Solving Cyber Insecurity

Martin LEE

BRKSEC-1159

Agenda

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

A National & Regional Risk

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

Home Office

Department for Science, Innovation & Technology

Experiencing a cyber breach or attack in previous 12 months:

- 50% businesses
- 32% charities

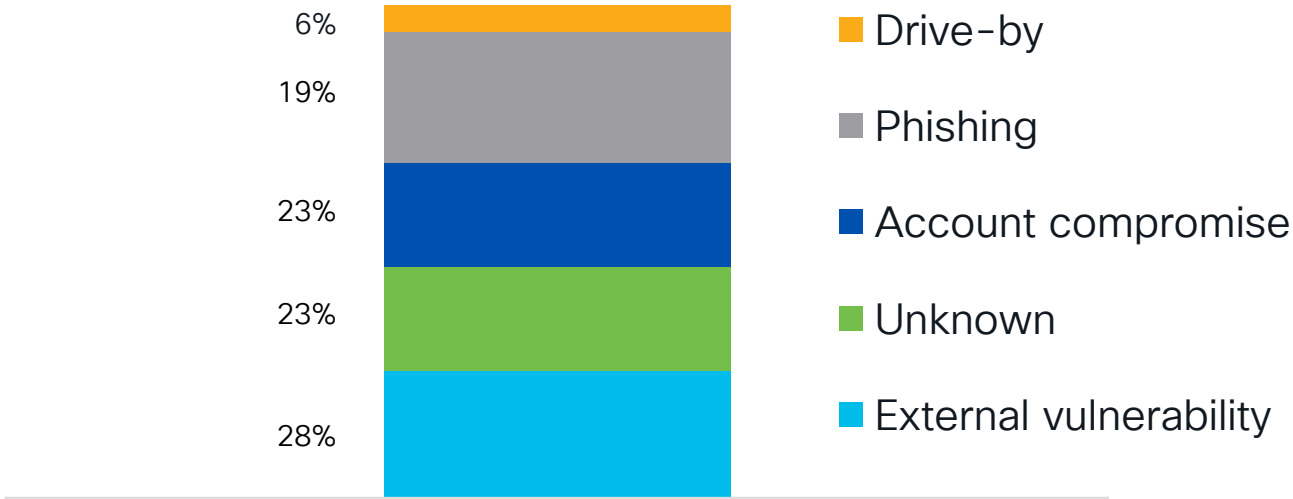
“Just over two-fifths (of these) ended up being victims of cyber crime.”

Also:

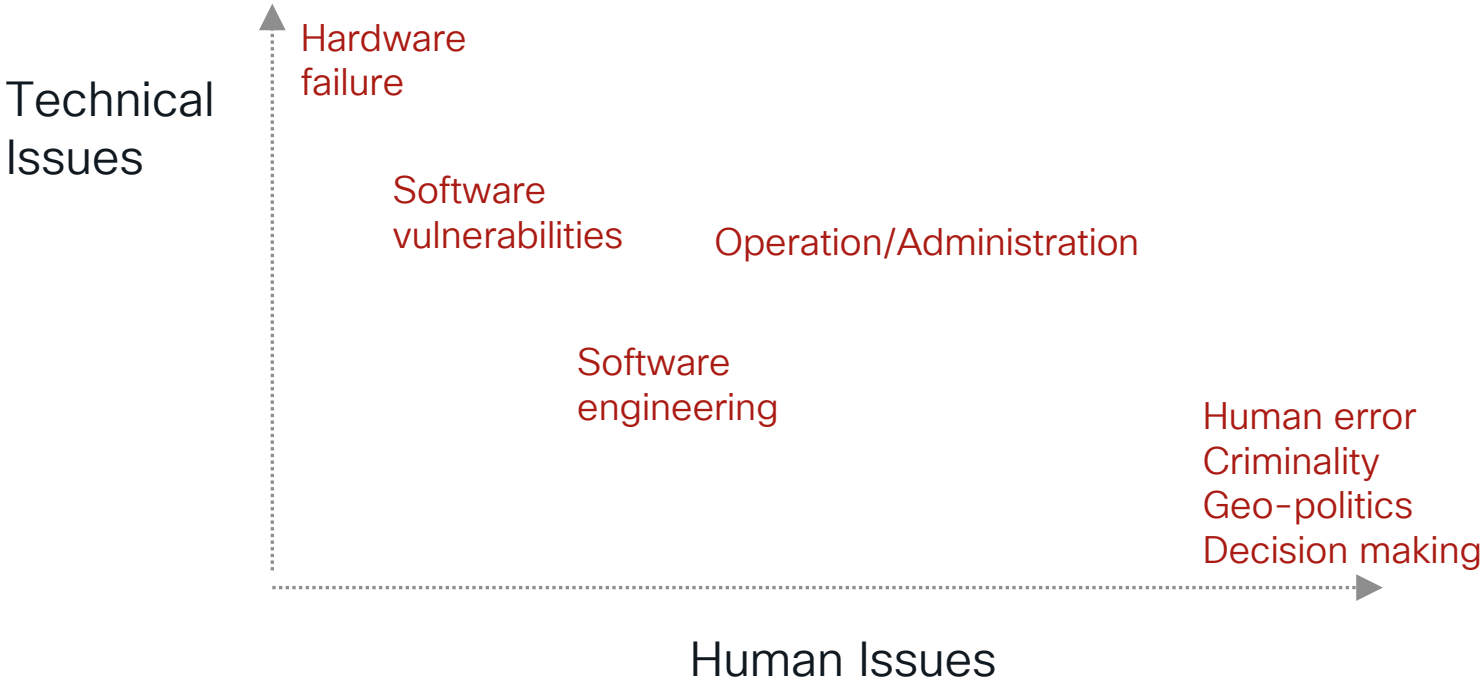
- Unavailability of services.
- Stress, anxiety.
- IT team burnout

