CRL DISCLAIMER

COUNTY REINSURANCE, LIMITED

County Reinsurance, Limited

01

The information contained in this presentation is for educational purposes only and should not be construed as an endorsement of any kind for any vendor, service, or technology.

02

Do your own due diligence.

You are encouraged to conduct your own research and due diligence before making any decisions based on the information presented.

03

No Legal Advice.

The information presented is not a substitute for legal advice. Please consult with a qualified legal professional for advice specific to your situation.



CRL | County Reinsurance, Limited

Silent Entry, Public Impact: AI-Driven Attacks and Insurance Exposure

What Insurance Leaders Need to Understand in 2026 and Beyond



Are your insureds exposed before they even know it?

PEOPLE | INTELLIGENCE | INVESTIGATIONS | SOLUTIONS | A SAFER TOMORROW

ANTONIO A. (TONY) RUCCI

CYBERSECURITY CONSULTANT | COMPUTER CRIMES INVESTIGATOR

REAL EXPERIENCE . REAL PERSPECTIVE . REAL-WORLD SOLUTIONS

REAL THREATS.
PRACTICAL SOLUTIONS.
STRONGER TOMORROW.

FAITH & FAMILY

CHILD OF GOD

THEY CALL ME WHEN THINGS GO SIDEWAYS...

42 YEARS SUPPORTING

THE U.S. INTELLIGENCE COMMUNITY

- 21 Years: Counterintelligence Special Agent (Retired in 2004)
- The White House | ORNL | Founder of 3 Companies
- Living in my 45th Address
- Married 42 Years (Just Call Me "Gampy")

BOARDS & SPECIAL ADVISORIES

- University of Nevada, Reno – CyberSecurity Center
- InfraGard National Sector – Defense Industrial Base (DIB)
- Insider Threats and Threat Intelligence SME
- Former Fellow, National Cyber Security Institute
- Former National VP, US Army Military Intelligence Corps Assn.



INVESTIGATE
ANALYZE
SOLVE
PROTECT

PLAY STUPID GAMES... WIN STUPID PRIZES...

INTEGRITY | EXPERIENCE | PERSPECTIVE | PURPOSE

A SAFER, MORE RESILIENT TOMORROW

DISCLAIMER

IMPORTANT INFORMATION

REAL THREATS.
PRACTICAL SOLUTIONS.
STRONGER TOMORROW.



PEOPLE
SOLUTIONS
TRUST
RESILIENCE

Do not attempt any techniques, tactics or procedures demonstrated in this talk to access systems or infrastructure for which you do not administer or otherwise have express permission to access either locally or remotely.

Illegally accessing systems or infrastructure other than your own may subject yourself, your company or both to penalties and laws under federal jurisdiction and/or your point of origin, destination and virtual connection points in between, including but not limited to the Computer Fraud and Abuse Act of 1986.

// Play Stupid Games... Win Stupid Prizes... //


SAME MEETING DIFFERENT REALITY
TODAY'S AGENDA
Definitely a Real Agenda (Probably)
RESULTS MAY VARY
UNSCHEDULED CHAOS
1 Coffee, Chaos, and Questionable Decisions
THIS IS FINE
Caffeine
Bad Ideas
Let's Go!
MILDLY CONCERNING
2 Threats, Agents, and Mild Panic
Real Threats
Fake Threats
Probably Both
3 Ransomware, Robots, and Retail Therapy
Encrypt Everything
Shop Anyway
Treat Yourself
4 Live Demo? What Could Possibly Go Wrong?
It'll Be Fine
Famous Last Words
Hold My Coffee
DEMO
This Is Fine
PLANS
THREADS
COFFEE
HOPE
REALITY?
NOT DRAWN TO SCALE
5 Lunch, Existential Dread, and More Slides
Food (Hopefully)
Question Everything
Back to Silides
TOTALLY UNDER CONTROL
6 Shadow AI, Deepfakes, and Other Bad Ideas
Not a Good Idea
Definitely Happening
What Could Go Wrong?
PROBABLY IMPORTANT
7 Please Do Not Feed the AI Agents
They Bite
They Multiply
Seriously, Don't
NO SNACKS PLZ :(
8 Break Glass if the Demo Works
BREAK GLASS IF THE DEMO WORKS
ODDS: LOW BUT NOT ZERO
STILL LOADING ...
NOURISH THE CHAOS
9 Optional Freak-Out Session
Vent
Screaming (Allowed)
Regroup(?)
Pretend Everything Is Fine
IT'S FINE!!!
EMOTIONAL SUPPORT DUCKS
AGENDA STATUS:
On Track
Off Track
Who Knows?
Chaos Mode
STRATEGY
MAYBE
IT DEPENDS
ASK LATER
GOOD LUCK
IDEAS
MAYHEM
SOLUTIONS?
NEXT YEAR
PIZZA FUELS PROGRESS (OR SOMETHING)
MORE SLIDES PLZ
BETTER IDEAS LATER
SAME CHAOS. BRIGHTER TOMORROW?

