THREAT INTELLIGENCE, INFOSHARING & OTHER MYTHS

YOU ARE NOW A BANK

DATA IS YOUR FUTURE

ADAPTIVE ADVERSARIES

THEY HAVE THREE THINGS YOU DO NOT

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

WE ARE BAD AT RISK

AND WE ARE GOOD AT FORGETTING

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

THE NEW HOLY GRAIL

BUY THREAT INTELLIGENCE OR HACKERS WILL EAT YOUR CHILDREN

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

SO MANY TOOLS

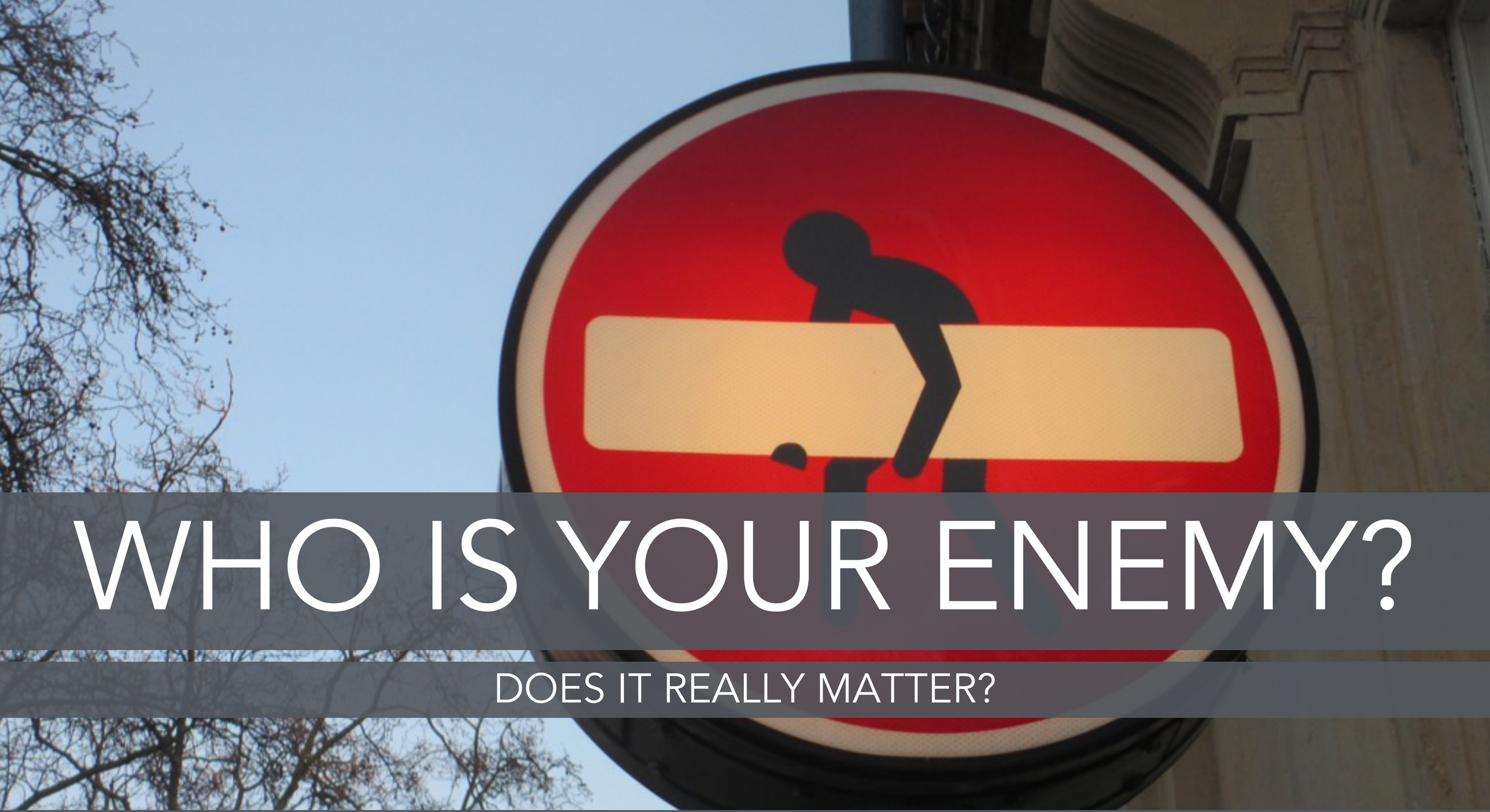
FIREWALLS, IDS, ANTIMALWARE, WHITELISTING, CONFIG, HONEYPOT, AI

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

KNIVES TO GUNFIGHTS

EVEN THE BEST SECURITY ORGS AND TOOLS ARE OR WILL BE HACKED

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com



WHO IS YOUR ENEMY?

DOES IT REALLY MATTER?

