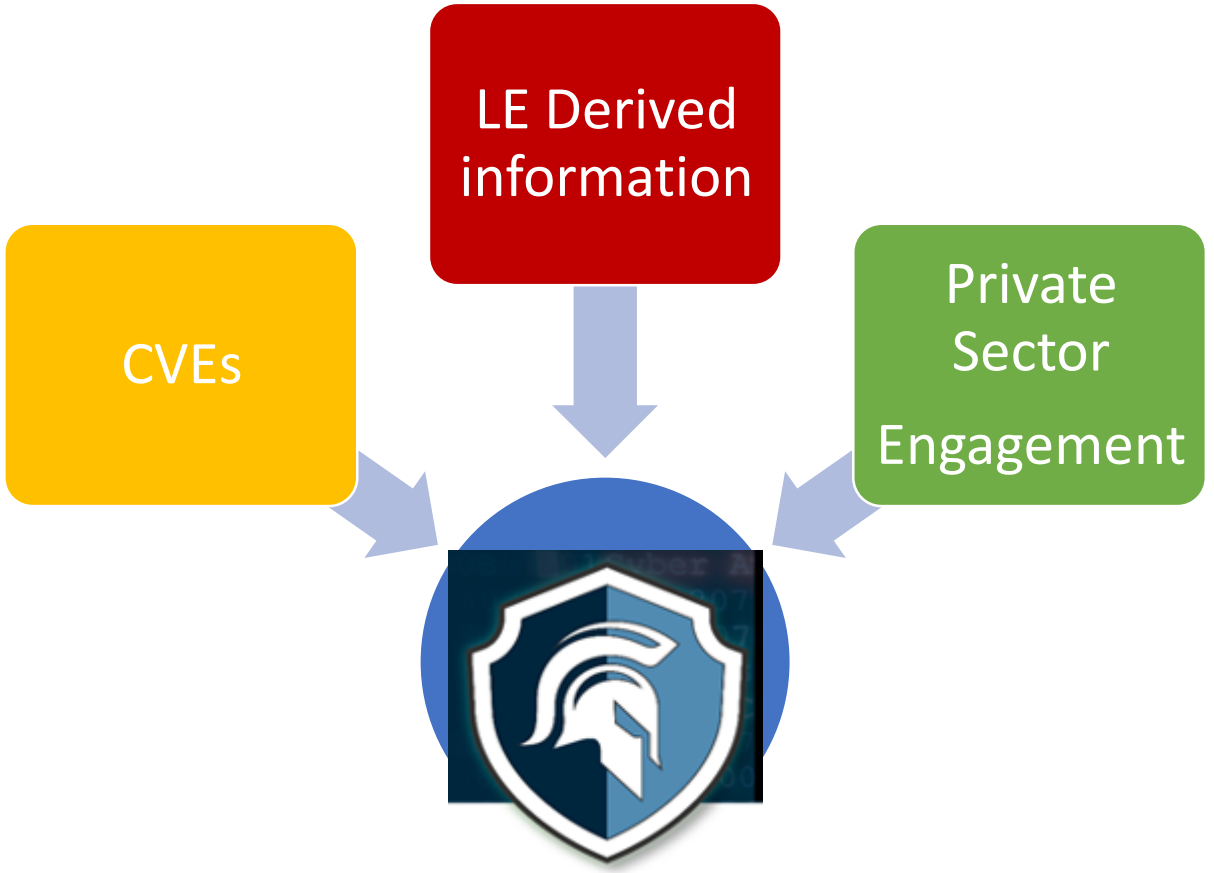
What: Prevents cyber-attacks posed by transnational criminal organizations (TCOs) and foreign government sponsored organizations.

How: Detect vulnerabilities in critical infrastructure and alerts victims to take action before further damage occurs.