Only So Many Ways to Compromise a System

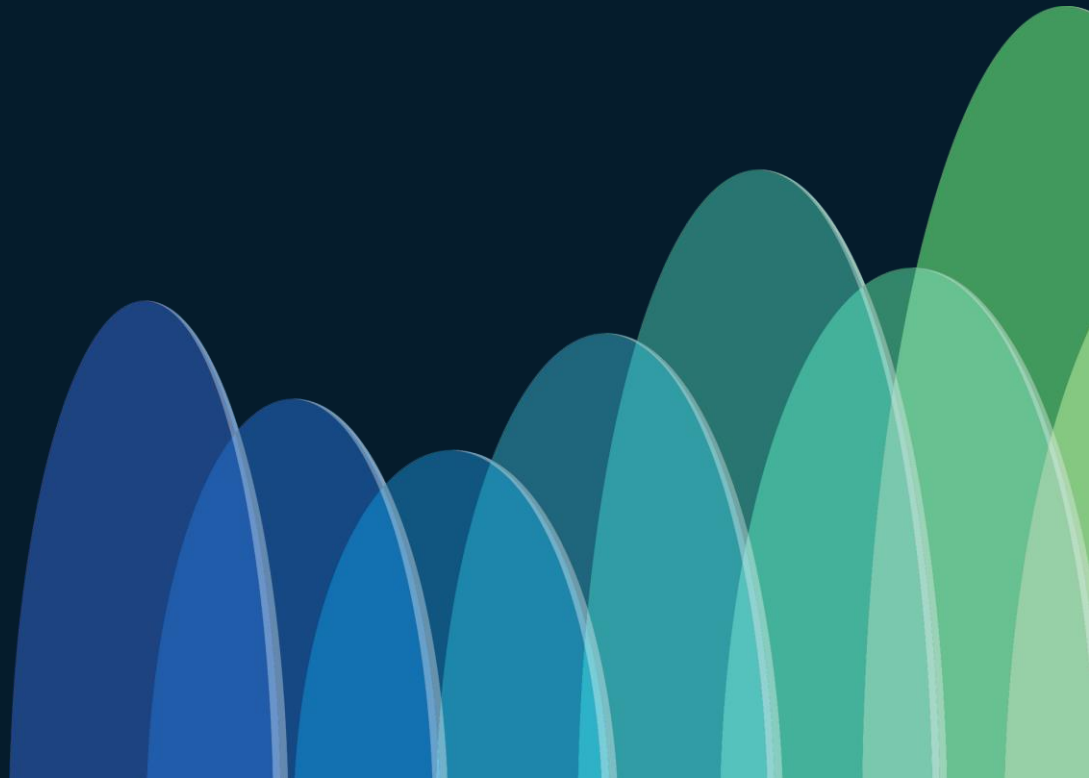
Talos Incident Response data



The Two Axes of Cyber Insecurity



Technical Issues



Writing Software is Hard

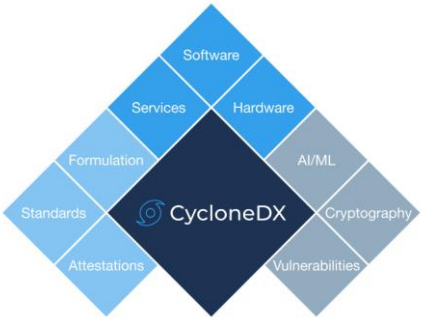
15 weaknesses present every year since 2019!

