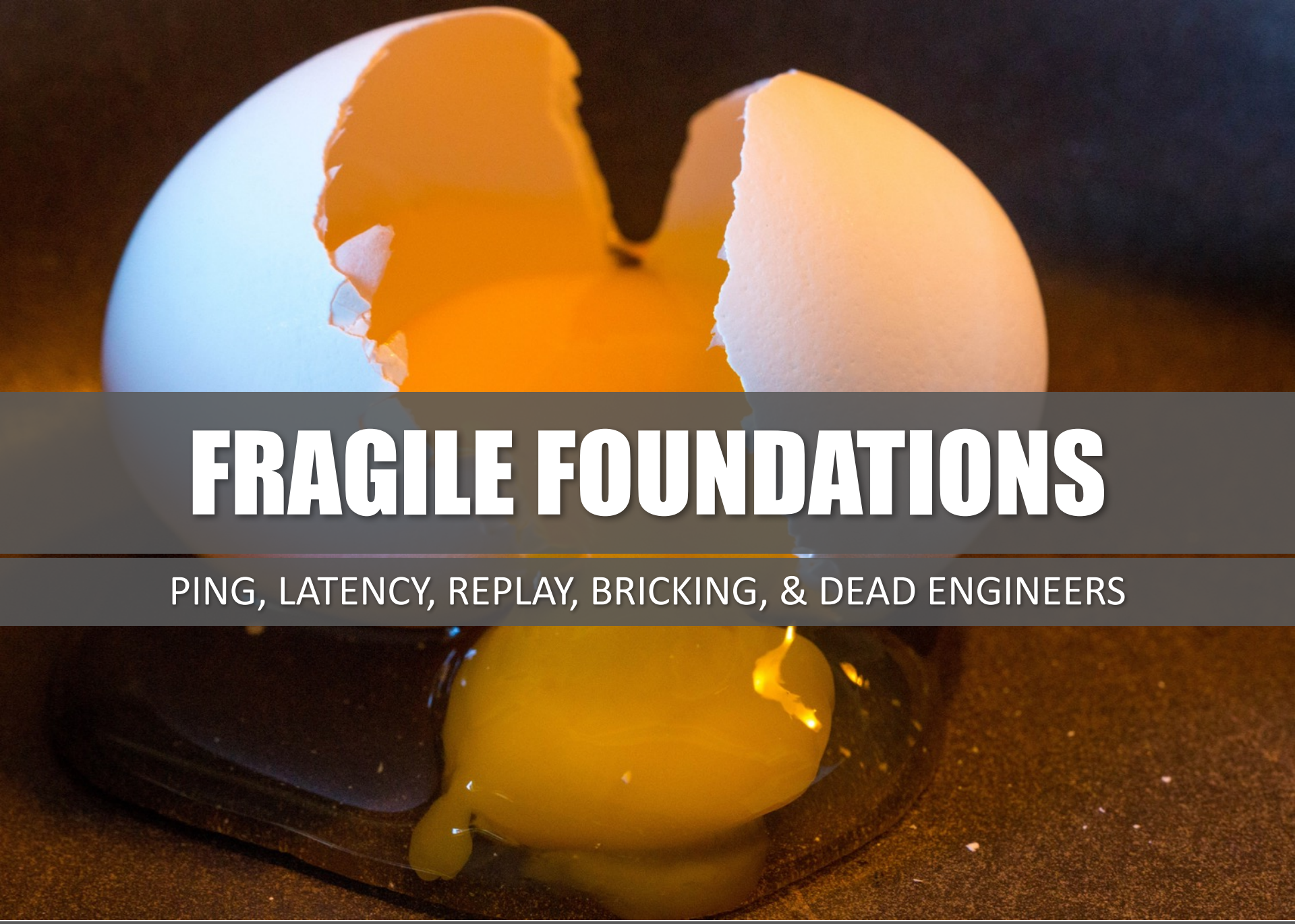
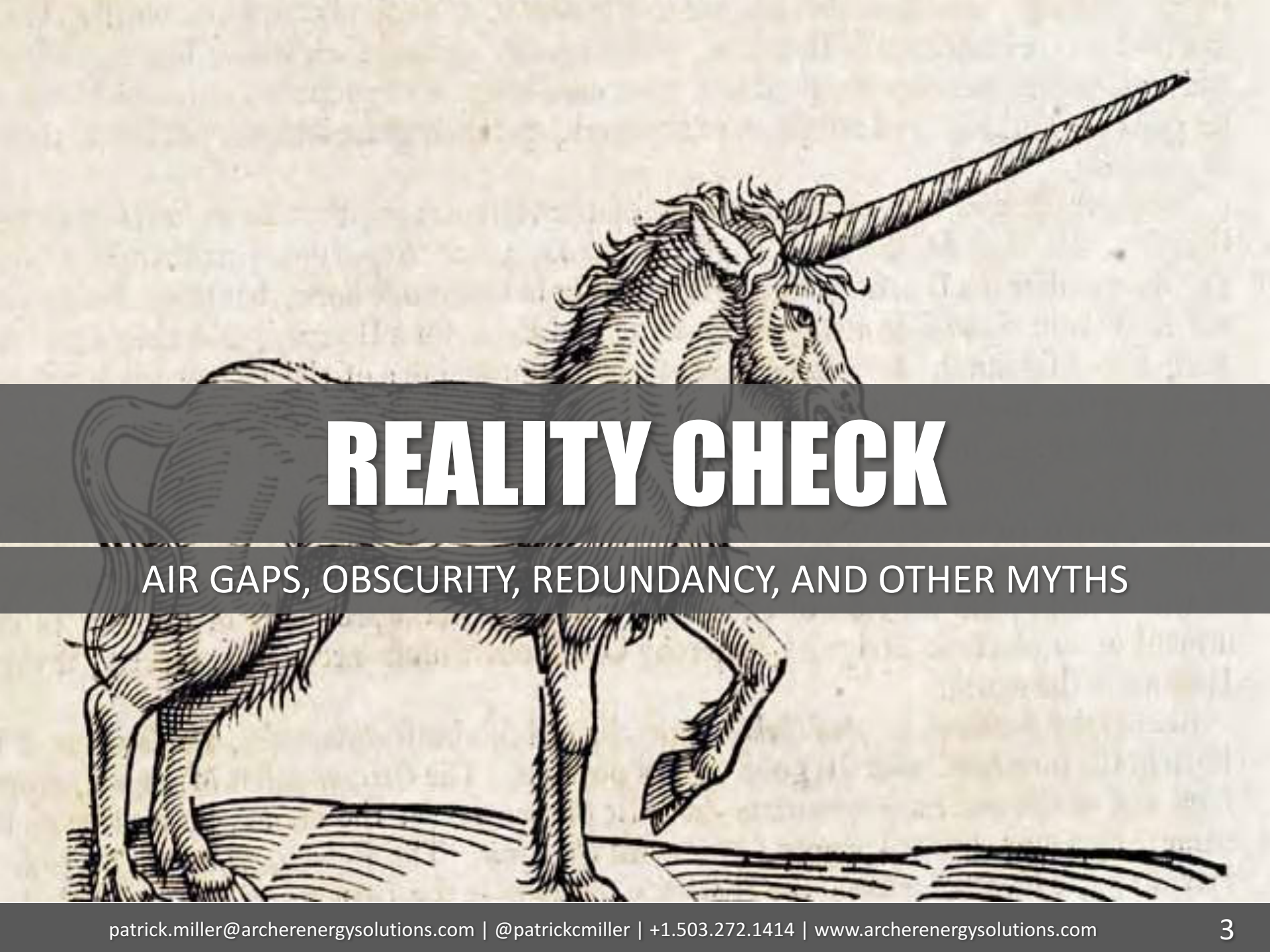
CYBERSECURITY IN THE ENERGY SECTOR