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

UNINTENDED USE

WHAT WAS A SECURITY TOOL BECAME AN OPERATIONAL TOOL

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

DOORS & WINDOWS

SECURITY BASICS, TOOL PROFICIENCY & PROCESS MATURITY

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

SIMPLIFY THE PROBLEM

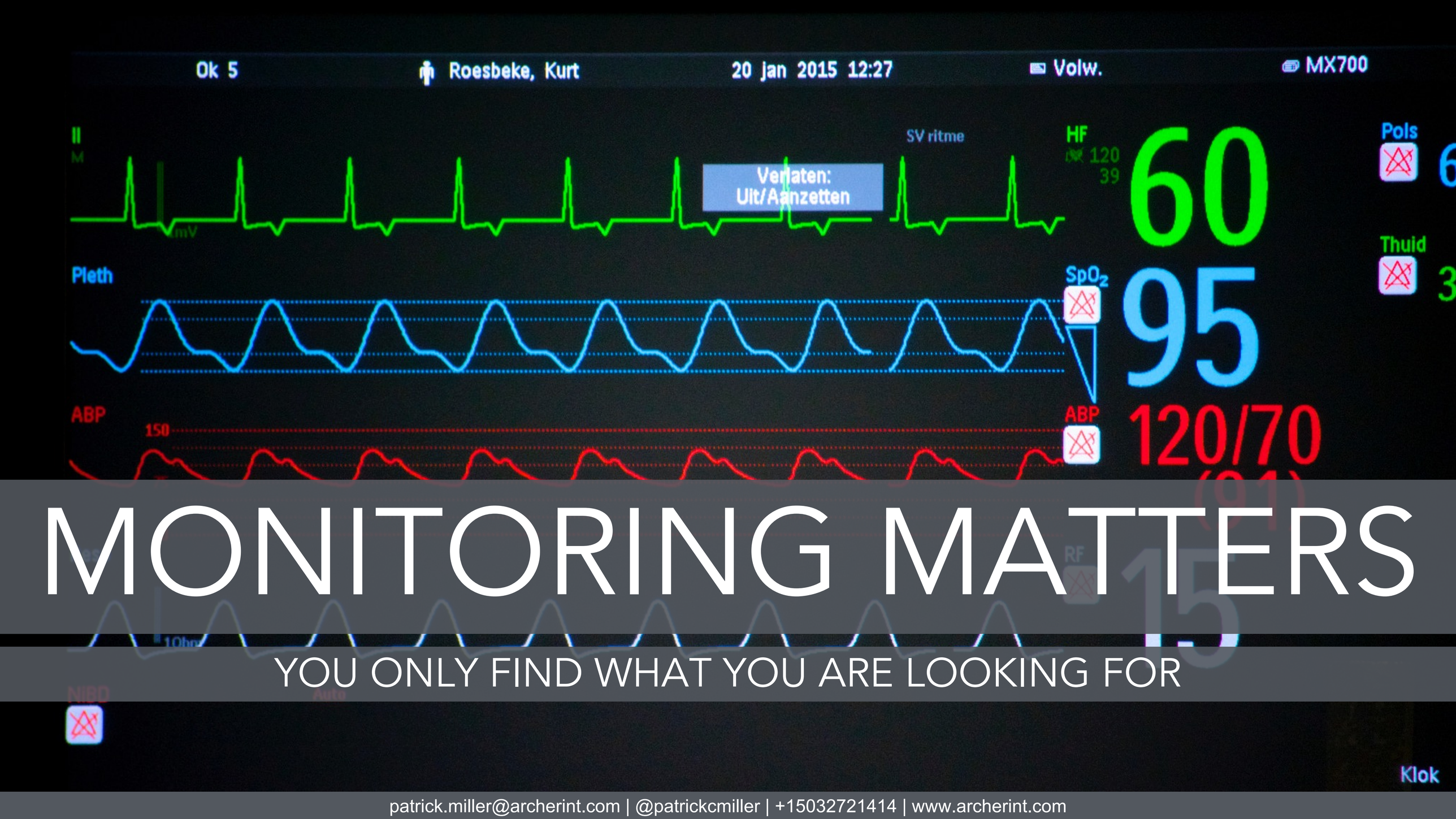
ZERO TRUST, ZERO DEPENDENCE, CONSTANT COMPROMISE