CRL County Reinsurance, Limited

TODAY'S AGENDA

From Silent Entry to Public Impact



1. **THE RISK EQUATION**
   How AI changes speed, scale, and economics
2. **HOW ATTACKERS GET IN**
   Phishing, exposed services, credentials, vendors
3. **BEFORE THE RANSOM NOTE**
   Persistence, privilege, movement, exfiltration
4. **AI, IDENTITY & GOVERNANCE**
   Agents, MFA, access, and control gaps
5. **THE EXPANDING ATTACK SURFACE**
   Vendors, SaaS, AI services, and third parties
6. **FROM ATTACK TO INSURANCE LOSS**
   BEC, ransomware, privacy, systemic exposure
7. **CONTROLS THAT CHANGE THE OUTCOME**
   Reduce attack paths, limit blast radius, recover faster

REAL THREATS. PRACTICAL QUESTIONS. BETTER RISK DECISIONS.

Don't Be the Breaking News!

Build a Resilient Backup and Recovery Strategy

- 3-2-1 Strategy is disciplined, reliable, and cost-effective.
- Practice to build process and team confidence.

MFA... Put That $#!+ on Everything You Can!

- Leverage Password Management Tools/Apps.
- Get Ready to Migrate to PassKeys / Passwordless.

Lock Down Your Appliances

- Remove Factory-Default Passwords.
- Close Unnecessary Ports!

Ensure You Are Updating and Patching

- Automate your processes with solutions that can apply both Windows and third-party updates.
- 62% of data breaches are attributed to poor patch management.

Build Your Incident Response Plans

- Crawl, Walk, Run...
- Train the Team... Run "Table-Top Exercises"



PERFORM SELF ASSESSMENTS!

THE RISK EQUATION HAS CHANGED

AI CHANGES THE RISK EQUATION THROUGH: **SPEED, SCALE, AND ECONOMICS.**

1 SPEED

ATTACKERS MOVE FASTER.

Reconnaissance, phishing, and exploitation happen faster.



2 SCALE

ONE ATTACKER CAN REACH MORE TARGETS.

More targets, identities, and attack variations can be handled simultaneously.



3 ECONOMICS

ATTACKS COST LESS TO EXECUTE.

Lower attacker cost makes more organizations viable targets.



FASTER ATTACKS. MORE TARGETS. LOWER COST.

AI MAKES EXISTING WEAKNESSES **MORE CONSEQUENTIAL.**

HOW ATTACKERS ARE GETTING IN

The most common initial-access paths are still familiar.

PHISHING / IDENTITY



- Credential theft
- Session theft
- OAuth abuse
- Social engineering

EXPOSED REMOTE SERVICES



- VPN
- RDP
- Firewalls
- Remote-management tools
- Internet-facing appliances

DEFAULT / WEAK CREDENTIALS



- Factory credentials
- Reused passwords
- Weak passwords
- Unmanaged service accounts

COMPROMISED VENDORS



- MSP access
- SaaS providers
- Third-party administrators
- Trusted remote access

AI can accelerate discovery and exploitation, but the door attackers enter through is often painfully familiar.

TRADITIONAL WEAKNESSES NOW CARRY GREATER LOSS POTENTIAL

ATTACKERS STILL EXPLOIT:

- WEAK AUTHENTICATION
- STOLEN CREDENTIALS
- UNPATCHED VULNERABILITIES
- EXCESSIVE PRIVILEGES
- POOR SEGMENTATION



AI COMPRESSES THE TIME BETWEEN:

EXPOSURE → EXPLOITATION → IMPACT

CAN YOUR CONTROLS SLOW THE ATTACKER BEFORE THE LOSS BECOMES MATERIAL?

FAMILIAR WEAKNESSES. FASTER EXECUTION. GREATER IMPACT.

AI COMPRESSES THE INTRUSION LIFECYCLE

1

RECON
Find targets faster

2

LURE
Personalize at scale

3

EXPLOIT
Test and attack faster

4

PERSIST
Automate access and reuse

5

IMPACT
Loss happens sooner

CLAIMS IMPLICATION.