23 del Congreso del Mercado de Energía Mayorista (MEM) | Hotel Hilton | Cartagena, Colombia | November 1 2017



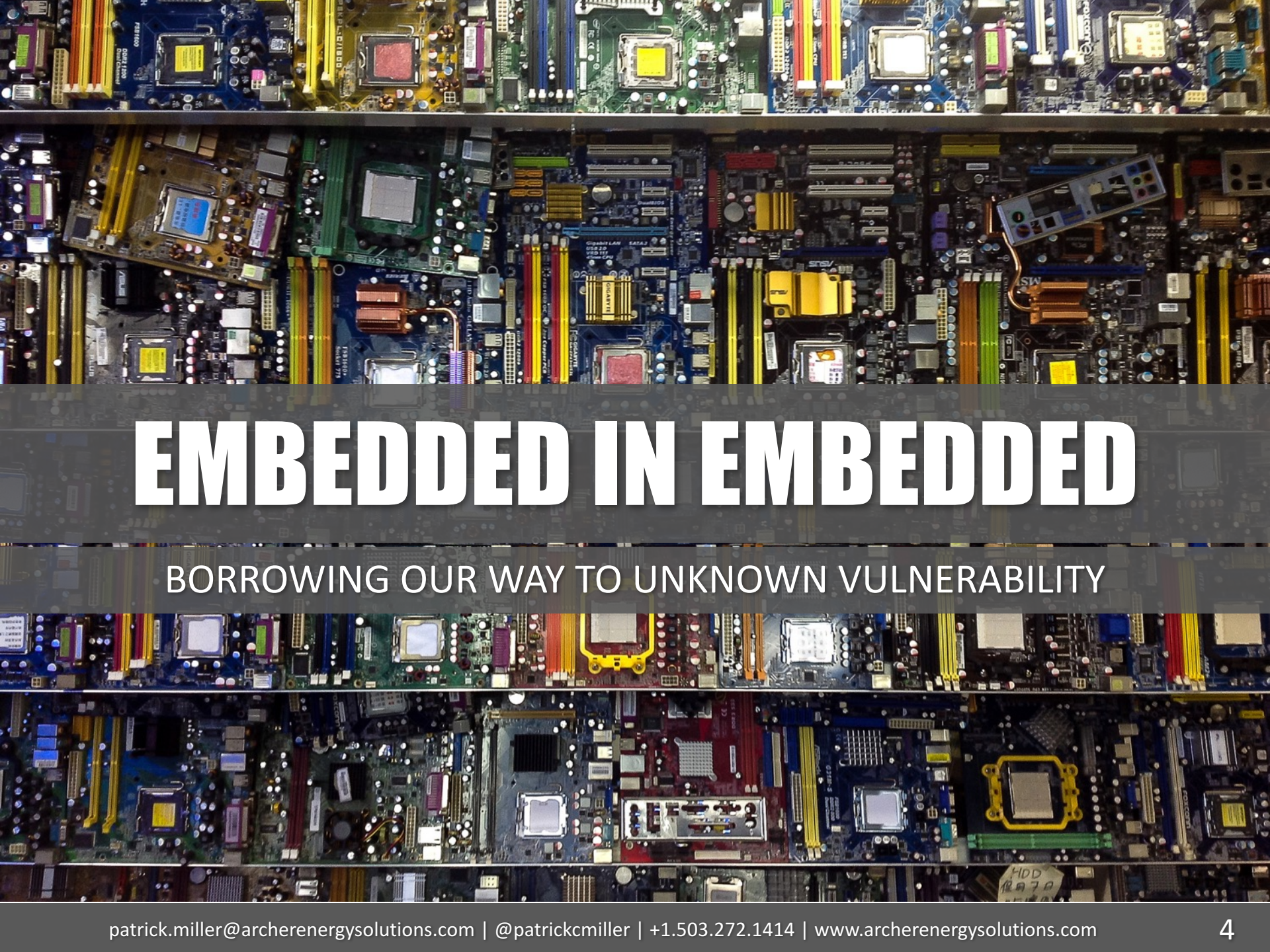
FRAGILE FOUNDATIONS

PING, LATENCY, REPLAY, BRICKING, & DEAD ENGINEERS



REALITY CHECK

AIR GAPS, OBSCURITY, REDUNDANCY, AND OTHER MYTHS



EMBEDDED IN EMBEDDED

BORROWING OUR WAY TO UNKNOWN VULNERABILITY

patrick.miller@archerenergysolutions.com | @patrickcmiller | +1.503.272.1414 | www.archerenergysolutions.com