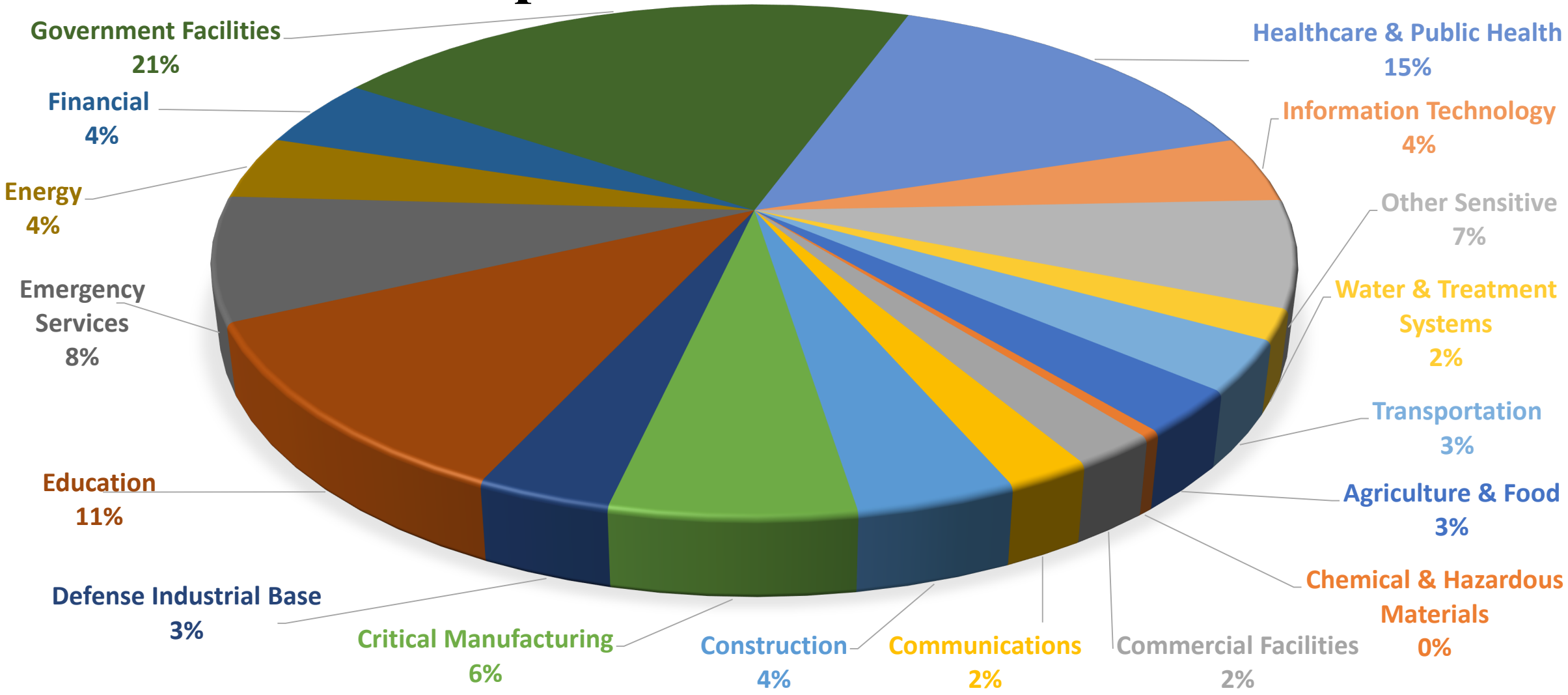
Cyber Crimes Center Operation

Operation Derived Information

- Vulnerability Identification
  (Passive CVE identification)
- Law Enforcement Derived Information
  - Court Orders
  - Subpoenas
- Private Sector Engagement
- Data Analytics



FY 2021-2024
Disruptions of Network Access



HONOR | SERVICE | INTEGRITY

Homeland Security Investigations

- Victim centered approach
  - HSI is not a regulatory agency and is only concerned with assisting victims and prosecuting threat actors
  - HSI will not evaluate or criticize victim's IT security practices
  - Will work within the parameters of what the victim is willing and able to provide
  - Will strive to have minimum possible impact or disruption to victim's operations
- May share information located during an investigation that can assist the victim with remediation

Report Cyber Crime

HSI Tip Line

1-877-4-HSI-TIP (1-877-447-4847)

Contact Your Local HSI Office

DHS.gov/HSI/contact/sac-offices

Additional Resources

- Guidance on the Democratic People's Republic of Korea Information Technology Workers (May 16, 2022) https://ofac.treasury.gov/media/923126/download?inline

- Mandiant North Korean IT Workers Threat Podcast on Spotify: https://open.spotify.com/episode/0xeaavXjlX2XLm3oibOv6g?si=C4uBNKuWS_Ss8v87ztuFIA&nd=1&dlsi=1f3e8437549940cd