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

LAND OF THE BLIND

START SIMPLE, BUT LOG EVERYTHING EVENTUALLY

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com



MONITORING MATTERS

YOU ONLY FIND WHAT YOU ARE LOOKING FOR

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

AGGREGATION IS HARD

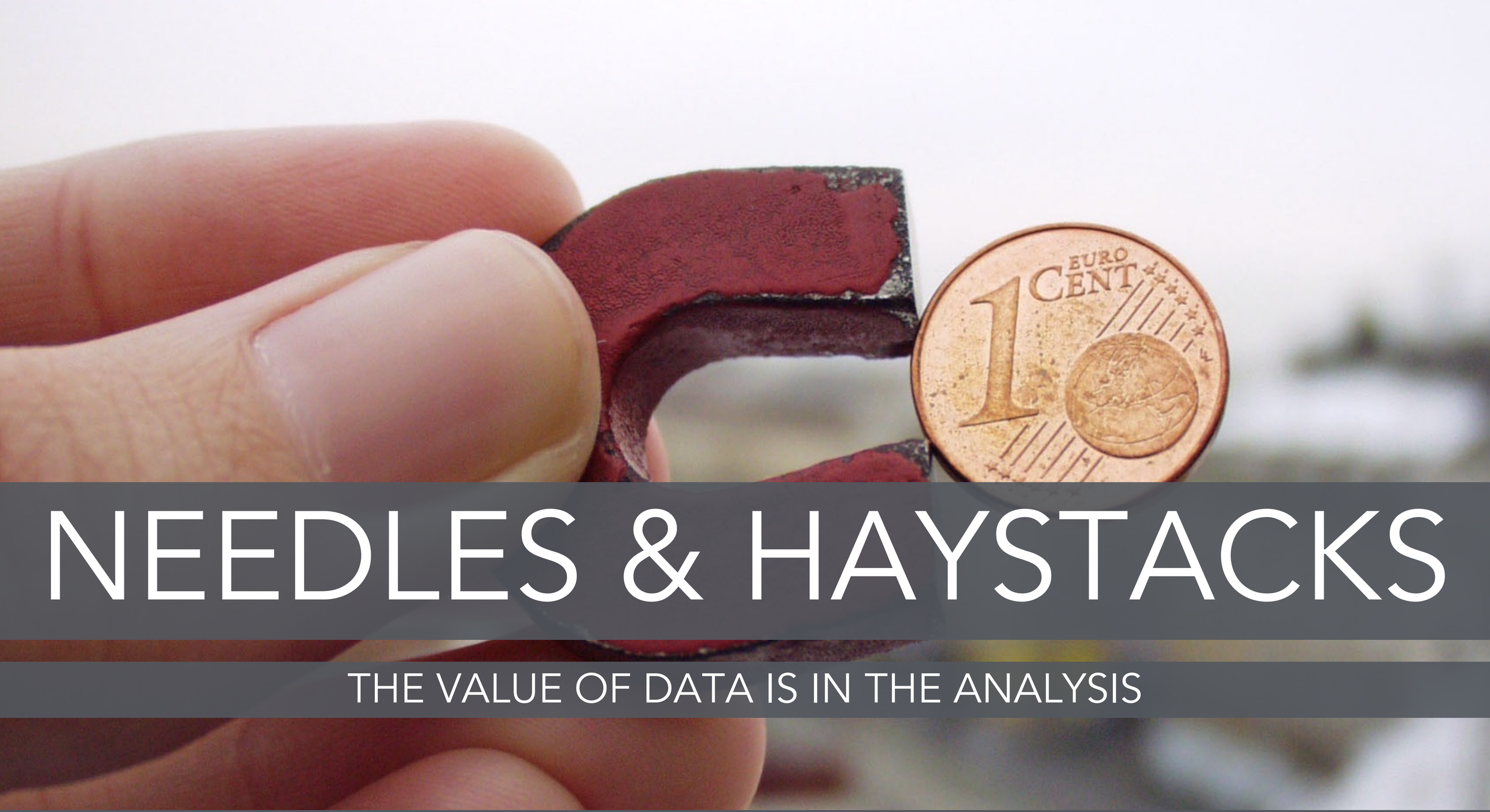
BUT AFTER YOU DO, EVERYTHING ELSE IS EASIER

