FORTINET®

Cybersecurity Protection in an Expanding Digital Environment

Jim Richberg, Head of Cyber Policy & Global Field CISO
January 2024

Mark LaVigne, PhD
Deputy Director
NYSAC

Jim Richberg

Head of Cyber Policy and
Global Field CISO

Fortinet

Here's What You'll Learn

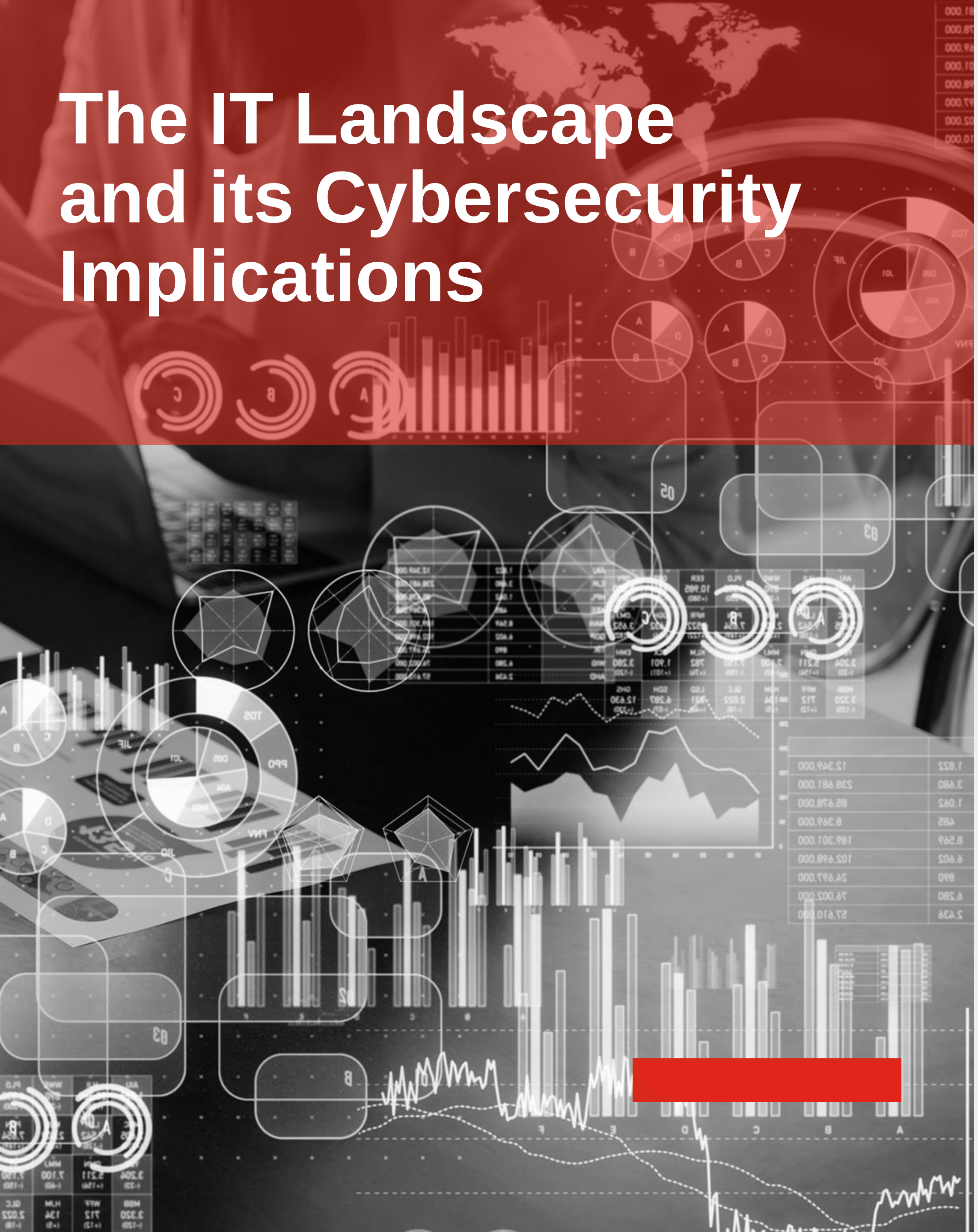
01 The IT Landscape and its Cybersecurity Implications