NOWHERE FOR DATA TO HIDE

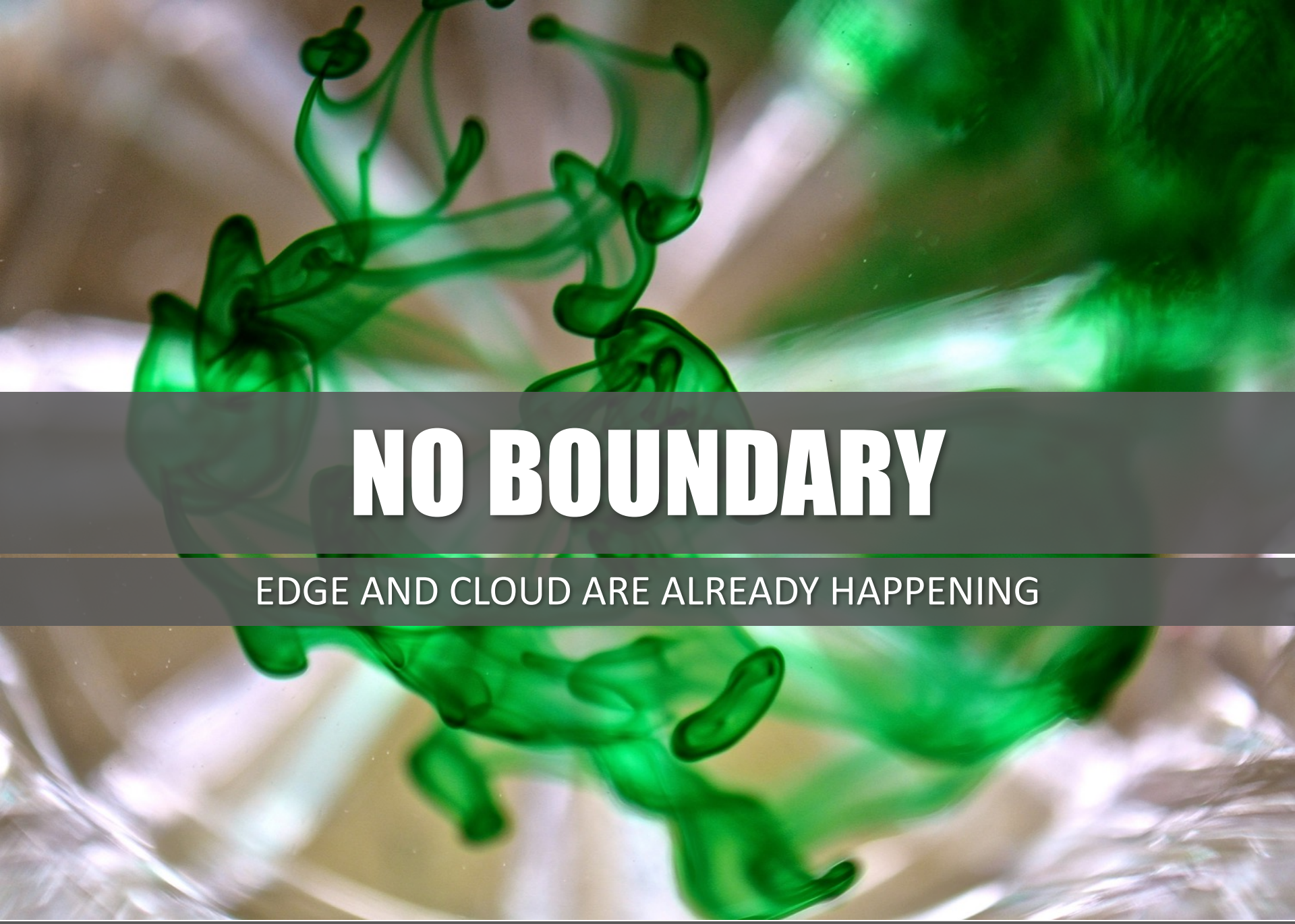
SMART EVERYTHING WILL BE CONNECTED TO SMART EVERYTHING

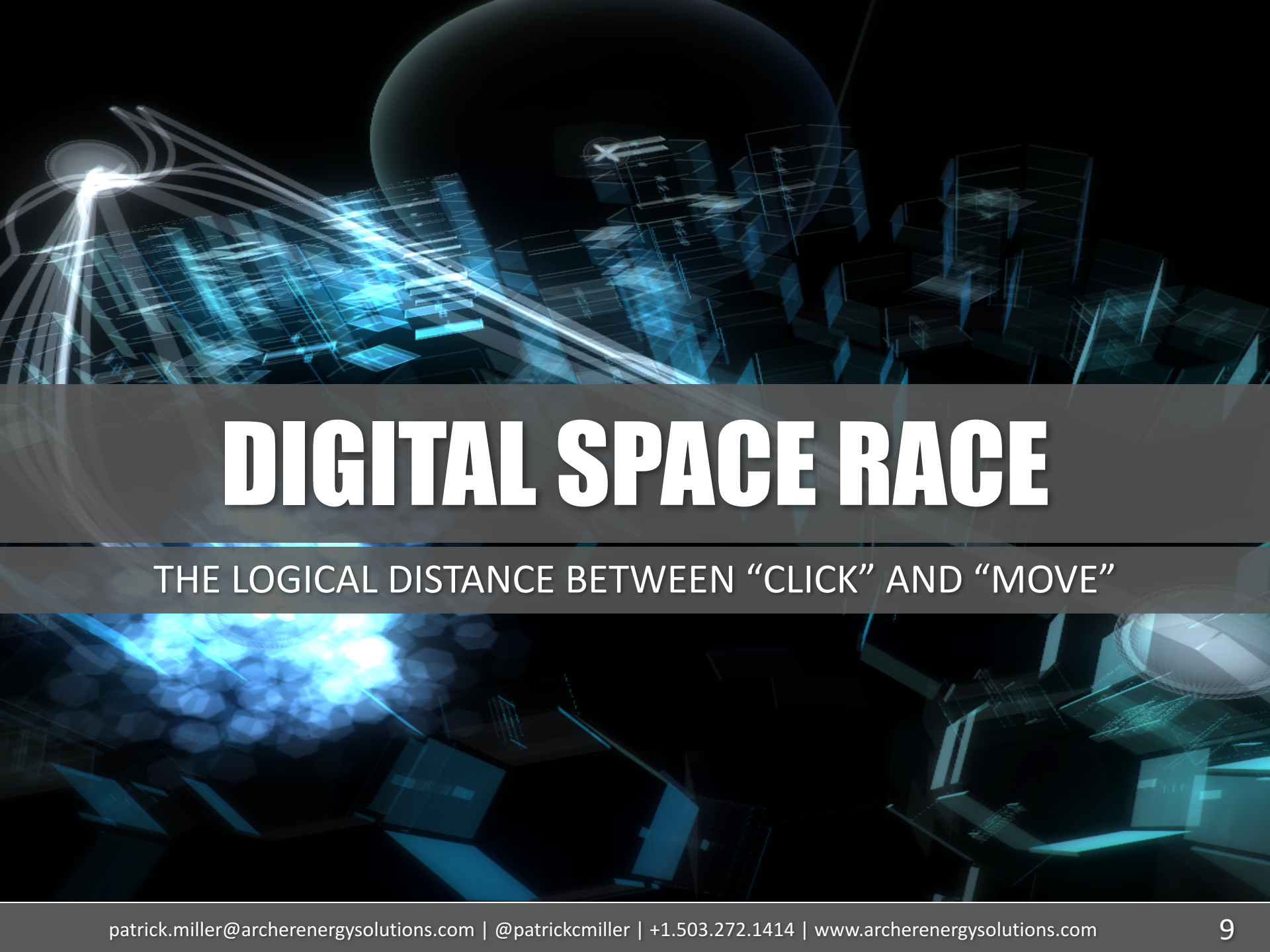
UNSTOPPABLE INNOVATION

TODAY'S GREAT NEW TECH IS TOMORROW'S SECURITY LIABILITY

DISAPPEARING ACT

OLD TECHNOLOGY WILL REMAIN, NEW TECHNOLOGY WILL VANISH


NO BOUNDARY
EDGE AND CLOUD ARE ALREADY HAPPENING



DIGITAL SPACE RACE

THE LOGICAL DISTANCE BETWEEN “CLICK” AND “MOVE”