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

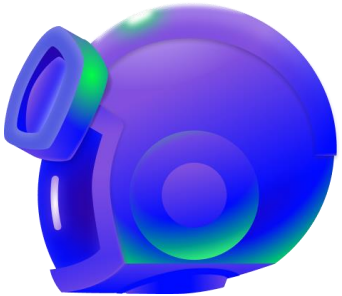
Cisco AI Assistant

Automate routine tasks
Simplify complex tasks

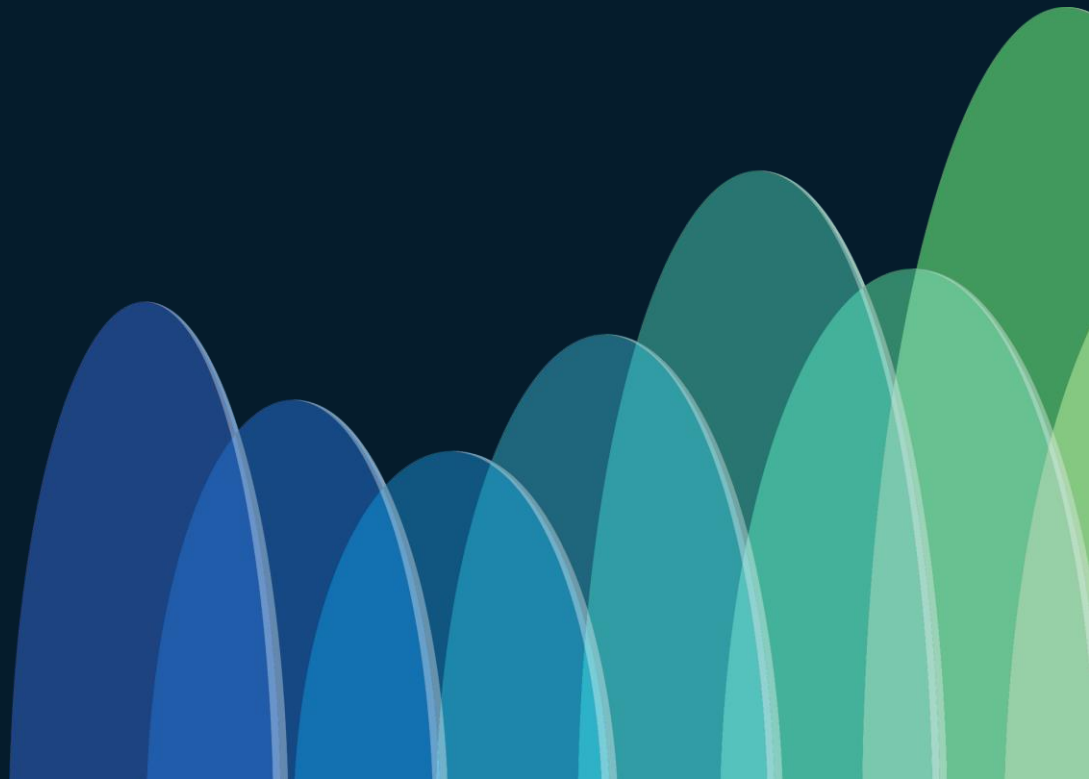
cisco AI Assistant

GitHub Copilot

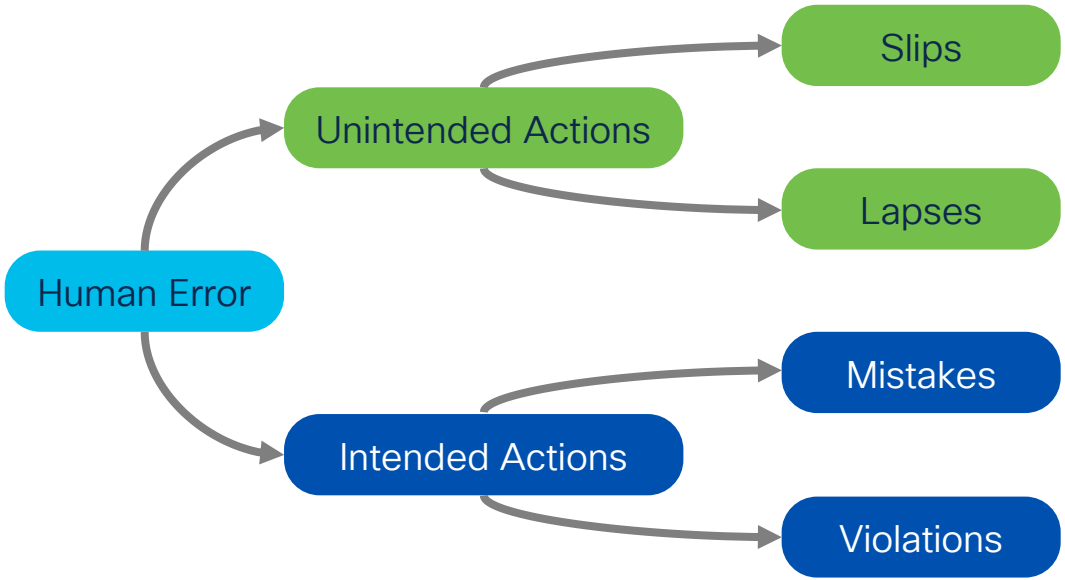
Automate routine tasks
Support developer
Review & improve code



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

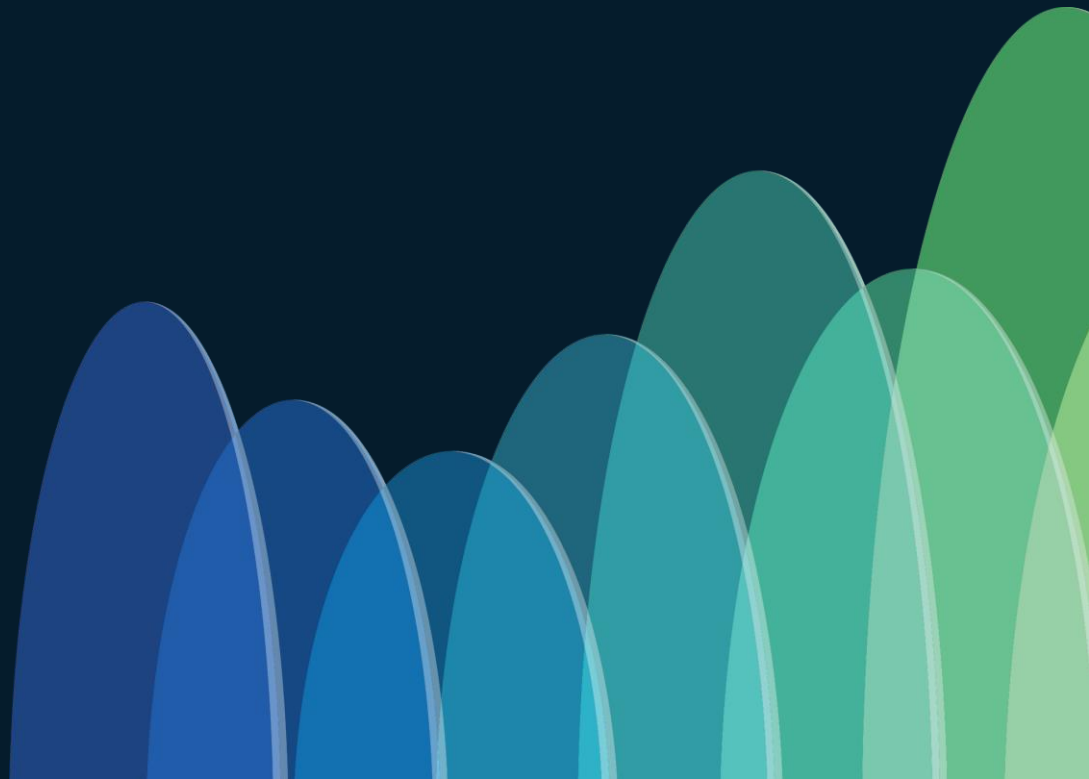
UK-based engineering group identified as target of fraud that used digitally cloned CFO to trick staff