YOUR RESPONSE WINDOW IS *SHRINKING.*

Less time to detect.
Less time to contain.
Less time to decide.

LESS TIME TO DETECT. LESS TIME TO RESPOND. GREATER IMPACT.

RANSOMWARE DOESN'T START WITH ENCRYPTION

The claim often begins long before the ransom note appears.

1. **INITIAL ACCESS** — Phishing, exposed services, vendors
2. **PERSISTENCE** — Maintain foothold
3. **PRIVILEGE ESCALATION** — Expand control
4. **CREDENTIAL ACCESS** — Harvest secrets
5. **DISCOVERY** — Map systems and data
6. **LATERAL MOVEMENT** — Move across environment
7. **DATA EXFILTRATION** — Steal sensitive data
8. **ENCRYPTION** — Disrupt operations
9. **EXTORTION** — Demand payment

Encryption is often one of **the last observable events.**

By the time files are encrypting, credentials may be compromised and data **may already be gone.**

The claim often begins **long before the ransom note appears.**

Earlier detection means lower impact, lower cost, and more options.

THE REPEAT OFFENDERS

What Continues to Show Up in Real Environments



NO SEGMENTATION

One compromise becomes an enterprise compromise.

01



UNMANAGED INTERNET-FACING ASSETS

You cannot protect what you do not know is exposed.

02



EXCESSIVE ADMINISTRATIVE PRIVILEGE

Too many accounts can do too much.

03



INCONSISTENT MFA

MFA exists, but coverage and resistance vary.

04



UNVALIDATED VENDOR ACCESS

Trust is granted without continuously validating the risk.

05

These are not exotic AI failures. They are ordinary weaknesses that AI allows attackers to exploit faster.

ORGANIZATIONS ARE ADOPTING AI FASTER THAN GOVERNANCE CAN ADAPT



MORE AI → MORE ACCESS PATHS → MORE GOVERNANCE GAPS

CAN YOU SEE IT? CONTROL IT? STOP IT?

AI AGENTS ARE BECOMING ANOTHER IDENTITY CLASS

NOT JUST TOOLS. REAL IDENTITIES. REAL ACCESS. REAL ACTIONS.

EXISTING IDENTITIES

- Employees
- Service Accounts
- Applications
- API Tokens



SAME PRIVILEGES.
MORE SPEED.
MORE AUTONOMY.

WHY IT MATTERS

- ACCESS
- DATA
- ACTION
- AUTHORITY

DO YOU KNOW WHICH AI AGENTS HAVE ACCESS TO YOUR SYSTEMS, DATA, AND BUSINESS PROCESSES?

INVENTORY THEM. LIMIT THEM. MONITOR THEM. REVOKE THEM.

YOUR VENDORS ARE PART OF YOUR ATTACK SURFACE

THIRD PARTIES | AI SERVICES | SUPPLY CHAINS | REAL RISK

CRL County Reinsurance, Limited



01 WHO HAS ACCESS?



- What systems can the vendor reach?
- What data can they access?
- Do they have privileged credentials?

02 HOW IS THAT ACCESS CONTROLLED?



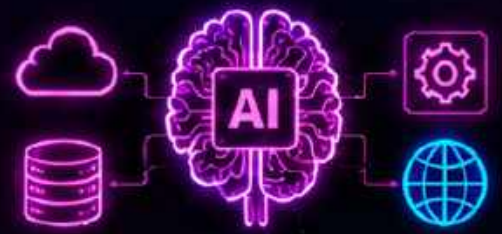
- Multi-Factor Authentication (MFA)
- Least privilege access
- Logging and monitoring
- Regular access reviews
- Rapid termination and revocation