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

DATA FINDS A WAY

SUTTON'S LAW, HALON'S RAZOR & DATA ENTROPY

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com



NEEDLES & HAYSTACKS

THE VALUE OF DATA IS IN THE ANALYSIS

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

SHARING IS EASY

OR IS IT?

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

TRIO OF TRADEOFFS

ACCURATE, ACTIONABLE OR FAST - PICK TWO (MAYBE)

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

SIZE MATTERS

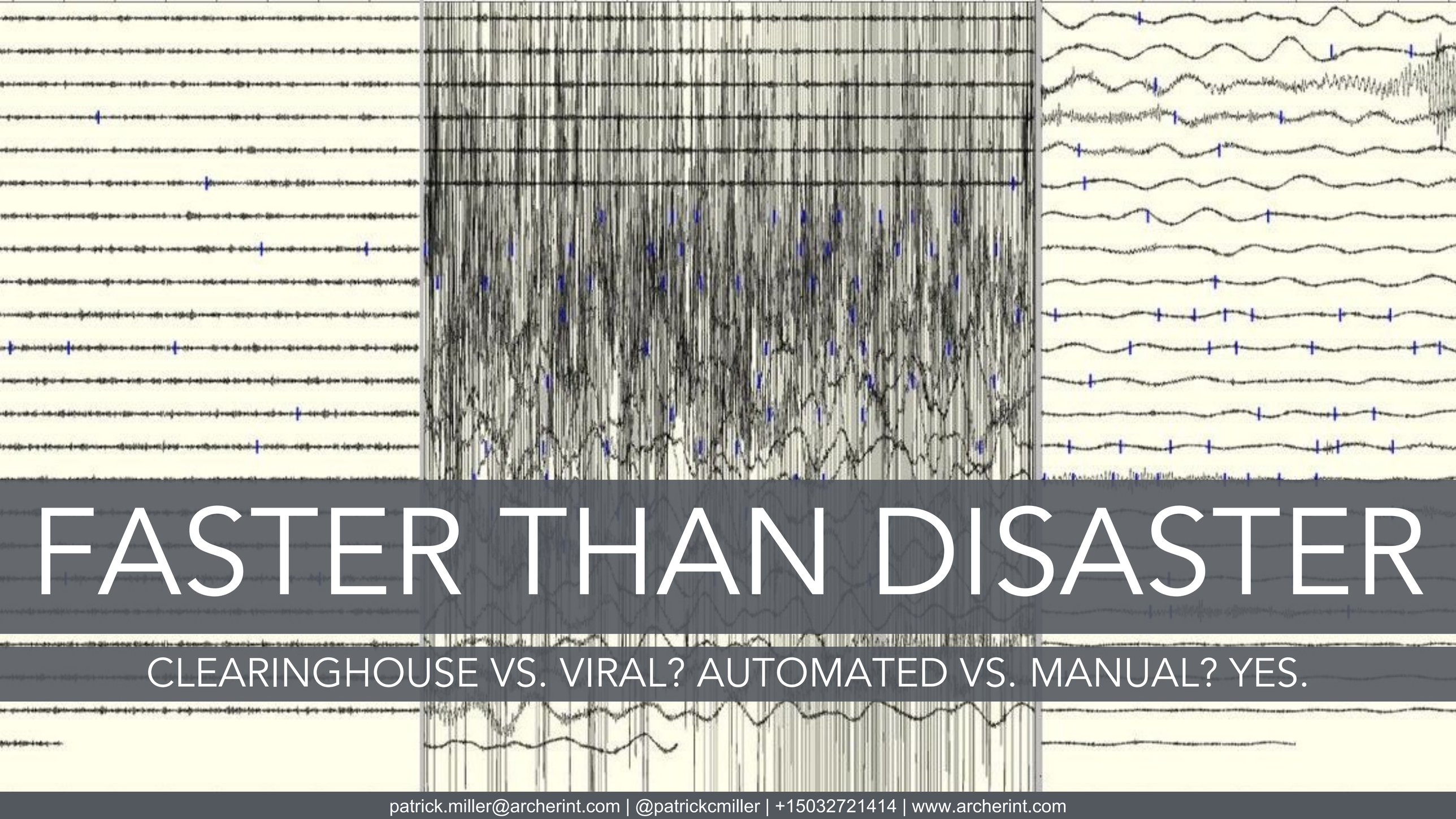
VALUE OF INFO IS INVERSELY PROPORTIONAL TO DISTRIBUTION

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

COMPARTMENTALIZE

SHARE DIFFERENT INFO WITH DIFFERENT CHANNELS DIFFERENT WAYS

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com



FASTER THAN DISASTER

CLEARINGHOUSE VS. VIRAL? AUTOMATED VS. MANUAL? YES.

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

AWARE PERSON SYSTEM

EVERYTHING IN SECURITY COMES DOWN TO YOU

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

WHO DO YOU CALL?

