

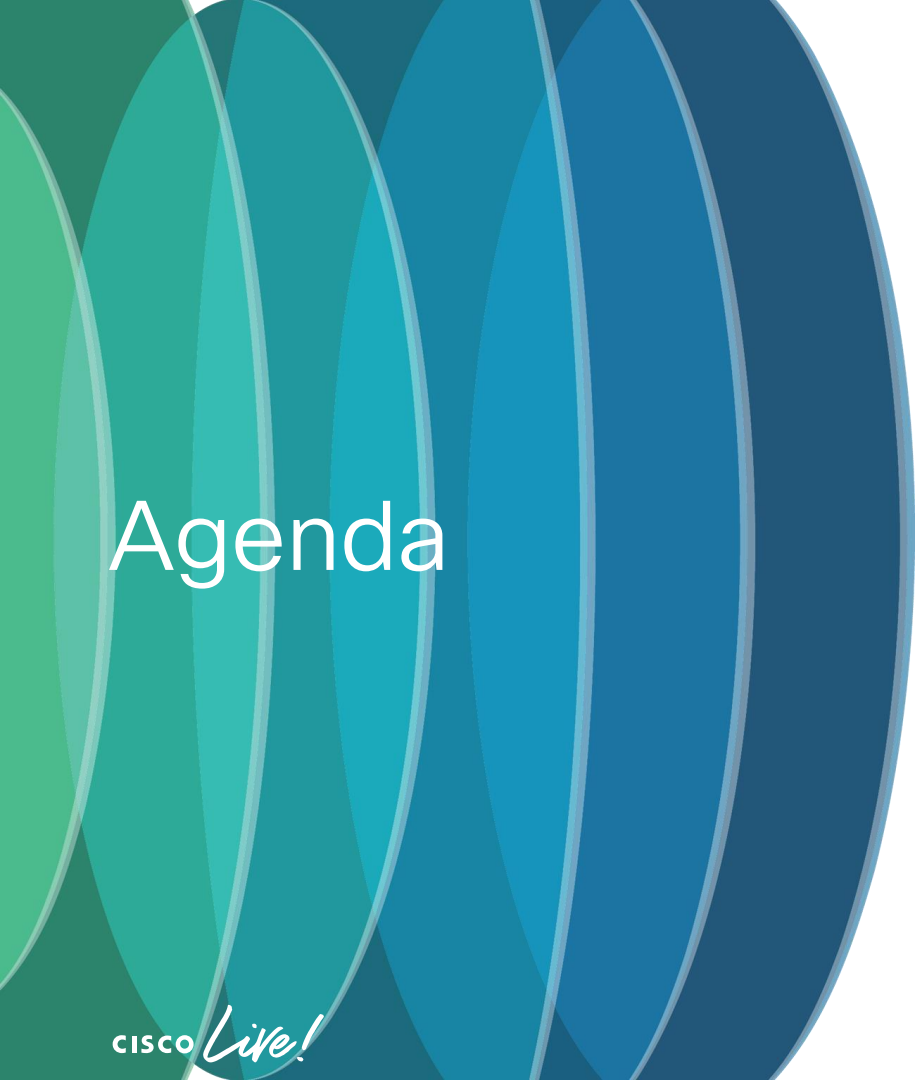


# Solving Cyber Insecurity

Martin LEE  
BRKSEC-1159

CISCO *Live!*





# Agenda

- A Problem to Solve
- Technical Issues
- Human Issues
  - Human error
  - Criminality & Geo-Politics
- Conclusion

# A National & Regional Risk

Commission staff working document

Overview of natural  
and man-made disaster risks  
the European Union  
may face

## ENISA THREAT LANDSCAPE 2024

July 2023 to June 2024

SEPTEMBER 2024

### Risk drivers:

- Climate change
- Urbanisation
- Environmental degradation
- Changing security landscape
- Technological developments
- Ransomware
- Malware
- Social Engineering
- Threats against data
- Threats against availability: Denial of Service
- Information manipulation and interference
- Supply chain attacks

# Impacts



Official Statistics

## Cyber security breaches survey 2024

Published 9 April 2024

Experiencing a cyber breach or attack in previous 12 months:

50% businesses

32% charities

“Just over two-fifths (of these) ended up being victims of cyber crime.”

Also:

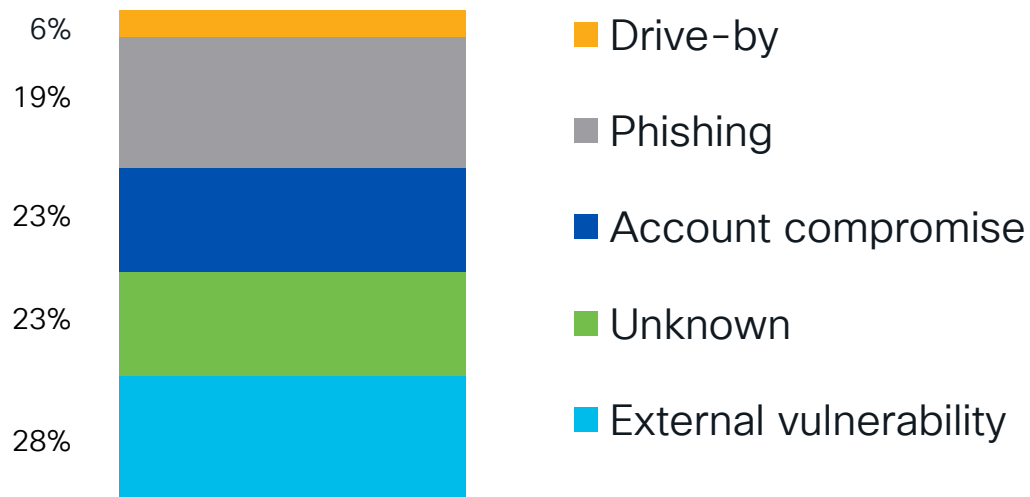
Unavailability of services.