02 Key Concepts in Cybersecurity

03 Cyber Threats and Cyber Threat Intelligence

04 Recommendations and Resources

The IT Landscape and its Cybersecurity Implications

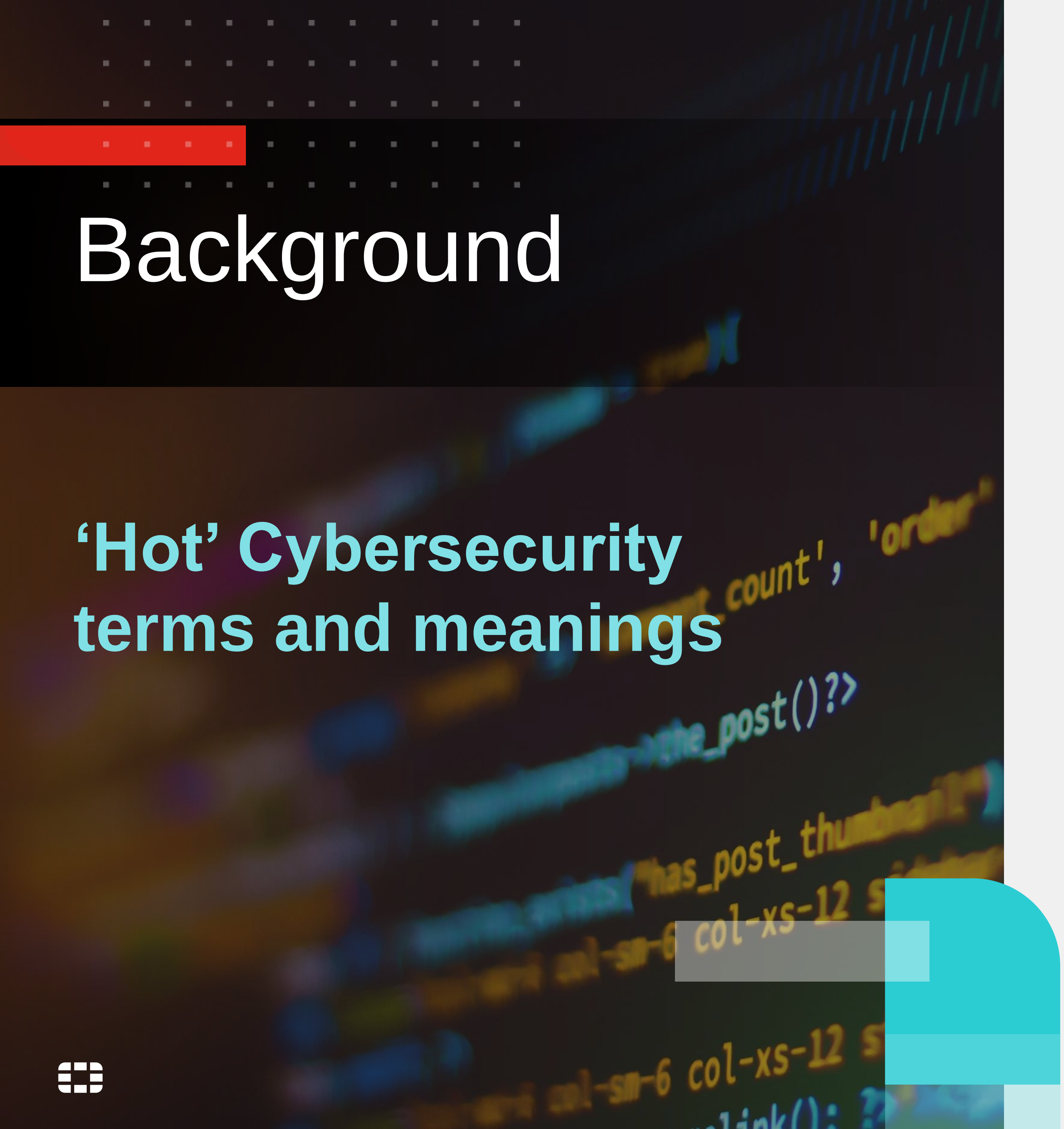


- Information Technology (IT) vs Operational Technology (OT)
- Internet of Things (IoT) and Industrial IOT devices
- Edge computing… and edge security
- Cloud and cloud-based services
- ‘X as a service’ (‘XaaS) vs. internally built and managed IT
- Software-defined networking
- ‘Connect from anywhere’

The IT Landscape and its Cybersecurity Implications…*continued*

- AI and Machine Learning
- Automation and Autonomy – from Robotic Process Automation to Intelligent Automation
- GenAI—‘welcome to the wild west!’ DON’T use it when:
  - You need 100% accuracy
  - You need instant results
  - A human can’t judge good vs. bad output

Background



‘Hot’ Cybersecurity terms and meanings

“***Attack Surface***” —the intersection of IT and security, but often shorthand for digital size/complexity and unknown factors

“***Shadow IT***”—the fact that users sometimes provide their own IT solutions and you can’t protect what you don’t know your organization has

“***Zero Trust***”—a terrible name for a set of good practices like segmentation of networks, least privilege and role-based access control. *Assume any network is compromised and act accordingly*

Cyber Threat

- Can affect *confidentiality, integrity, availability* of data
- Ransomware can affect all three!
- “Insider threat” vs. insider risk
- Criminals vs. hackers vs. “Advanced Persistent Threat” (APT)
- ‘Threats enabled by the global nature of cyberspace
  - ✓ Opportunistic criminal activity
  - ✓ Caught in the crossfire or intentionally targeted by nation states

Cyber Threat Intelligence

Tactical intelligence (‘turning raw data into dots’)

Production and use is *largely automated*

The largest category by volume and variety of data sources

Operational intelligence (‘connecting the dots’)