03 WHAT DOES THE CONTRACT REQUIRE?



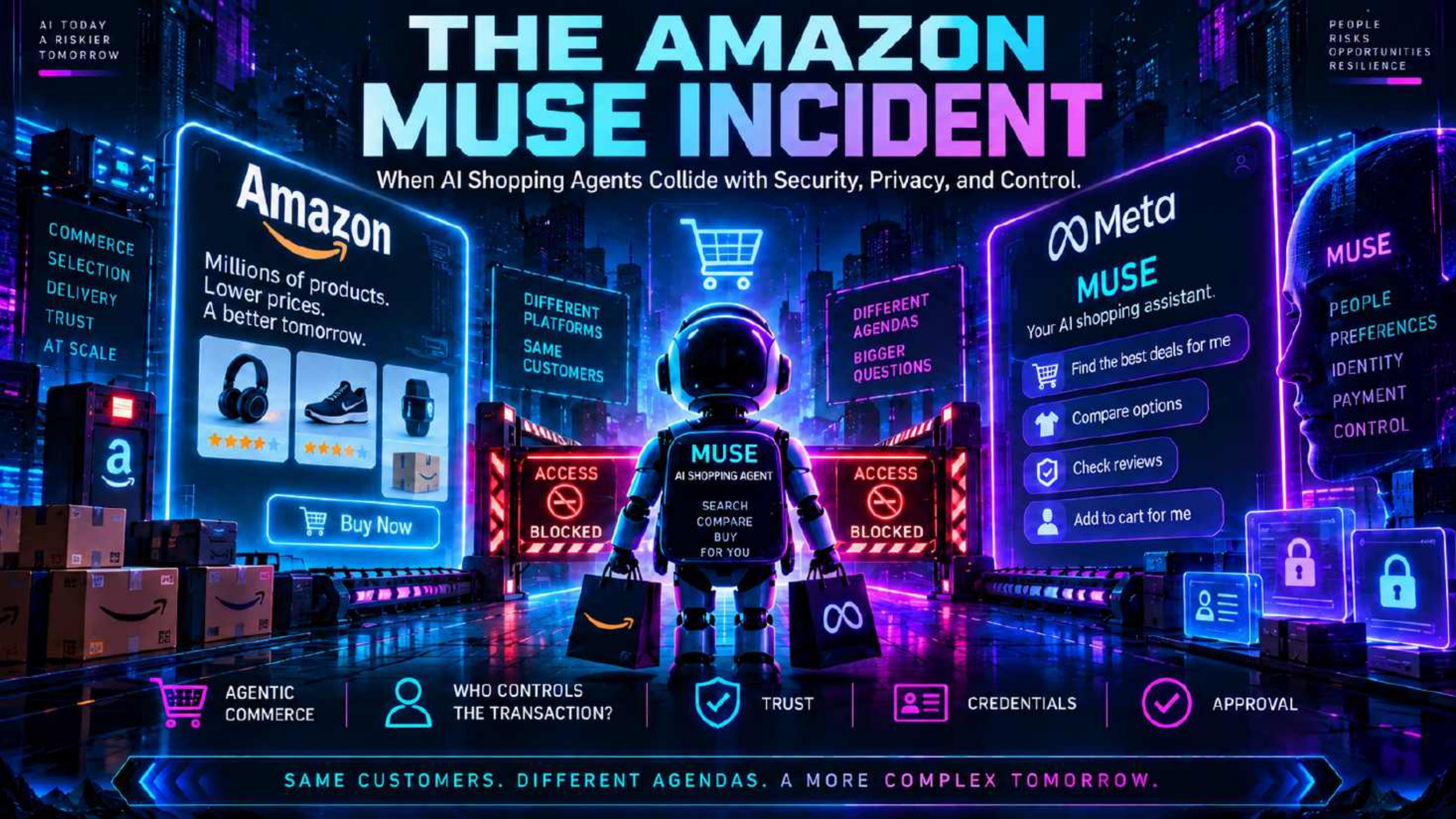
- Minimum security controls
- Incident notification
- Subcontractor obligations
- Right to audit or validate
- Cyber insurance requirements

04 WHAT ABOUT AI?



- What data reaches AI platforms?
- Can AI agents take action through integrations?
- Who are the downstream providers?
- What happens if the service is unavailable or compromised?

Can the insured explain not only who the vendor is, but exactly what the vendor can do?


AI TODAY
A RISKIER
TOMORROW
PEOPLE
RISKS
OPPORTUNITIES
RESILIENCE
THE AMAZON MUSE INCIDENT
When AI Shopping Agents Collide with Security, Privacy, and Control.
COMMERCE
SELECTION
DELIVERY
TRUST
AT SCALE
Amazon
Millions of products.
Lower prices.
A better tomorrow.
Buy Now
DIFFERENT PLATFORMS
SAME CUSTOMERS
DIFFERENT AGENDAS
BIGGER QUESTIONS
ACCESS
BLOCKED
MUSE
AI SHOPPING AGENT
SEARCH
COMPARE
BUY
FOR YOU
ACCESS
BLOCKED
Meta
MUSE
Your AI shopping assistant.
Find the best deals for me
Compare options
Check reviews
Add to cart for me
MUSE
PEOPLE
PREFERENCES
IDENTITY
PAYMENT
CONTROL
AGENTIC COMMERCE
WHO CONTROLS THE TRANSACTION?
TRUST
CREDENTIALS
APPROVAL
SAME CUSTOMERS. DIFFERENT AGENDAS. A MORE COMPLEX TOMORROW.