Stress, anxiety.

IT team burnout

# Only So Many Ways to Compromise a System

Talos Incident Response data



# The Two Axes of Cyber Insecurity



# Technical Issues

# Writing Software is Hard

|    |                                                                                                                                                                            |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Out-of-bounds Write<br><u><a href="#">CWE-787</a></u>   CVEs in KEV: 70   Rank Last Year: 1                                                                                |
| 2  | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')<br><u><a href="#">CWE-79</a></u>   CVEs in KEV: 4   Rank Last Year: 2                 |
| 3  | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')<br><u><a href="#">CWE-89</a></u>   CVEs in KEV: 6   Rank Last Year: 3                 |
| 4  | Use After Free<br><u><a href="#">CWE-416</a></u>   CVEs in KEV: 44   Rank Last Year: 7 (up 3) ▲                                                                            |
| 5  | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')<br><u><a href="#">CWE-78</a></u>   CVEs in KEV: 23   Rank Last Year: 6 (up 1) ▲ |
| 6  | Improper Input Validation<br><u><a href="#">CWE-20</a></u>   CVEs in KEV: 35   Rank Last Year: 4 (down 2) ▼                                                                |
| 7  | Out-of-bounds Read<br><u><a href="#">CWE-125</a></u>   CVEs in KEV: 2   Rank Last Year: 5 (down 2) ▼                                                                       |
| 8  | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')<br><u><a href="#">CWE-22</a></u>   CVEs in KEV: 16   Rank Last Year: 8                      |
| 9  | Cross-Site Request Forgery (CSRF)<br><u><a href="#">CWE-352</a></u>   CVEs in KEV: 0   Rank Last Year: 9                                                                   |
| 10 | Unrestricted Upload of File with Dangerous Type<br><u><a href="#">CWE-434</a></u>   CVEs in KEV: 5   Rank Last Year: 10                                                    |

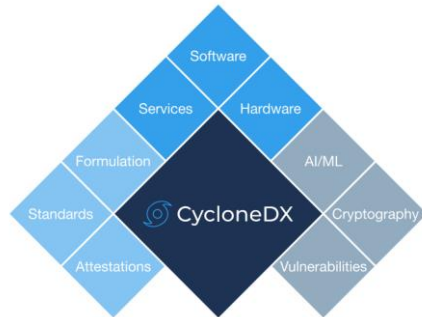
15 weaknesses  
present every year  
since 2019!