TECHNOLOGY DEPENDENCE

LOSING TOUCH WITH THE MANUAL CRAFT

GHOST IN THE MACHINE

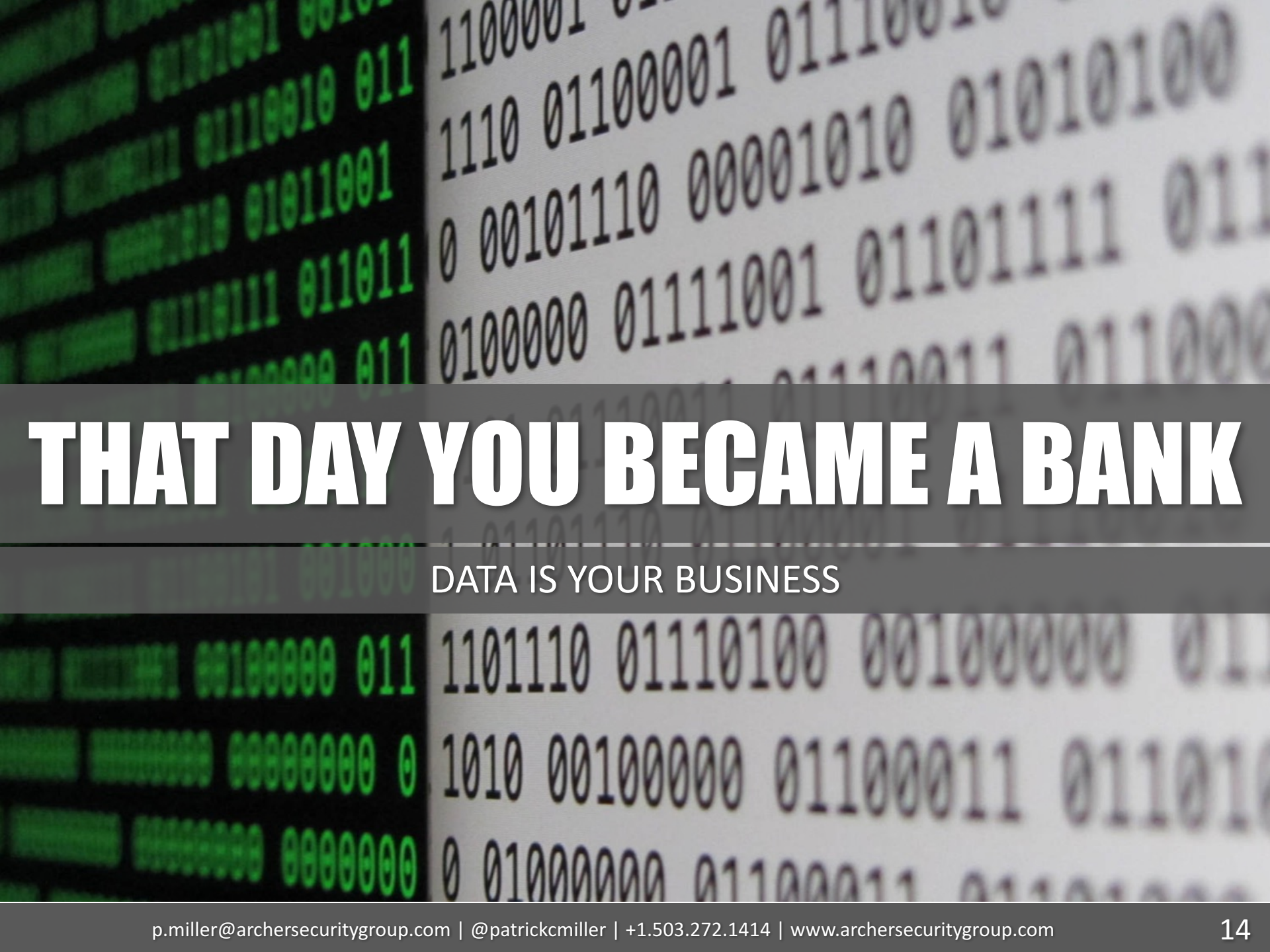
BIRDS, FISH, WILDEBEEST AND MODERN INFRASTRUCTURE

HARD SECURITY TRUTH

EVERYTHING AND EVERYONE CAN BE (PROBABLY HAS BEEN) HACKED

HIGH VALUE/IMPACT TARGET

HISTORY, INTERDEPENDENCY AND COMPLACENCY



THAT DAY YOU BECAME A BANK

DATA IS YOUR BUSINESS

DATA WANTS TO BE FREE

MORE DATA MEANS MORE POTENTIAL FOR LEAKS

ADAPTIVE ADVERSARIES