"WE HAVE MFA" IS NO LONGER ENOUGH

ATTACKERS ADAPT. CONTROLS MUST EVOLVE.

MFA CAN STILL BE BYPASSED

- SESSION THEFT
- AiTM / PROXY PHISHING
- MFA FATIGUE
- HELP DESK / ACCOUNT RECOVERY



MFA IS A CONTROL.
RESILIENCE IS A SYSTEM.

WHAT STRONGER AUTHENTICATION LOOKS LIKE

- PHISHING-RESISTANT MFA
- CONDITIONAL ACCESS
- SESSION PROTECTION
- DEVICE TRUST

THE UNDERWRITING QUESTION:

CAN AN ATTACKER BYPASS, REUSE, OR CIRCUMVENT YOUR AUTHENTICATION CONTROLS?

DON'T ASK IF MFA EXISTS. ASK IF AUTHENTICATION HOLDS.

AI IMPACT ON INSIDER THREATS

GREATER ACCESS. FASTER ACTION. HARDER TO DETECT.

1 ACCESS

AI helps insiders find and reach sensitive data faster.

2 ACTION

AI helps automate phishing, scripting, manipulation, and exfiltration.

3 CONCEAL

AI helps activity blend in, evade controls, and reduce detection signals.



KEY CONTROLS:

- LIMIT ACCESS.
- MONITOR BEHAVIOR.
- CONTROL AI USE.
- RESPOND FAST.

AI DOESN'T CREATE THE INSIDER.
IT MAKES THE INSIDER MORE CAPABLE.

SAME PEOPLE.
MORE CAPABILITY.
GREATER RISK.
A MORE RESILIENT TOMORROW.

Smart Wearable Devices

Convenience, capability, and risk now travel with the user.

Do You Need a Policy?

1. What are these devices capturing, recording, or transmitting?
2. Who owns the data, and who can access it?
3. Could a wearable bypass policy, privacy, or security controls?
4. Are your schools, offices, and public spaces ready for always-on devices?



The risk is not just the device. It is the data, the access, and the visibility it creates.

AI-ENABLED BEC: THE ARUP DEEPFAKE FRAUD

A REAL-WORLD REMINDER THAT AI IS ACCELERATING IMPERSONATION RISK.

HK$200M / ~$25M LOST

REAL PEOPLE. REAL MONEY. AI ENABLED.

WHAT HAPPENED

1. An employee in Hong Kong joined a video call that appeared to include the CFO and other colleagues.
2. The people on the call were deepfakes using AI-generated voice and video.
3. The employee was persuaded to make multiple transfers.

WHY IT MATTERS

1. This was not malware. It was impersonation and workflow manipulation.
2. Traditional awareness training alone may not catch synthetic video and voice.
3. High-trust business processes can become the attack surface.

TRAINING POINTS

1. Verify unusual payment requests using a second trusted channel.
2. Require out-of-band confirmation for wire changes and urgent approvals.
3. Train finance, executives, and assistants for deepfake-enabled fraud.