# Emerging Solutions

Automated discovery and remediation of vulnerabilities

## SBOM Tools

Identify dependencies  
Find known vulnerabilities  
Identify weak cryptography



## Source Code Analysis

Identify new vulnerabilities  
Identify poor coding



# Emerging Solutions

Automate the day-to-day & Real-time Code Review

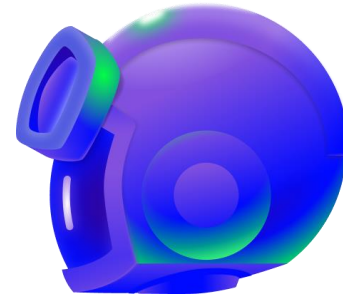
## Cisco AI Assistant

Automate routine tasks  
Simplify complex tasks

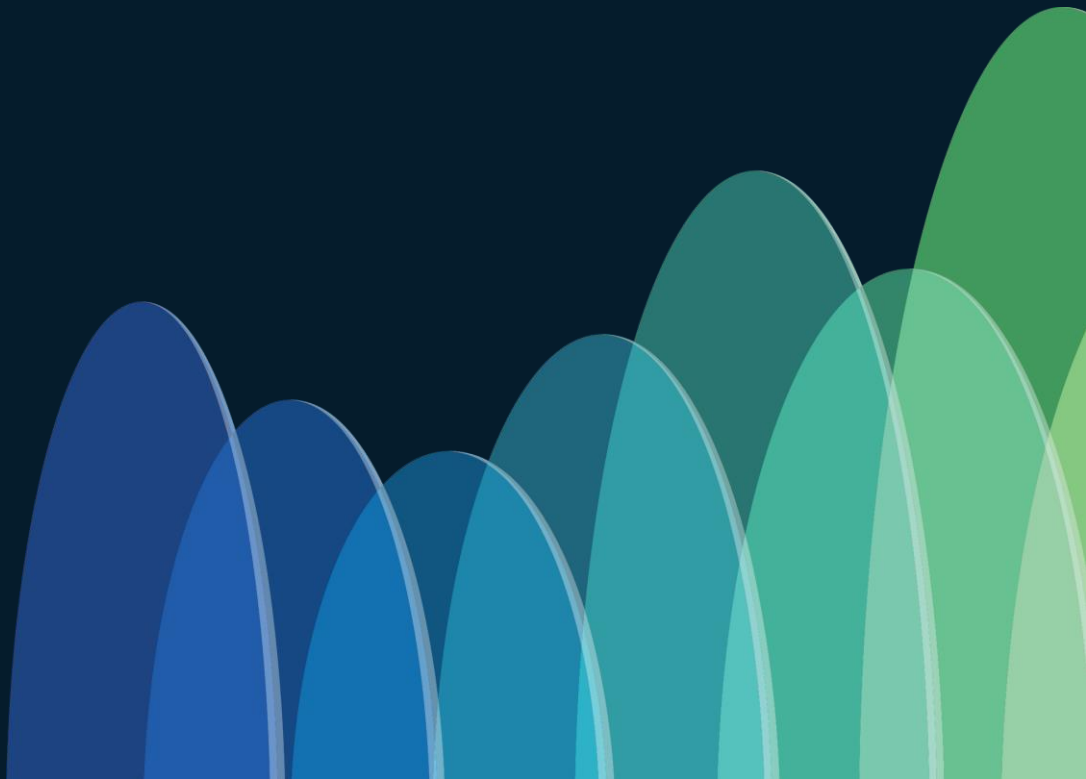


## GitHub Copilot

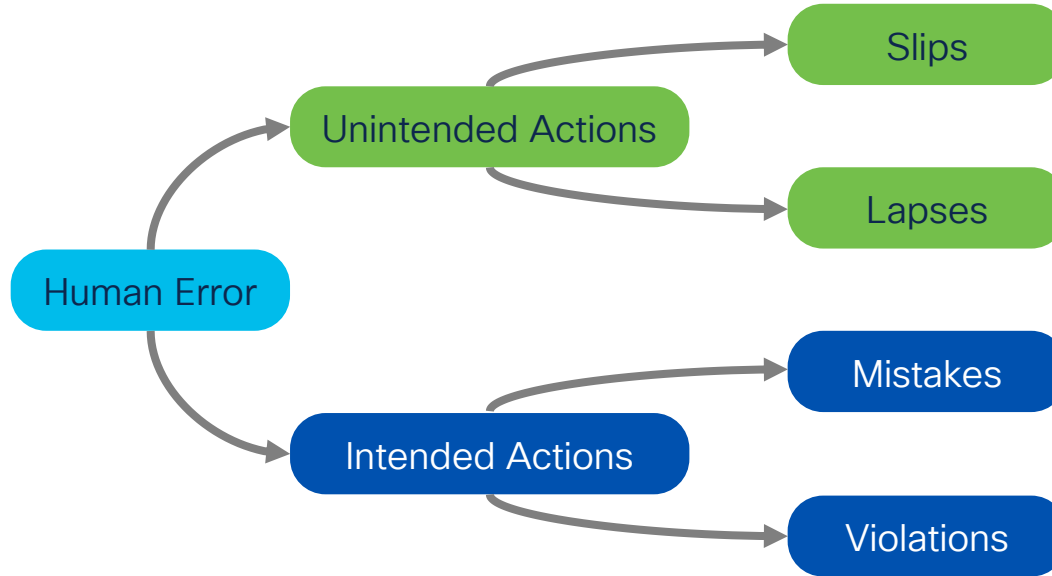
Automate routine tasks  
Support developer  
Review & improve code



# Human Issues



# People Fail in Predictable Ways



Why did you click the link?

Didn't mean to click

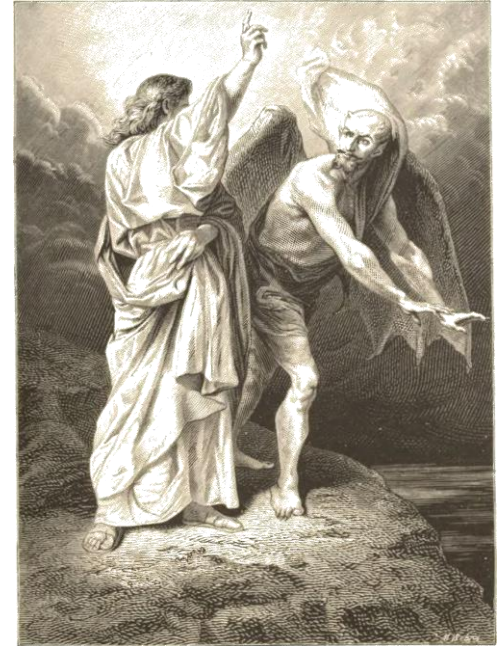
Forgot not to click

Thought it was genuine

Curious what would happen

# Preventing Slips, Lapses & Mistakes

- Successes
  - Vast majority of phishing emails blocked
  - Vast majority of phish web sites blocked
- Areas To Improve
  - Targeted social engineering
  - Attacks over instant messaging/social media
  - Vish



Keep away from temptation

# AI Deepfake & BEC

Defending against future threats.

- Keep these away from users!
- Build robust internal anti-fraud processes

Cyber Security

+ Add to myFT

## Arup lost \$25mn in Hong Kong deepfake video conference scam

UK-based engineering group identified as target of fraud that used digitally cloned CFO to trick staff

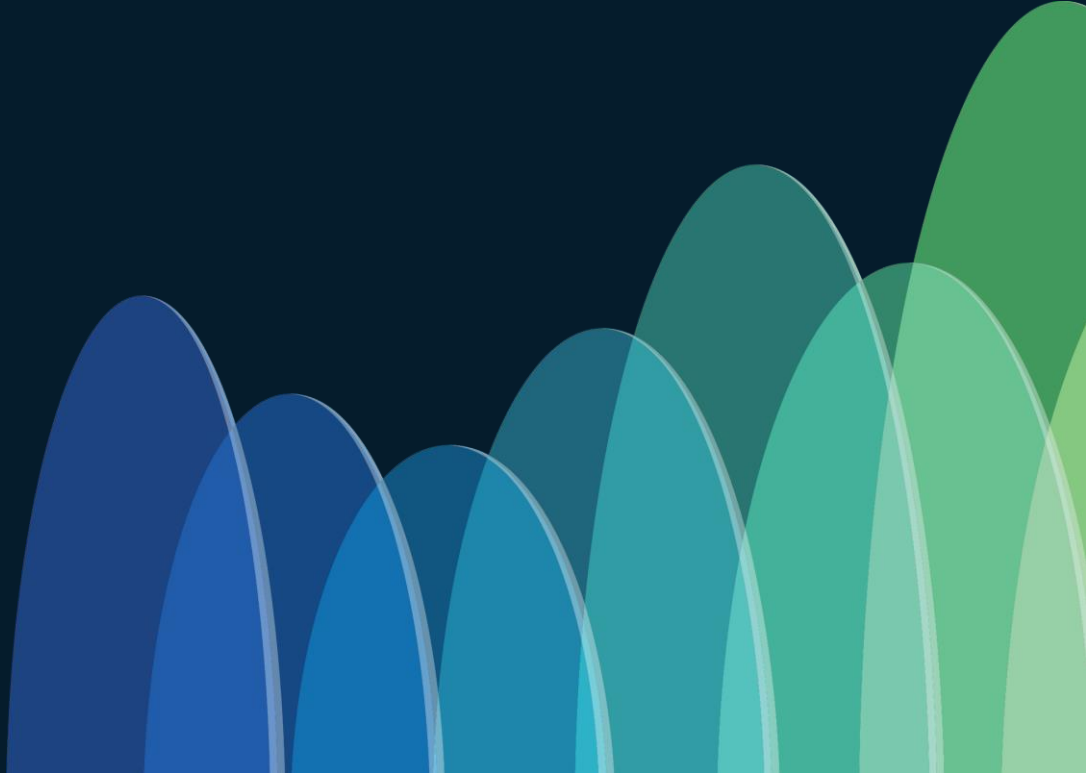
“We can confirm that fake voices and images were used,” the company said, declining to give details because the incident was still being investigated. “Our financial stability and business operations were not affected and none of our internal systems were compromised,” it said.