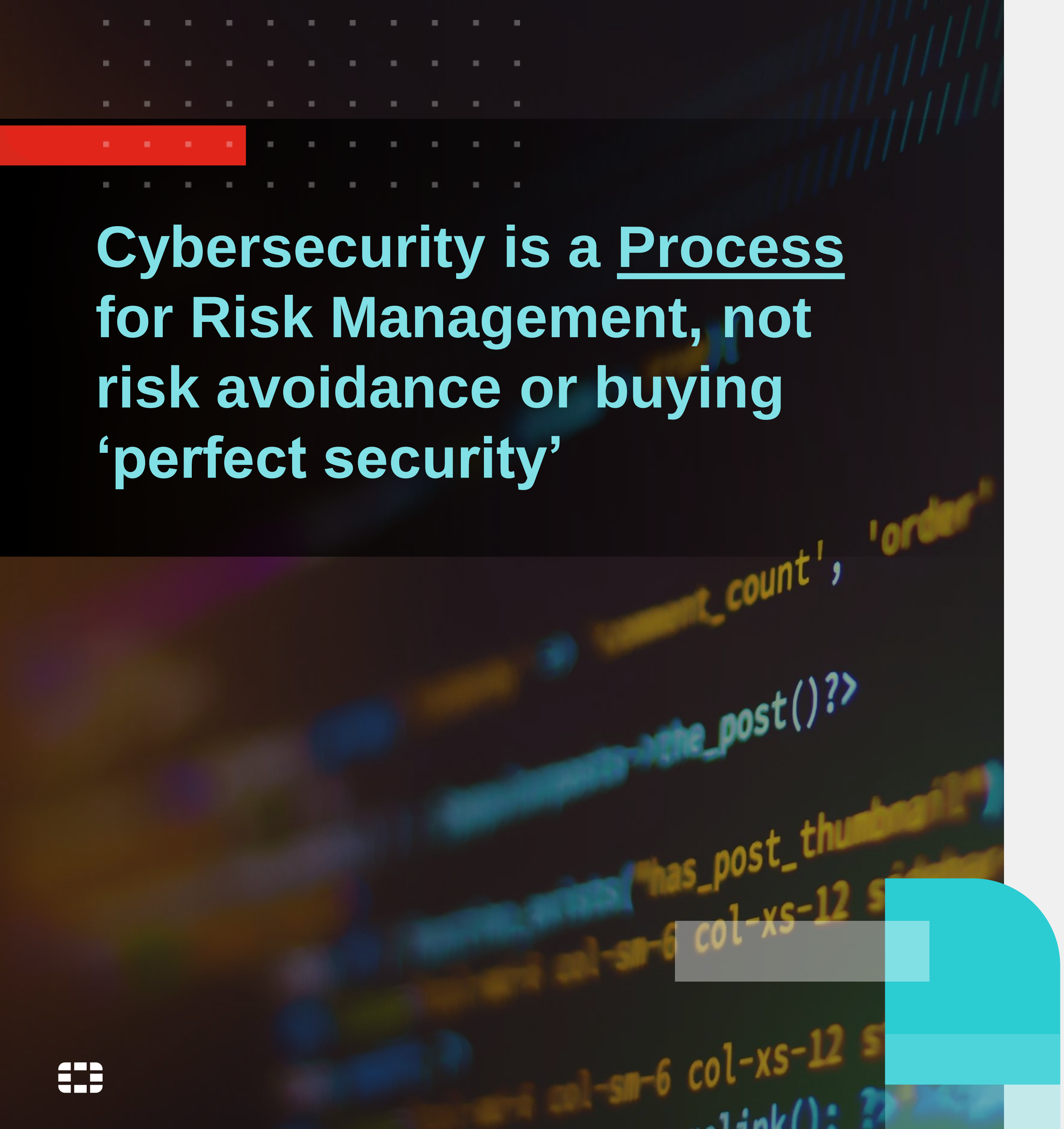
Human curated; quality and focus often uneven

Strategic intelligence (‘making pictures or patterns’ out of the dots)

Human generated; relatively uncommon

Resist the temptation to ‘do it yourself’– outsource or partner!

Recommendations



Cybersecurity is a Process for Risk Management, not risk avoidance or buying ‘perfect security’

Follow best practices like the US National Institute of Standards and Technology Cybersecurity Framework (“NIST CSF”) with its functions of:

- ***Identify*** the assets and processes that matter most to your organization
- ***Protect*** them
- ***Detect*** threat activity directed at these assets
- ***Respond*** to these threats
- ***Recover*** from successful threat activity

…because cybersecurity needs top level direction to succeed, the new version of the CSF will add ***Govern*** as a process touching each of these five