THEY HAVE THREE THINGS YOU DO NOT: PEOPLE, MONEY AND TIME

NOT ADVANCED
SPREADSHEETS, PDFs AND NAKED CELEBRITIES

ACCIDENTS HAPPEN

SQUIRRELS, CONSTRUCTION EQUIPMENT AND EMPLOYEES

HELP IS UNCERTAIN

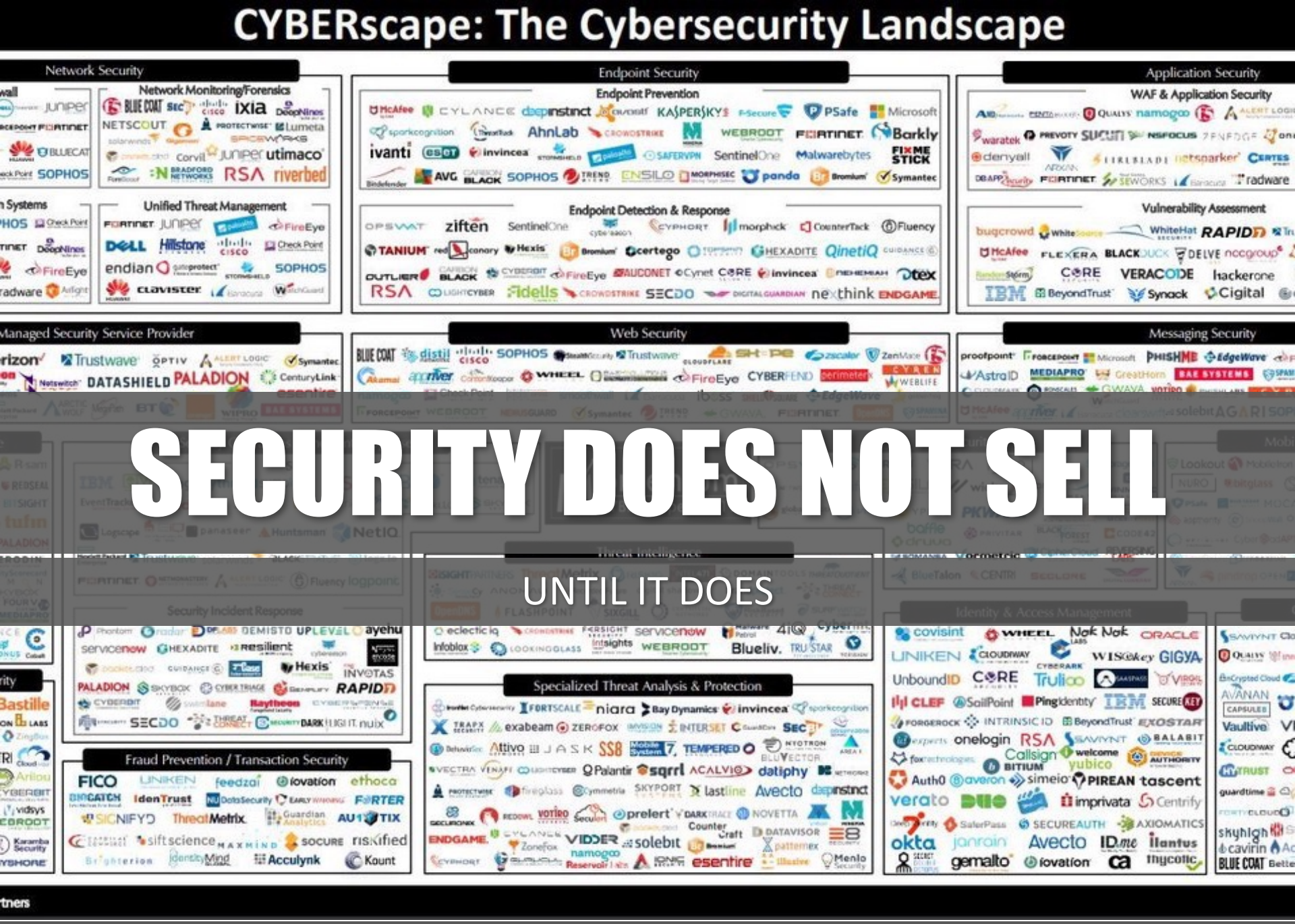
WORKFORCE, INCIDENT RESPONSE AND CYBERINSURANCE

HACKERS ARE FASTER THAN LAWS

YOU CAN PRESCRIBE ACTION, BUT YOU CAN NOT PRESCRIBE ATTITUDE

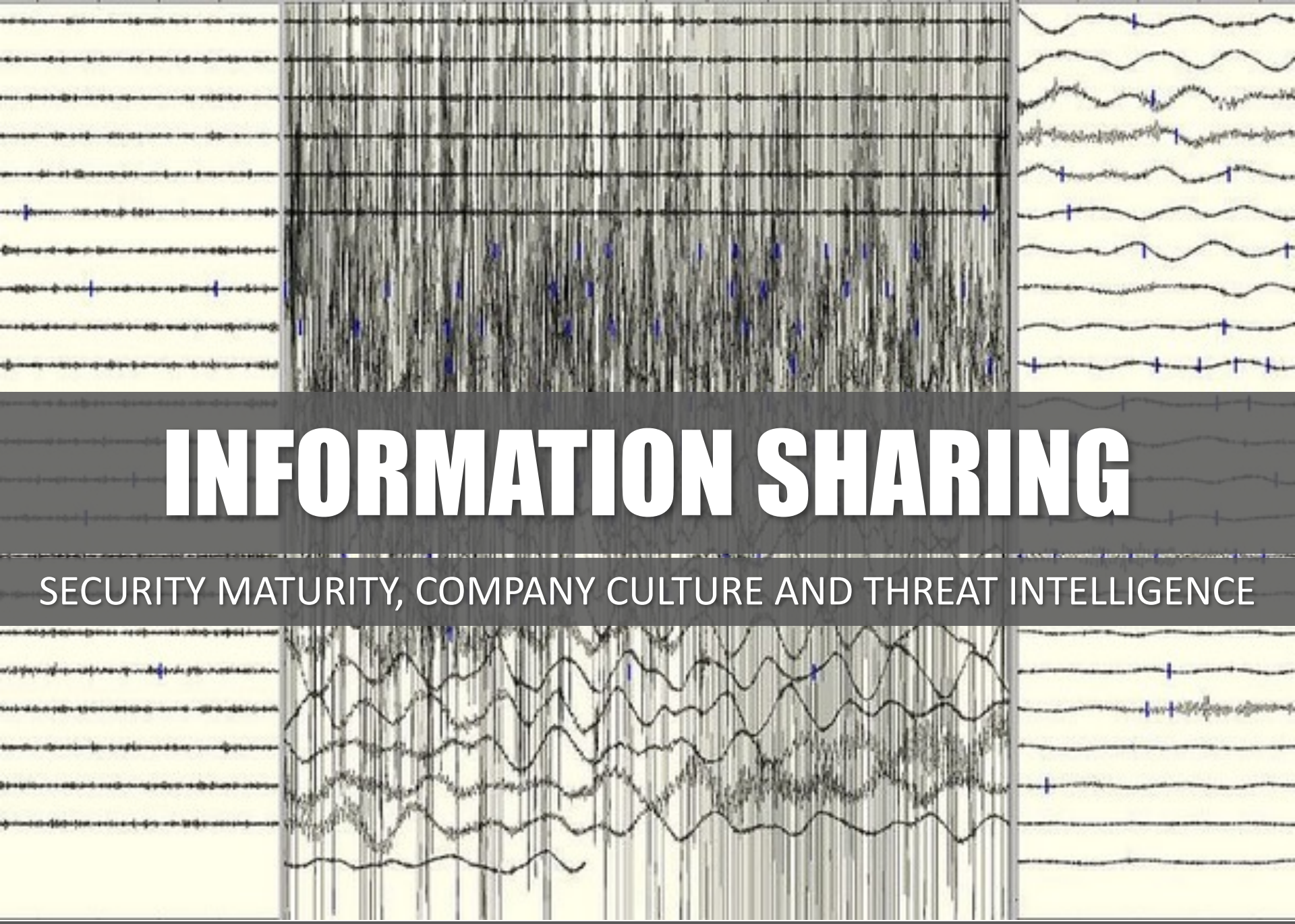
MONEY TALKS

PROCUREMENT LANGUAGE, CONTRACTS AND USER GROUPS


CYBERscape: The Cybersecurity Landscape
Network Security
Network Monitoring/Forensics
Unified Threat Management
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Managed Security Service Provider
Web Security
Messaging Security
SECURITY DOES NOT SELL
UNTIL IT DOES
Security Incident Response
Threat Intelligence
Specialized Threat Analysis & Protection
Identity & Access Management
Fraud Prevention / Transaction Security