GOVERNMENT AGENCY, CERT, ISAC, SERVICE PROVIDER, OEM, MEDIA

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

GET CONNECTED

RELATIONSHIPS + TRUST = SHARING + ACTION = RESILIENCE

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

WHEN ALL ELSE FAILS

WHAT IF IT REALLY DOES HAPPEN TO YOU?

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

HIGH BUSINESS VALUE

ACTUARIAL DATA, OPERATIONAL EFFICIENCY, REDUCED RISK, RESILIENCE

patrick.miller@archerint.com | @patrickcmiller | +15032721414 | www.archerint.com

LESSONS LEARNED

- SOMEONE WANTS YOUR THINGS & YOU PROBABLY CANNOT STOP THEM
- YOU ALREADY HAVE TOO MANY TOOLS AND NOT ENOUGH PEOPLE
- MASTER BASIC SECURITY PRACTICES BEFORE BUYING ANYTHING ELSE
- THREAT INTELLIGENCE SHARING CAN HELP, BUT ONLY IF READY
- PREPARING TAKES TIME, RESOURCES, NETWORK DESIGN, MATURITY
- TO GET STARTED: LOG, MONITOR, ANALYZE, THEN SHARE
- KNOW WHO TO TRUST WHEN THINGS GO WRONG
- BENEFITS EXTEND BEYOND THREAT INTELLIGENCE & INFOSHARING

@PATRICKCMILLER

LINKEDIN.COM/IN/MILLERPATRICKC

PATRICK.MILLER@ARCHERINT.COM

WWW.PATRICKCMILLER.COM

WWW.ARCHERINT.COM

+15032721414