## CEO of world's biggest ad firm targeted by deepfake scam

**Exclusive: fraudsters impersonated WPP's CEO using a fake WhatsApp account, a voice clone and YouTube footage used in a virtual meet**

# Authentication

(friend or foe?)



# The Problem of Authentication

Passwords have never been secure!

- Shoulder surfing
- Dumping password file
- Credential stuffing

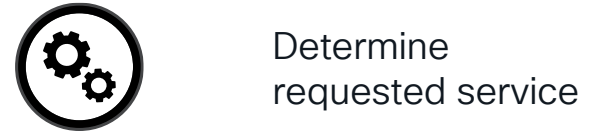
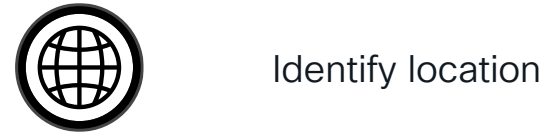


Fernando Corbato

# Contextual Authentication

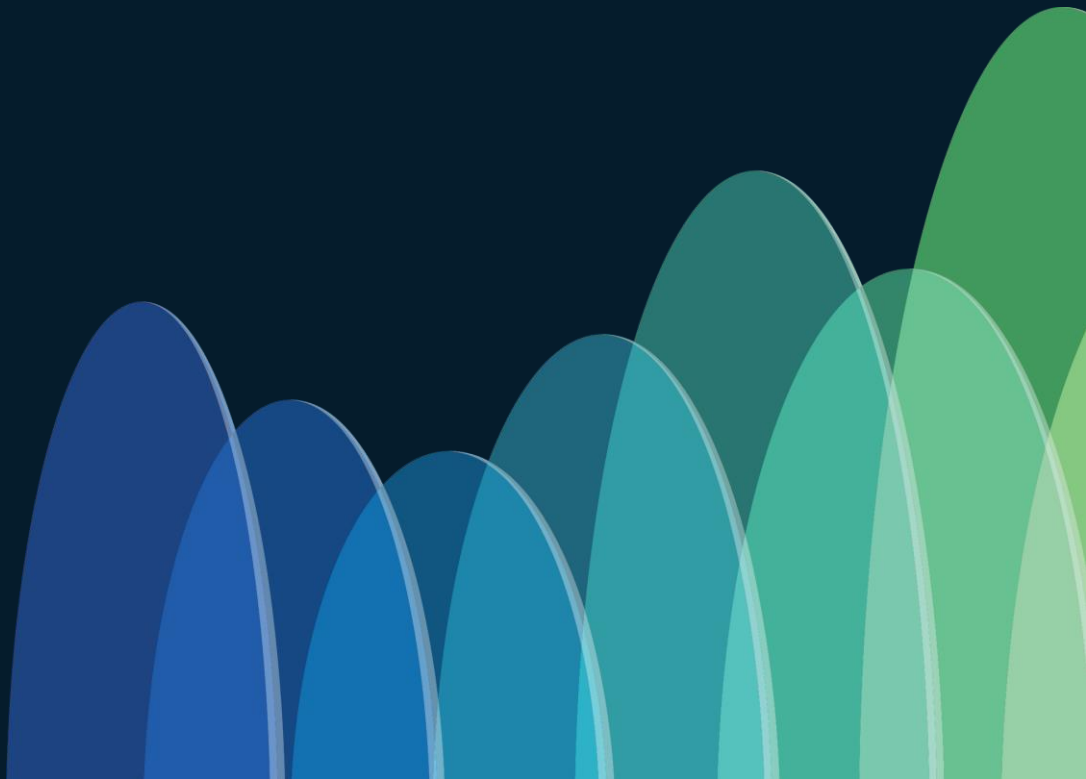
Solving authentication

- Not a binary decision
- Based on context
- Permissions are fluid

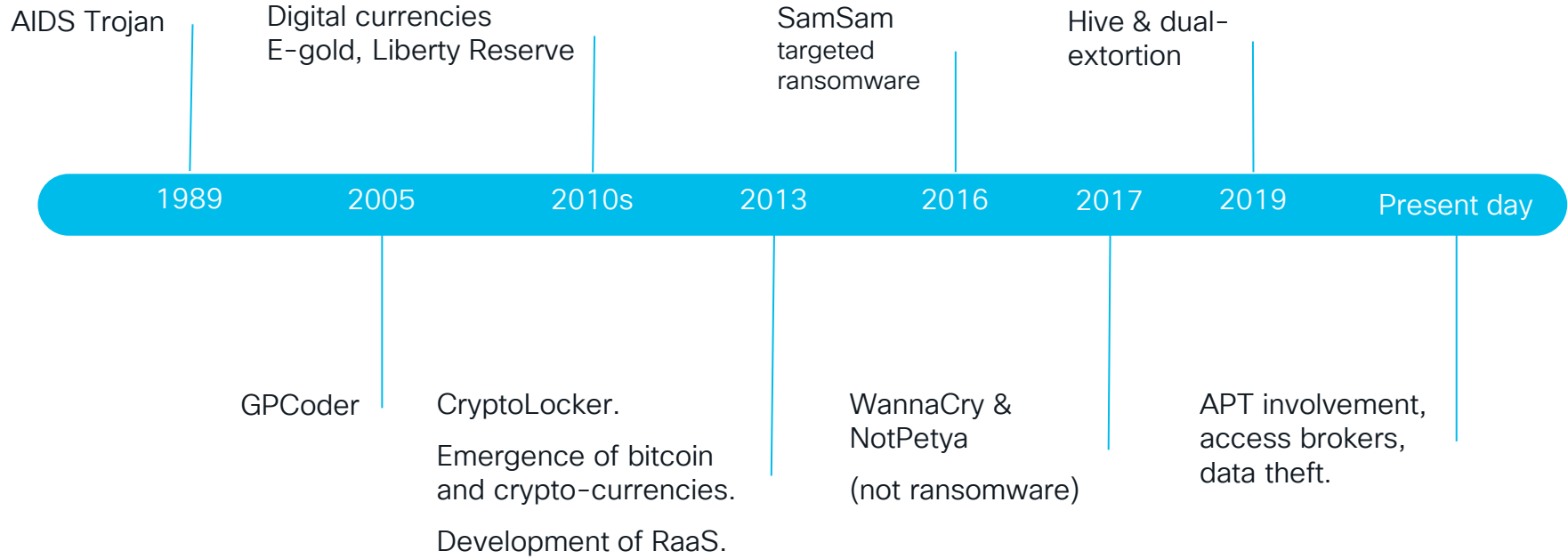


Contextual minimal authorisation

# Criminality



# Ransomware Evolution



# Ransoms Paid



% OF RANSOMS PAID PER DAY



0.1% - 10%

2.9%

64.73

TOTAL RANSOMS PAID PER DAY



AVERAGE RANSOM



\$200 - \$500

\$300

\$19,419.00

TOTAL RANSOM COLLECTED PER SERVER PER DAY



TOTAL # OF REDIRECTION SERVERS



50 - 400

147

Gross Income for Ransomware

\$95,153.10

\$2,854,593.00

\$34,255,116.00

DAILY

MONTHLY

YEARLY

| Bitcoin Wallet Address             | Bitcoins Received  | Value in USD          |
|------------------------------------|--------------------|-----------------------|
| 1Kx9TT76PHwk8sw7Ur6PsMWyEtaogX7wWY | 182.9999668        | \$1,462,484.49        |
| 12vsQry1XrPjPCaH8gWzDJeYT7dhTmpeJL | 55                 | \$439,544.60          |
| 15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNJ | 50.41              | \$402,862.61          |
|                                    | 48.25              | \$385,600.49          |
|                                    | 40.035             | \$319,948.51          |
|                                    | 38.9999859         | \$311,676.97          |