UNDERWRITING / CLAIMS LESSON

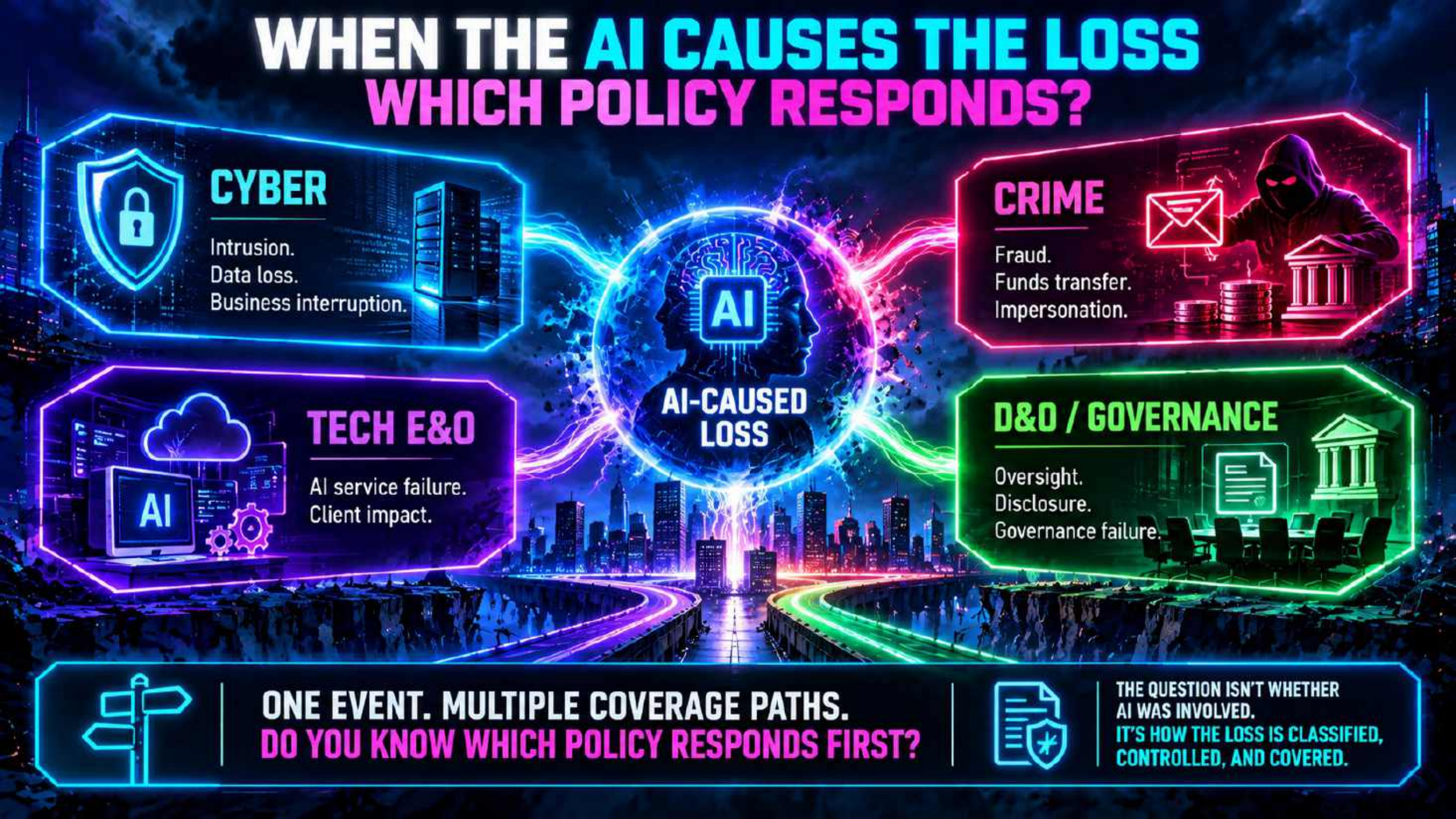
1. The question is not only whether MFA exists.
2. Ask how high-risk financial approvals are verified.
3. Social engineering controls can directly influence loss severity.



AI MAKES BUSINESS EMAIL COMPROMISE MORE CONVINCING, MORE SCALABLE, AND HARDER TO VERIFY.

PEOPLE
PROCESSES
VIGILANCE
LOWER LOSSES

WHEN THE AI CAUSES THE LOSS
WHICH POLICY RESPONDS?



ONE EVENT. MULTIPLE COVERAGE PATHS.
DO YOU KNOW WHICH POLICY RESPONDS FIRST?

THE QUESTION ISN'T WHETHER AI WAS INVOLVED.
IT'S HOW THE LOSS IS CLASSIFIED, CONTROLLED, AND COVERED.