"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!

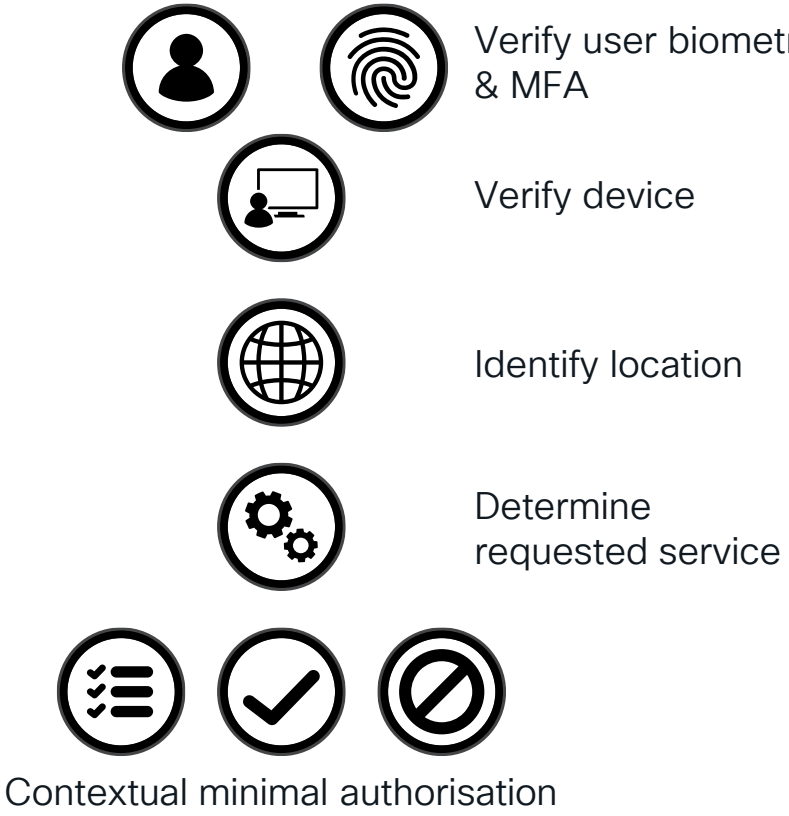
- Shoulder surfing
- Dumping password file
- Credential stuffing