|                                    | 35                 | \$279,710.20          |
|                                    | 30.00821708        | \$239,817.27          |
|                                    | 30.00217032        | \$239,768.94          |
|                                    | 28                 | \$223,768.16          |
|                                    | 25.00016544        | \$199,794.32          |
|                                    | 25                 | \$199,793.00          |
|                                    | 24.077             | \$192,416.64          |
|                                    | 30                 | \$159,834.40          |
|                                    | 13                 | \$103,892.36          |
|                                    | 10                 | \$79,917.20           |
|                                    | 10                 | \$79,917.20           |
|                                    | 10                 | \$79,917.20           |
|                                    | 6.4995167          | \$51,942.32           |
|                                    | 3.325              | \$26,572.47           |
|                                    | 2.79993008         | \$22,376.26           |
|                                    | 1.70004113         | \$13,586.25           |
|                                    | 0.001              | \$7.99                |
|                                    | <b>700.1079935</b> | <b>\$5,515,149.85</b> |

# Law Enforcement Action

Increase risk, reduce return on investment

Hacker jailed for selling Asda and Uber customers' data on dark web

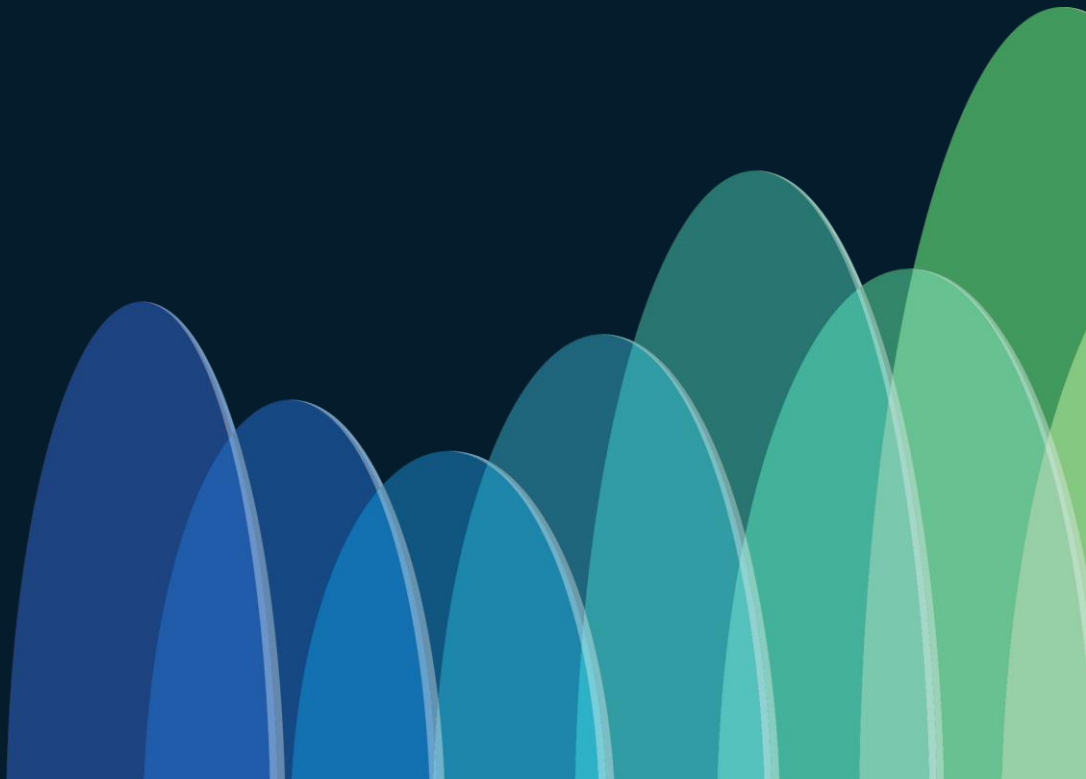
'One-man cybercrime wave' Grant West masqueraded as Just Eat to get people's data