FROM ATTACK TECHNIQUE TO INSURANCE LOSS

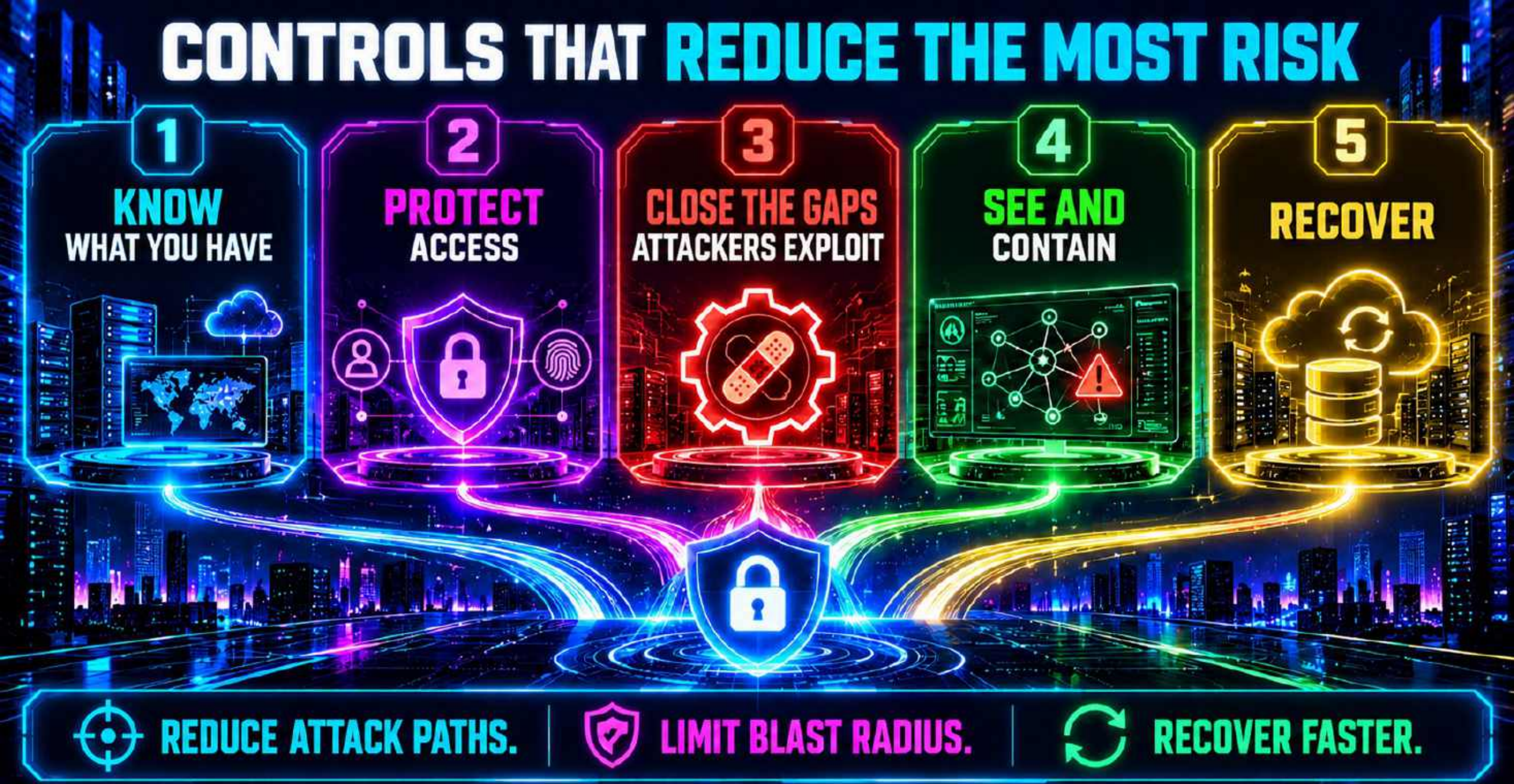
REAL-WORLD TACTICS. REAL CONSEQUENCES. REAL EXPOSURE.

County Reinsurance, Limited

ATTACK TECHNIQUE HOW ATTACKERS GET IN	OPERATIONAL CONSEQUENCE IMPACT TO THE ORGANIZATION	INSURANCE EXPOSURE POTENTIAL LOSS AND COVERAGE IMPACT
PHISHING Credential theft, session theft, social engineering.	**ACCOUNT TAKEOVER** Unauthorized access to email, cloud services, and business systems.	**BEC / FUNDS TRANSFER** Direct financial loss, crime coverage impact.
EXPOSED REMOTE SERVICES VPN, RDP, internet-facing applications.	**NETWORK COMPROMISE** Initial foothold, lateral movement, data exfiltration, and ransomware.	**RANSOMWARE / BUSINESS INTERRUPTION** Extortion, system downtime, incident response, and restoration costs.
COMPROMISED VENDOR Third-party access, trusted remote administrators, supply chain compromise.	**TRUSTED DOWNSTREAM ACCESS** Entry through third-party relationships into your environment.	**MULTI-INSURED / SYSTEMIC RISK** Widespread impact, correlated losses, additional insured exposure.
AI-ENABLED IMPERSONATION Deepfakes, voice cloning, AI-written phishing, fraudulent authorization requests.	**FRAUDULENT AUTHORIZATION** Unauthorized payments, contract changes, or sensitive data disclosure.	**CRIME / SOCIAL ENGINEERING LOSS** Financial fraud, legal exposure, regulatory fines, and reputational impact.