Fernando Corbato

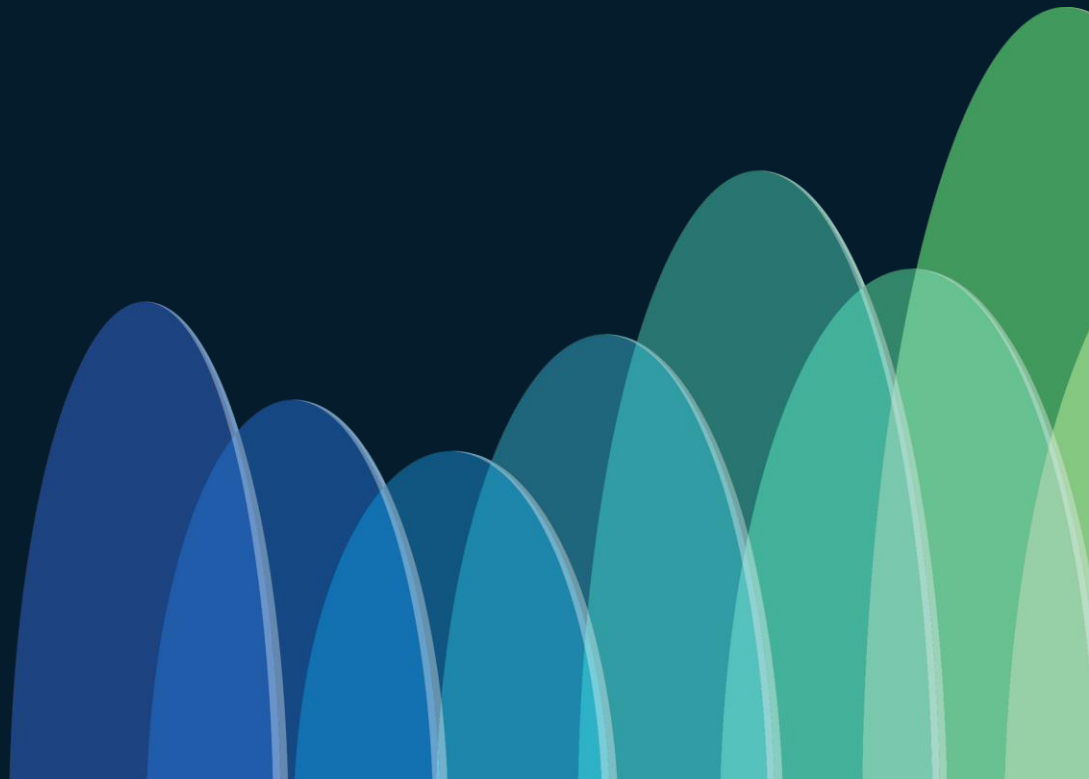
Contextual Authentication

Solving authentication

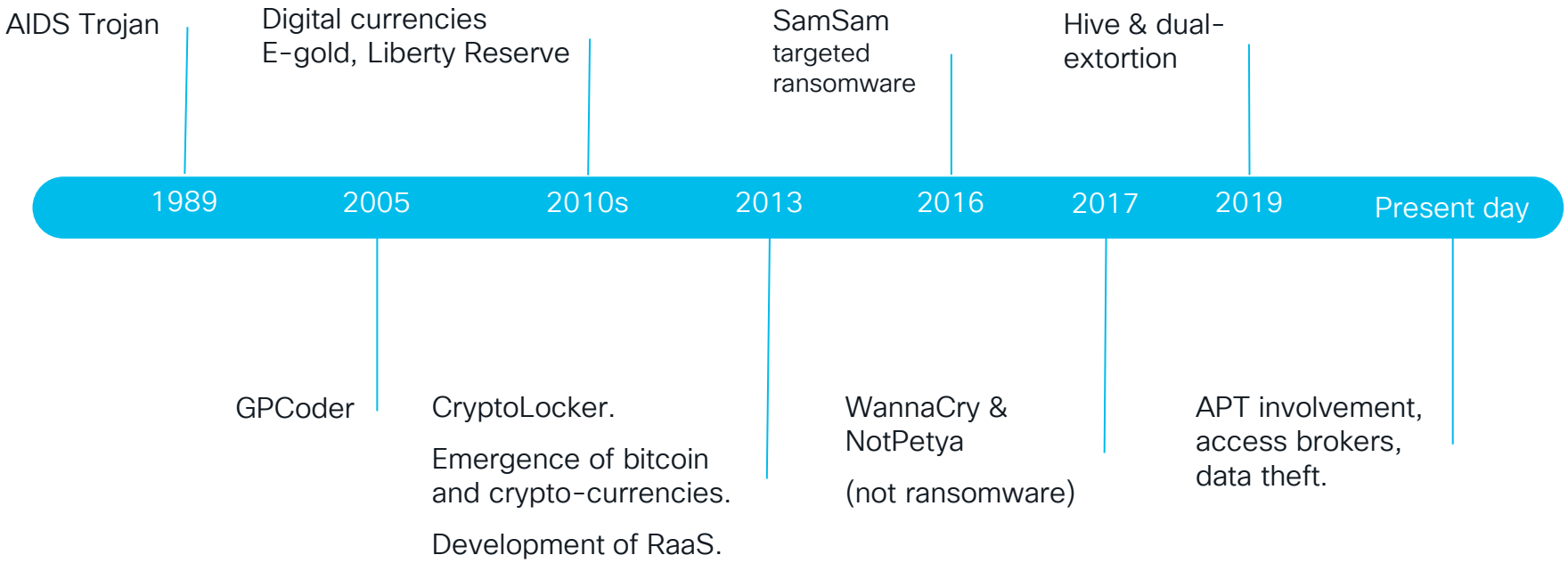
- Not a binary decision
- Based on context
- Permissions are fluid