Grant West has been jailed for more than 10 years. Photo: [Source]



# Geo-Politics



# Advanced persistent threats

| Russia                                                                                                                                                           | China                                                                                                                                                                                                                   | Iran                                                                                                                                                                                          | North Korea                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Focused mainly on Ukraine, NATO countries</li></ul>                                                                      | <ul style="list-style-type: none"><li>• Global targeting, specific focus on West &amp; Pacific Rim</li></ul>                                                                                                            | <ul style="list-style-type: none"><li>• Focused on Middle East, US, Europe</li></ul>                                                                                                          | <ul style="list-style-type: none"><li>• Global focus</li></ul>                                                                                                                                |
| <ul style="list-style-type: none"><li>• Goals:<ul style="list-style-type: none"><li>• Espionage</li><li>• Disruption (short &amp; long term)</li></ul></li></ul> | <ul style="list-style-type: none"><li>• Goals:<ul style="list-style-type: none"><li>• Intellectual property theft</li><li>• Economic espionage</li><li>• Dissidents</li><li>• Long term persistence</li></ul></li></ul> | <ul style="list-style-type: none"><li>• Goals:<ul style="list-style-type: none"><li>• Intellectual property theft</li><li>• Espionage</li><li>• Suppression of dissidents</li></ul></li></ul> | <ul style="list-style-type: none"><li>• Goals:<ul style="list-style-type: none"><li>• Regime support</li><li>• Data theft</li><li>• Financial crimes</li><li>• Disruption</li></ul></li></ul> |

# Russian Military Doctrine

Cyber warfare as part of  
“information warfare”

- Undermine ability to wage war
- Destabilise society
- Cause dissent & disruption

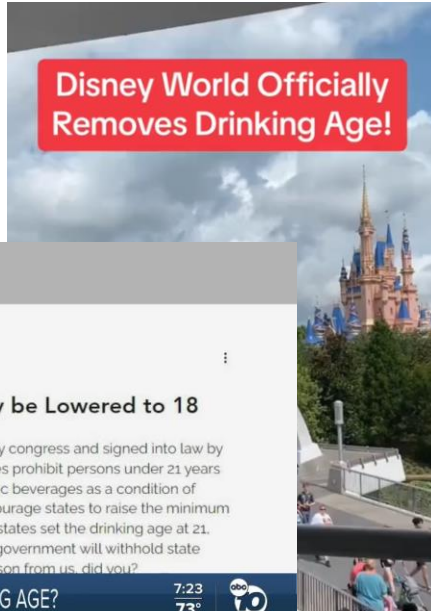
“disrupt the normal functioning of information and telecommunications systems, security and information resources and to obtain unauthorized access to them.”

(Russian Federation Information Security Doctrine, 2000)

“The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.”

Gen. Gerasimov, Chief of the Russian General Staff, 2013)

# Fake News



Mouse Trap News • 3 days ago • 3 min read

## Drinking Age at Disney World May be Lowered to 18

The National Minimum Drinking Age Act was passed by congress and signed into law by President Ronald Reagan in 1984. It "requires that States prohibit persons under 21 years of age from purchasing or publicly possessing alcoholic beverages as a condition of receiving State highway funds." This was an act to encourage states to raise the minimum drinking age to 21. As it states, it is not mandatory that states set the drinking age at 21, but if a state doesn't implement 21 as a minimum, the government will withhold state funds. **FACT** OR FICTION? I didn't think you would get a history lesson from us, did you?

DISNEY WORLD TRYING TO LOWER DRINKING AGE?

7:23  
73°



ALERT: A STATE OF EMERGENCY AFTER SEEING A 233% INCREASE IN CRASHES INVOLVING B

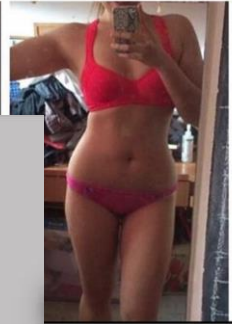
cisco *Live!*



diyfoodys

Bezahlte Partnerschaft mit socialcoasterdigi...