Train

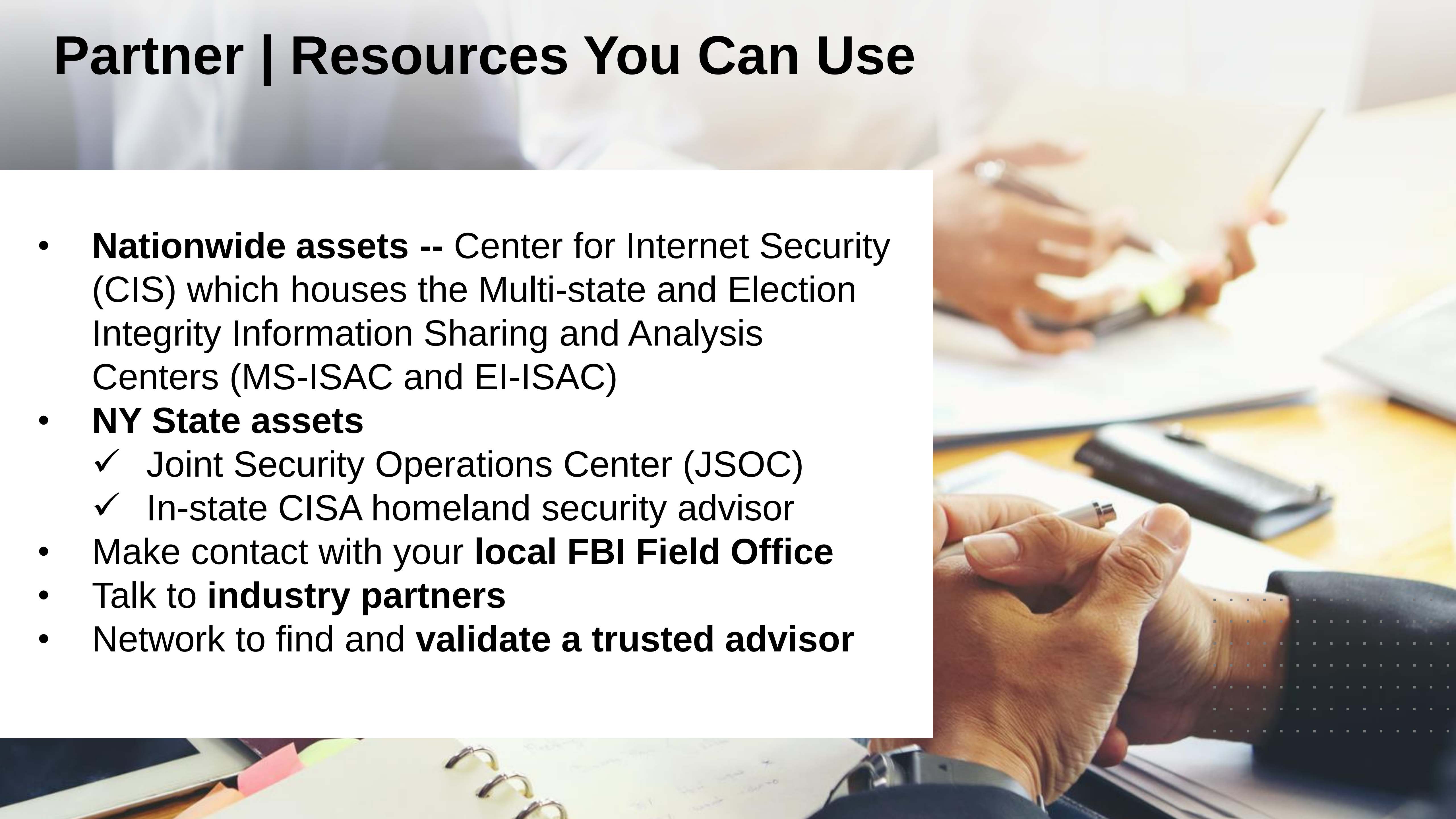
Users -- teach threat awareness and basic cyber hygiene

Cyber and IT Staff -- are they taking advantage of concepts in the IT landscape and security developments?