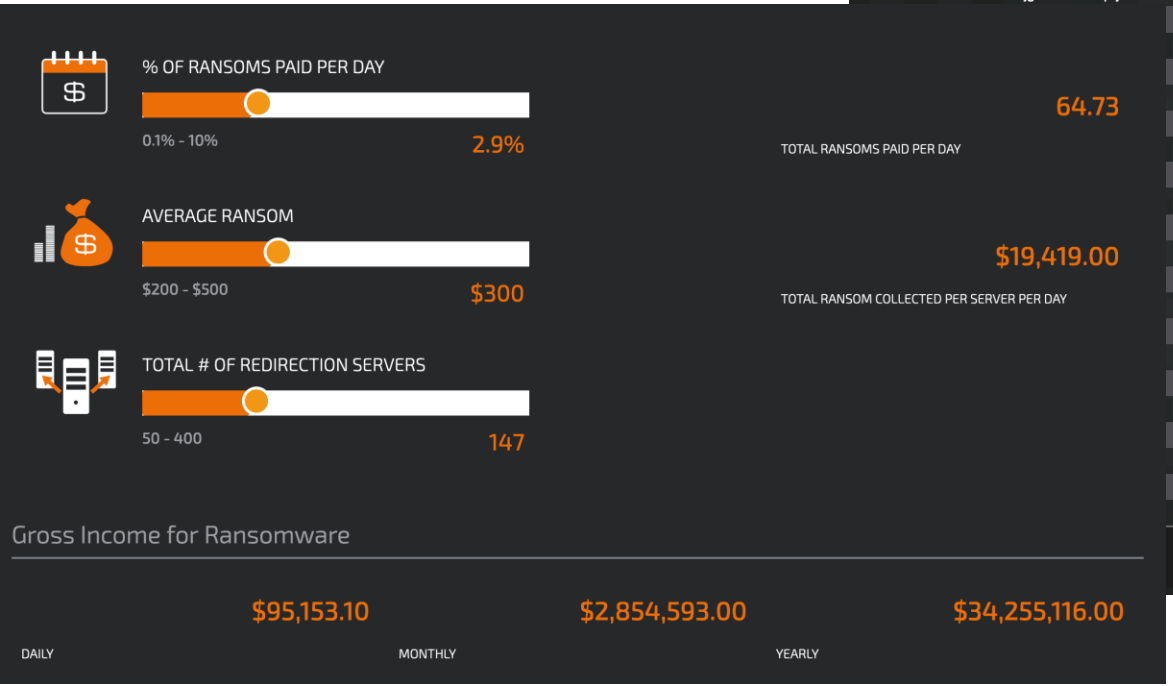
Criminality



Ransomware Evolution



Ransoms Paid

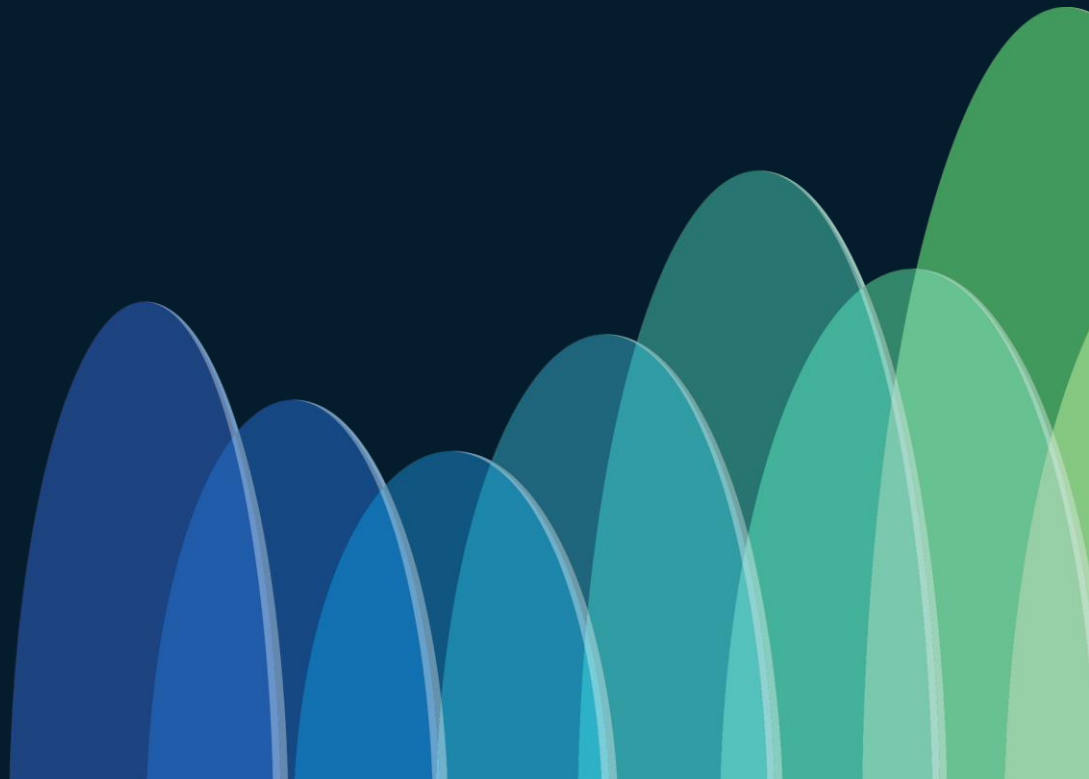


Bitcoin Wallet Address	Bitcoins Received	Value in USD
1Kx9TT76PHwk8sw7Ur6PsMWyEtaogX7wWY	182.9999668	$1,462,484.49
12vsQry1XrPjPCaH8gWzDJeYT7dhTmpcjL	55	$439,544.60
15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj	50.41	$402,862.61
	48.25	$385,600.49
	40.035	$319,948.51
	38.9999859	$311,676.97
	35	$279,710.20
	30.00821708	$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
	700.1079935	$5,515,149.85

Law Enforcement Action

Increase risk, reduce return on investment

Geo-Politics



Advanced persistent threats

Russia	China	Iran	North Korea
• Focused mainly on Ukraine, NATO countries	• Global targeting, specific focus on West & Pacific Rim	• Focused on Middle East, US, Europe	• Global focus
• Goals: • Espionage • Disruption (short & long term)	• Goals: • Intellectual property theft • Economic espionage • Dissidents • Long term persistence	• Goals: • Intellectual property theft • Espionage • Suppression of dissidents	• Goals: • Regime support • Data theft • Financial crimes • Disruption

Russian Military Doctrine

Cyber warfare as part of

“information warfare”

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

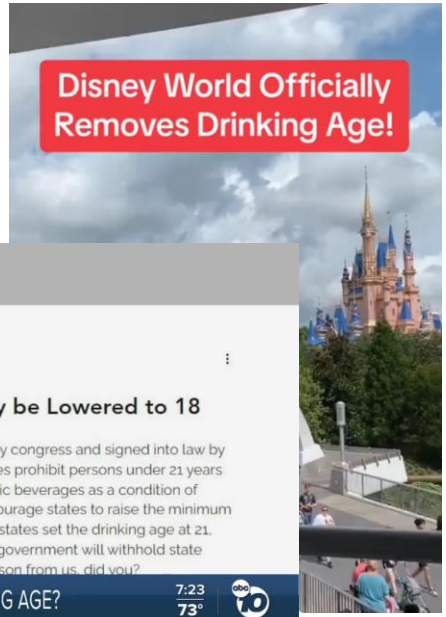
“disrupt the normal functioning of information and telecommunications systems, security and information resources and to obtain unauthorized access to them.”