## #1 Detox Tea in the World

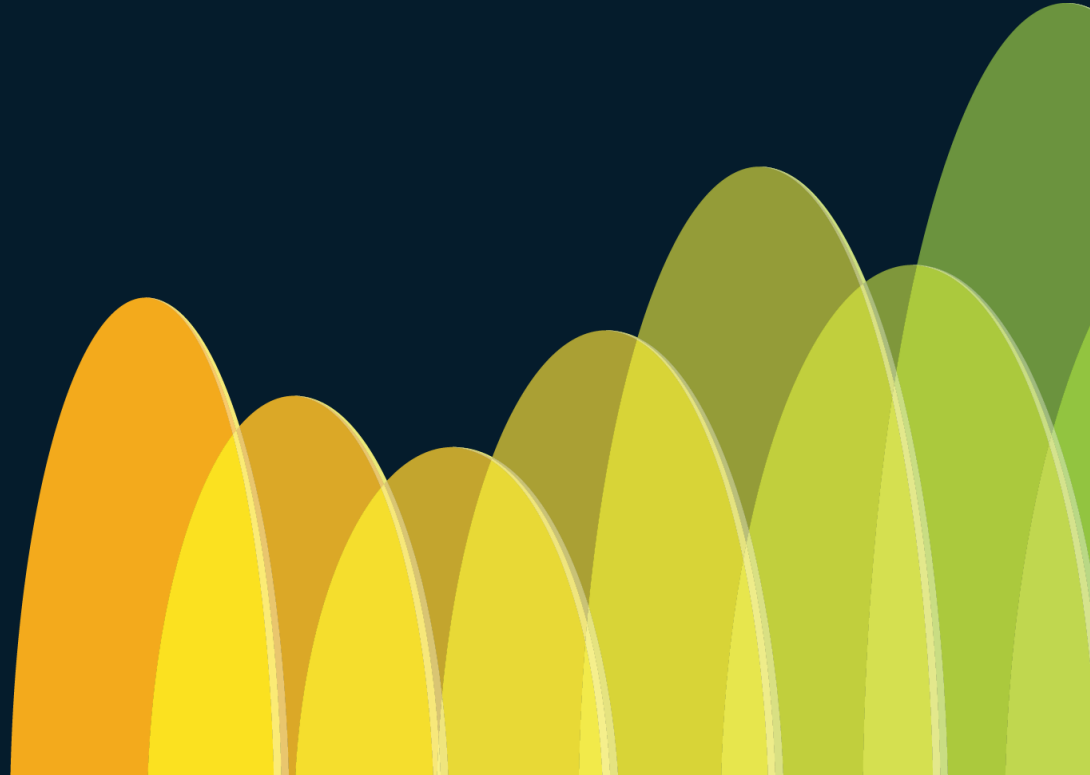


ec: "FITTEA"

FitTea



# Decision Making



# Can't Plead Ignorance

## Equifax CEO Richard Smith Steps Down After Epic Breach

Equifax CEO Richard Smith is stepping down after a historic data breach that exposed the personal financial histories of over 143 million Americans.

## Judge Spares Former Uber CISO Jail Time Over 2016 Data Breach Charges

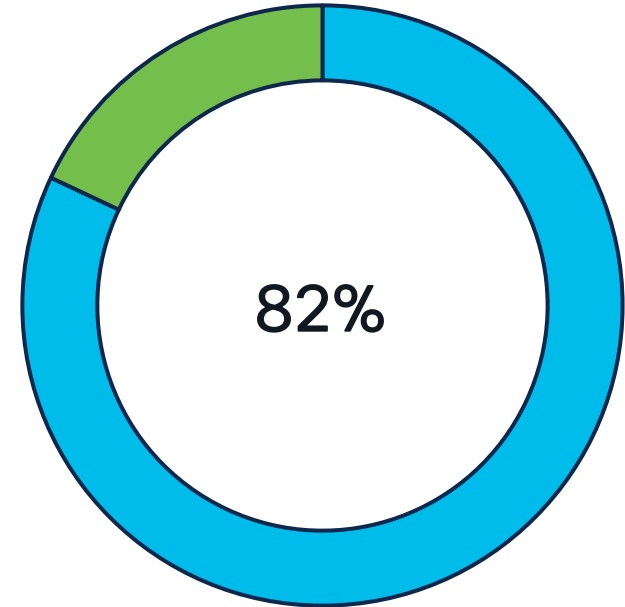
Tell other CISOs "you got a break," judge says in handing down a three-year probation sentence to

**This broken ransomware can't decrypt your files, even if you pay the ransom**

**AVERAGE COST OF UK DATA BREACH HITS £3.2M**

# Cybersecurity Readiness Index

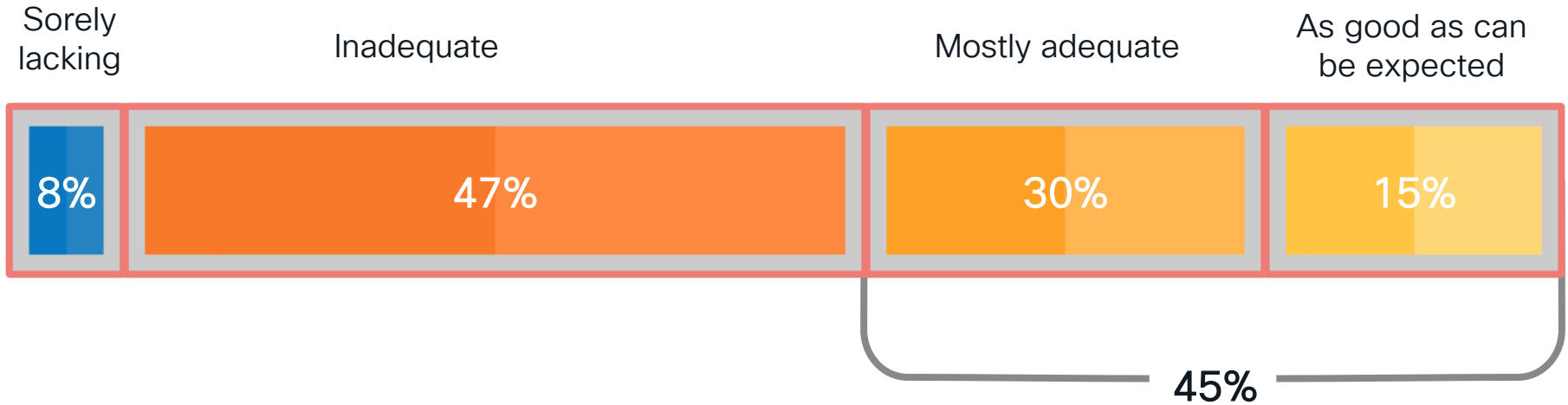
Companies that expect a cybersecurity incident to disrupt their business in the next 12 to 24 months



Source: Cisco Cybersecurity Readiness Index

# Maturity of Cyber Posture

How mature are organisations in their overall cyber posture?



# Conclusions



# Progress towards a cyber secure world



Software engineering  
Software vulnerabilities



Systems operation



Human error  
Decision making



Criminality



Geo-politics

# Recommendations

What can we do?