THE AWARE PERSON SYSTEM

BEST DEFENSE AGAINST A HUMAN IS A HUMAN



INFORMATION SHARING

SECURITY MATURITY, COMPANY CULTURE AND THREAT INTELLIGENCE

BEER ISAC/CERT

RELATIONSHIPS + TRUST = SHARING

TIME, TOOLS AND MATERIALS

RESILIENCE = BALANCED PREVENTION, DETECTION AND RESPONSE

GIVE SECURITY A NEW NAME

RESILIENCE, RISK REDUCTION, INCREASED UPTIME, DECREASED FINANCIAL LOSSES, YOUR COMPANY/JOB IS DEPENDENT ON IT

PROVEN RESILIENCE

1. REDUCE ATTACK SURFACE AREA
2. BUILD A DEFENDABLE ENVIRONMENT
3. ELIMINATE FRAGILE SYSTEMS
4. MANAGE AUTHENTICATION
5. SECURE REMOTE ACCESS
6. APPLICATION WHITELISTING
7. PATCH MANAGEMENT/CONFIGURATION MANAGEMENT
8. MONITOR EVERYTHING, ESPECIALLY THE NETWORK
9. OVER-PRACTICE INCIDENT RESPONSE AND RAPID RECOVERY
10. MEASURE FOR CONTINUOUS IMPROVEMENT

CREDITS

TITLE SLIDE – HTTPS://FLIC.KR/P/PRYZXB
FRAGILE FOUNDATIONS– HTTPS://FLIC.KR/P/QQM6CZ
REALITY CHECK – HTTPS://FLIC.KR/P/UY1P7R
EMBEDDED IN EMBEDDED – HTTPS://FLIC.KR/P/DBXNKK
NOWHERE FOR DATA TO HIDE – HTTPS://FLIC.KR/P/RGDKDL
UNSTOPPABLE INNOVATION – HTTPS://FLIC.KR/P/6DMHPF
DISAPPEARING ACT – HTTPS://FLIC.KR/P/748TCU
DISSAPEARING ACT – HTTPS://FLIC.KR/P/NGITKE
DIGITAL SPACE RACE – HTTPS://FLIC.KR/P/CRUMXA
TECHNOLOGY DEPENDENCE – HTTPS://FLIC.KR/P/54IIDH
GHOST IN THE MACHINE – HTTPS://FLIC.KR/P/97VZ2T
HARD SECURITY TRUTH – HTTPS://FLIC.KR/P/5PZ1UJ
HIGH VALUE/IMPACT TARGET – HTTPS://FLIC.KR/P/32RDQA
THAT DAY YOU BECAME A BANK – HTTPS://FLIC.KR/P/X9NKBK
DATA WANTS TO BE FREE - HTTPS://FLIC.KR/P/7D1KDC
ADAPTIVE ADVERSARIES – HTTPS://FLIC.KR/P/PHH2VM
NOT ADVANCED – HTTPS://FLIC.KR/P/NKVJ3I
ACCIDENTS HAPPEN – HTTPS://FLIC.KR/P/FAAGDP
HELP IS UNCERTAIN – HTTPS://FLIC.KR/P/6OB8P8
HACKERS ARE FASTER THAN LAWS – HTTPS://FLIC.KR/P/QVNJWJ
MONEY TALKS – HTTPS://FLIC.KR/P/6XSDG1
SECURITY DOES NOT SELL – CCI/MOMENTUMPARTNERS
AWARE PERSON SYSTEM – HTTPS://FLIC.KR/P/RGDKDL
INFORMATION SHARING – HTTPS://FLIC.KR/P/9PQHY4
GET CONNECTED – HTTPS://FLIC.KR/P/8VWTHD
TIME TOOLS AND MATERIALS – HTTPS://FLIC.KR/P/RZEWZI
GIVE SECURITY A NEW NAME - HTTPS://FLIC.KR/P/QXCAH
PROVEN RESILIENCE – HTTPS://FLIC.KR/P/9AXR88

TWITTER: @PATRICKCMILLER
LINKEDIN: LINKEDIN.COM/IN/MILLERPATRICKC
EMAIL: P.MILLER@ARCHERSECURITYGROUP.COM
WEB: WWW.ARCHERSECURITYGROUP.COM
WEB: WWW.PATRICKCMILLER.COM
TEL: +1.503.272.1414