(Russian Federation Information Security Doctrine, 2000)

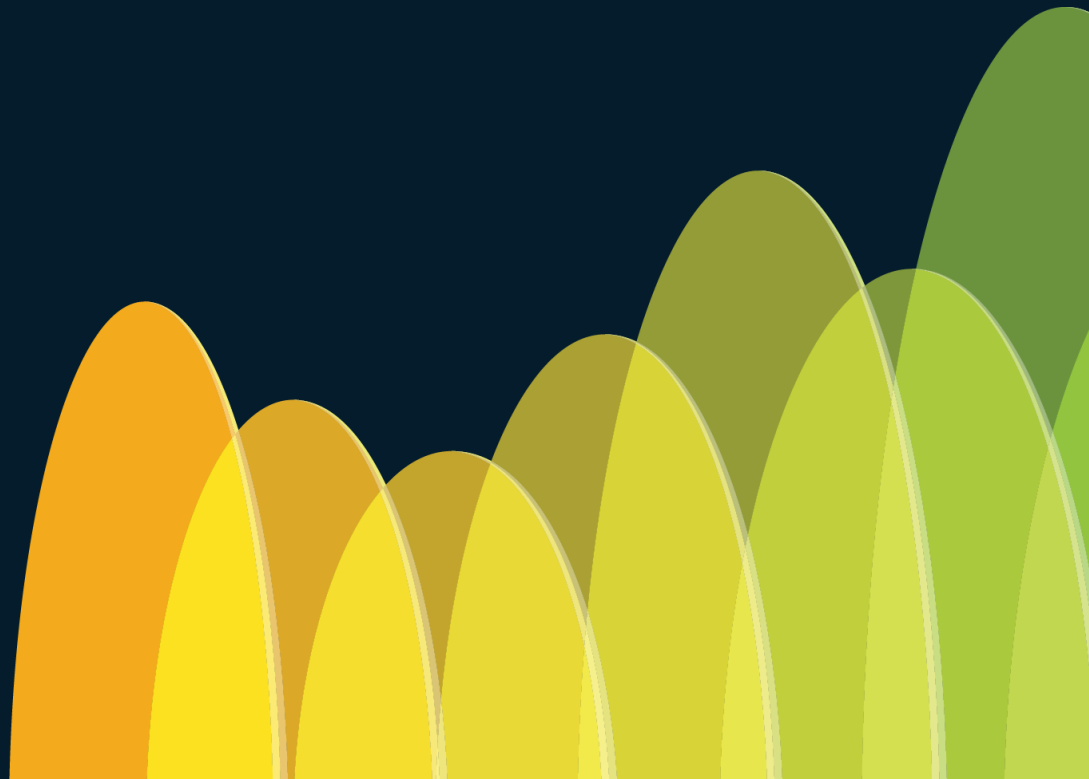
“The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.“

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

Fake News



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

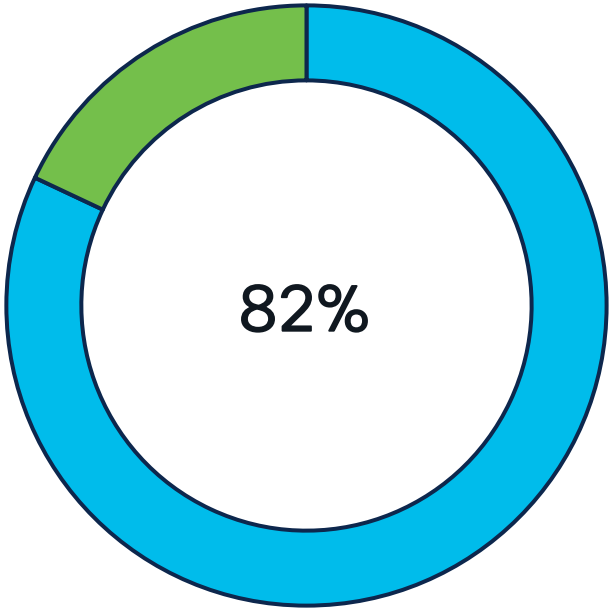
Tell other CISOs "you got a break," judge says in handing down a three-year probation sentence to