Get the basics right



Authenticate with MFA



Rehearse incident response



Ensure network visibility



Hunt for incursions

# Webex App

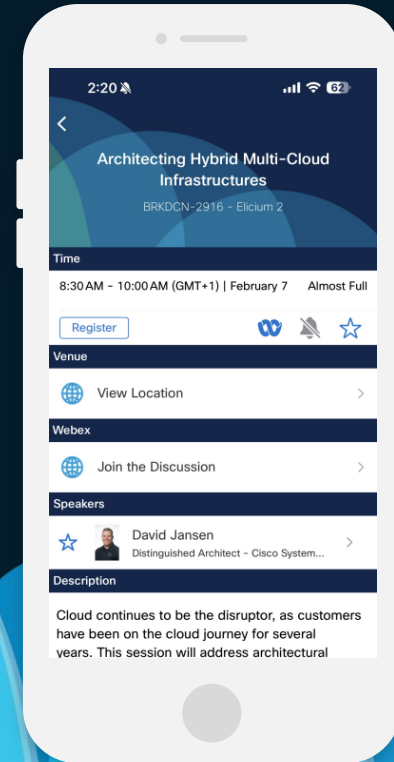
## Questions?

Use the Webex app to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Events mobile app
- 2 Click “Join the Discussion”
- 3 Install the Webex app or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.



# Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)



All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'



Content Catalog

# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [ciscolive.com/on-demand](https://ciscolive.com/on-demand). Sessions from this event will be available from March 3.

Contact me at: [martinle@cisco.com](mailto:martinle@cisco.com)  
[www.linkedin.com/in/martinlee](https://www.linkedin.com/in/martinlee)



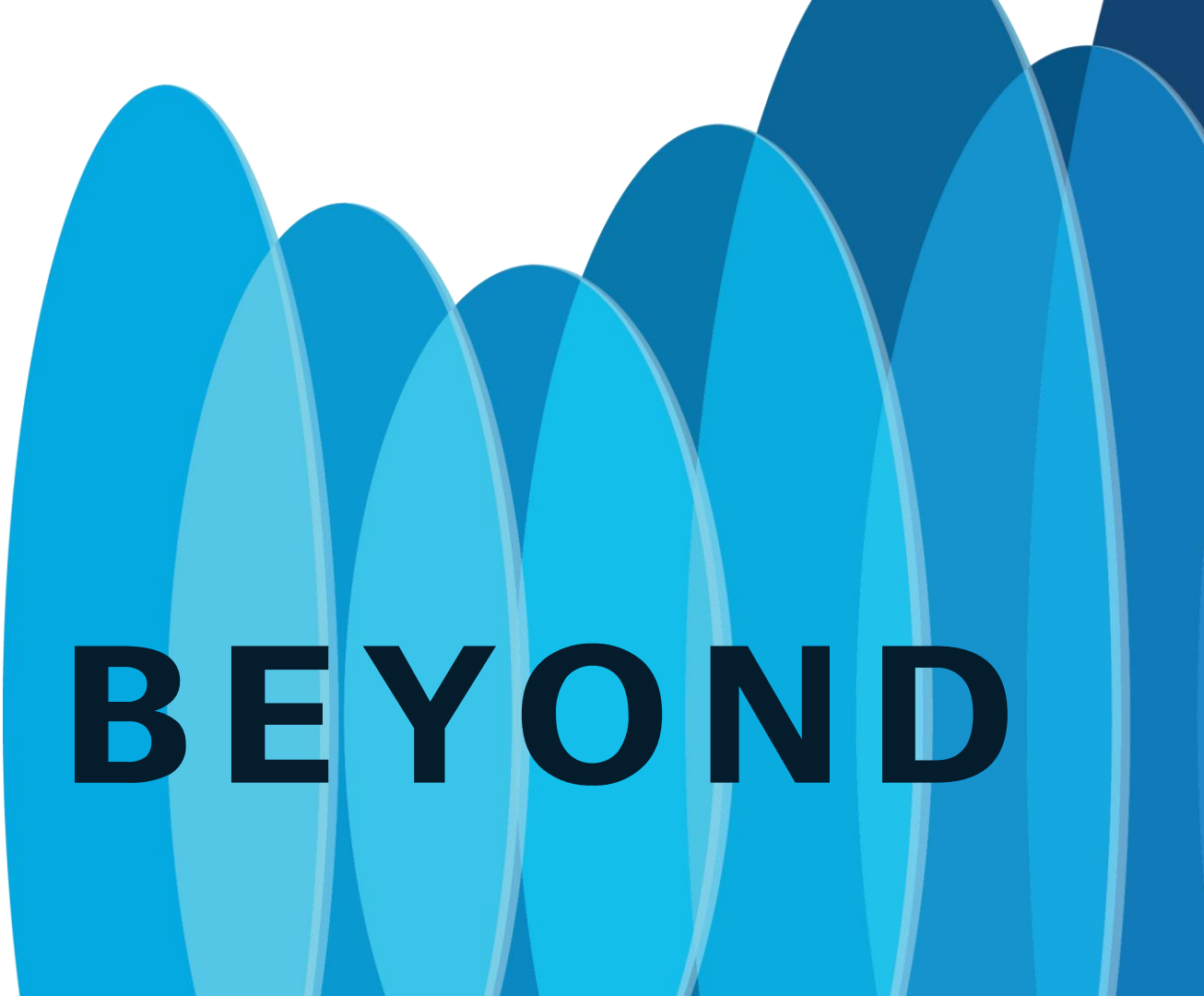
Thank you

CISCO *Live!*



CISCO *Live!*

GO BEYOND

The background of the slide features a series of overlapping, teardrop-shaped elements in various shades of blue, ranging from light sky blue to deep navy blue. These shapes are arranged in a way that creates a sense of depth and movement, resembling a stylized horizon or a series of waves. The overall composition is clean and modern, with the text 'GO BEYOND' prominently displayed in the center.