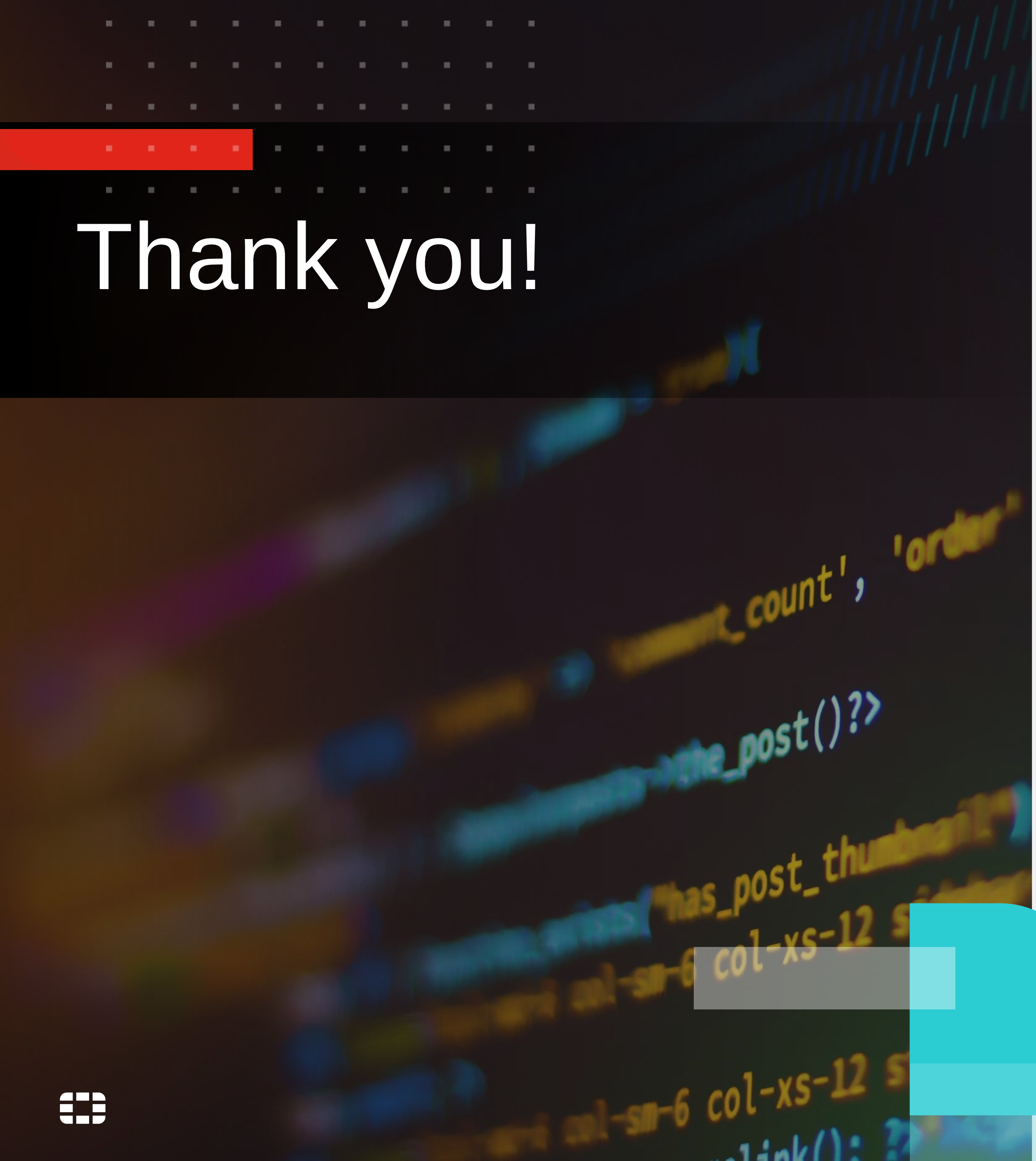
Procurement officials -- every program has a digital aspect that should be considered during procurement (*and you don’t have to re-invent the wheel on security requirements!*)

Leadership -- how should the organization respond to the inevitable cyber breach? *(‘tabletop exercises’ can be invaluable in finding problems and creating procedures)*

Partner | Resources You Can Use



- **Nationwide assets --** Center for Internet Security (CIS) which houses the Multi-state and Election Integrity Information Sharing and Analysis Centers (MS-ISAC and EI-ISAC)
- **NY State assets**
  - ✓ Joint Security Operations Center (JSOC)
  - ✓ In-state CISA homeland security advisor
- Make contact with your **local FBI Field Office**
- Talk to **industry partners**
- Network to find and **validate a trusted advisor**



Thank you!

Jim Richberg
Jrichberg@Fortinet.com

FORTINET®