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

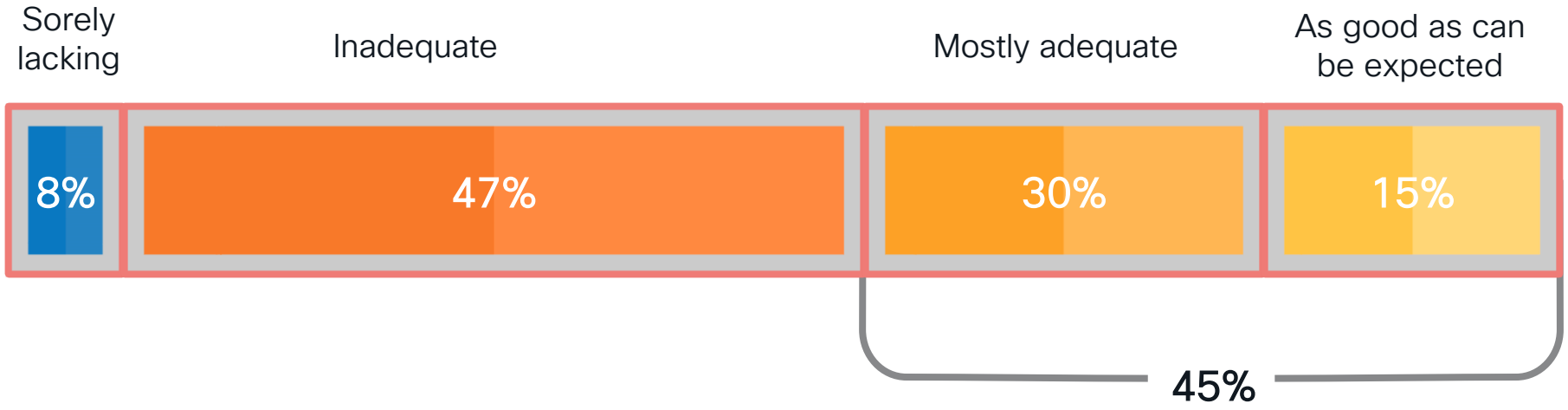
Companies that expect a cybersecurity incident to disrupt their business in the next 12 to 24 months



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

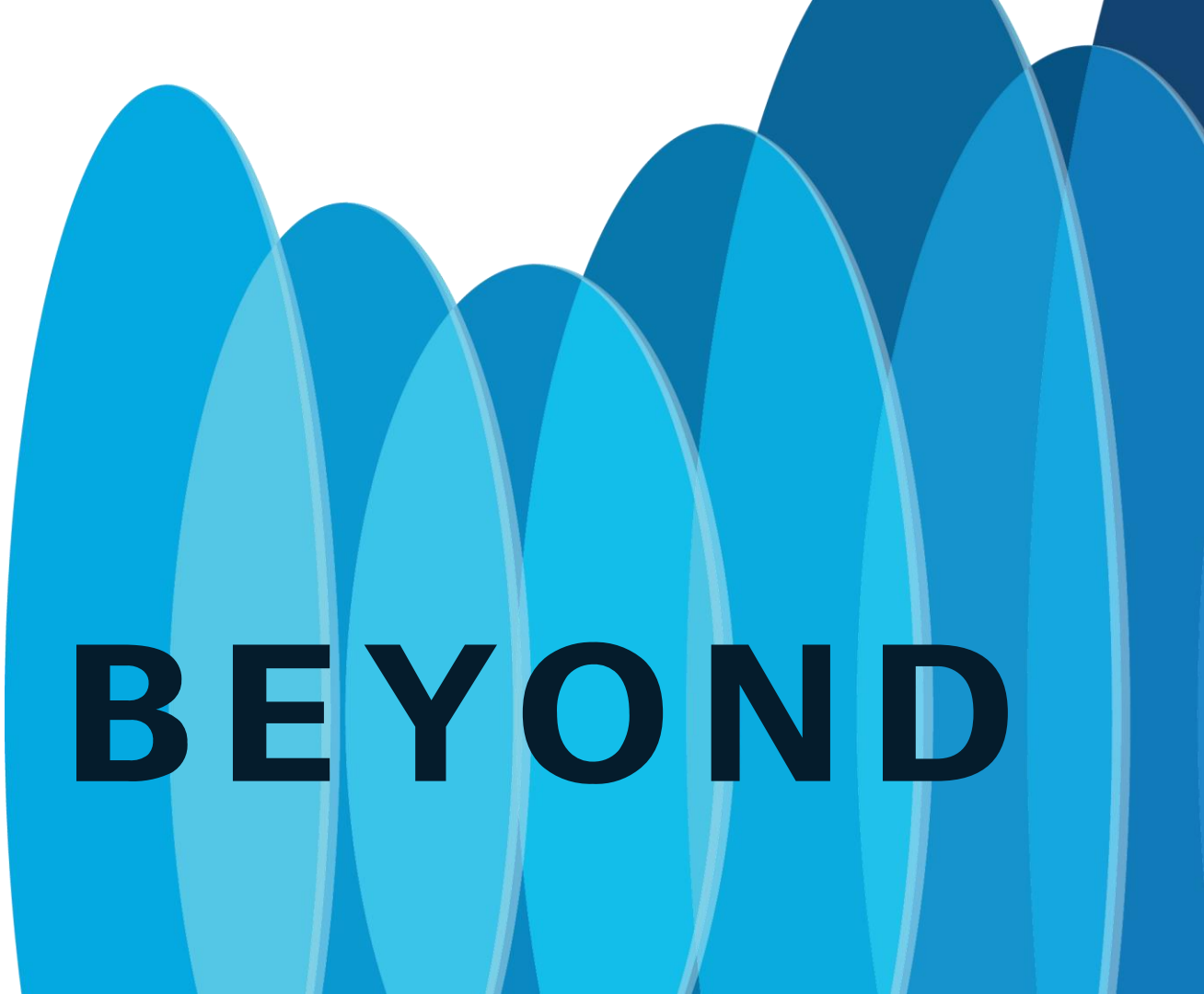
- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from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

Contact me at: martinle@cisco.com
www.linkedin.com/in/martinlee

Thank you

cisco Live!

cisco Live!



GO BEYOND