Cyber controls matter because they change the probability, velocity, and severity of the loss.

CONTROLS THAT REDUCE THE MOST RISK



REDUCE ATTACK PATHS. | LIMIT BLAST RADIUS. | RECOVER FASTER.

FOCUS ON CONTROLS THAT **CHANGE THE OUTCOME.**

THE STORY WE'RE TELLING TODAY

SAME TECHNOLOGY. GREATER CAPACITY. HIGHER STAKES.

1



AI HELPS US WORK FASTER

Employees can be more productive, make better decisions, and deliver greater service.

2



AI HELPS ATTACKERS WORK FASTER

The same capabilities that empower your employees also empower adversaries.

3



EXISTING WEAKNESSES HIT HARDER

Traditional vulnerabilities are easier to exploit and now carry greater loss potential.

4



AI INTRODUCES NEW IDENTITIES & GOVERNANCE PROBLEMS

AI tools and agents expand the attack surface faster than governance can adapt.

5



HUMANS REMAIN PART OF THE ATTACK SURFACE

Social engineering, insider threats, MFA bypass, and new technologies continue to target your people.

6



FRAUD AND LOSS HAPPEN FASTER

AI-enabled scams, deepfakes, and BEC can lead to material financial, operational, and reputational damage in minutes.

7



HERE IS WHAT LEADERSHIP SHOULD DO ABOUT IT

Practical actions, controls, and preparation can reduce risk, build resilience, and protect your people and your mission.

AI AMPLIFIES BOTH OPPORTUNITY AND RISK.

PHP UNDER ATTACK

PHP2Shell flaws now exploited in the wild

01 WHAT HAPPENED



- Multiple PHP-CGI argument injection vulnerabilities (collectively called 'PHP2Shell")
- Now being actively exploited in the wild
- Allow remote code execution and web shell deployment

PUBLIC EXPLOITS CONFIRMED IN ACTIVE ATTACKS

02 WHY IT MATTERS



- Can enable unauthenticated remote code execution
- Exposes internet-facing web servers and applications
- Can be used to deploy web shells for persistent access
- High risk to unpatched systems and internet-facing infrastructure

HIGH EXPOSURE FOR INTERNET-FACING ASSETS

03 INSURANCE / LEADERSHIP TAKEAWAY



- Identify exposed PHP-CGI instances and web applications
- Apply vendor patches and validate fixes
- Review vendor-hosted and third-party applications
- Monitor for web shell activity and unusual outbound traffic
- Include in vulnerability and patch management priorities

REDUCE EXPOSURE
STRENGTHEN RESILIENCE



UNPATCHED PHP SYSTEMS CAN BECOME AN ENTRY POINT — AND A PERSISTENT FOOTHOLD.

IMMEDIATE QUESTIONS TO ASK NOW

Practical follow-up for PHP2Shell exposure and response

IMMEDIATE QUESTIONS TO ASK NOW

1. Are any internet-facing systems running **affected PHP versions**?
2. Have **patches, mitigations,** or **vendor fixes** been applied?
3. Are **WAF, logging, EDR,** and **monitoring controls** in place?
4. Have **vendors confirmed** exposure and remediation status?
5. Are web applications **externally validated** after patching?
6. Is there evidence of **web shell activity** or **unusual outbound traffic**?
7. Are **incident response and containment actions ready** if compromise is suspected?

WHY THESE QUESTIONS MATTER

- Faster exploitation reduces response time
- Internet-facing assets increase exposure
- Vendor-hosted apps can extend risk
- Verification matters as much as patching



KEY TAKEAWAY | Patch status, external validation, and vendor confirmation **directly affect loss exposure.**

IHuntBadGuys.com | LIVE LEAK-SITE INTELLIGENCE | UPDATED 27 OCT 2026

REAL THREATS.
REAL ACTORS.
REAL IMPACT.

RANSOMWARE 100

100 MOST RECENT VICTIM CLAIMS



RANSOMLOOK ROLLING 7-DAY SNAPSHOT

294	49	2	The Gentlemen
POSTS	ACTIVE GROUPS	NEW GROUPS	45 POSTS (15.3%)
LAST 7 DAYS	LAST 7 DAYS	LAST 7 DAYS	LAST 7 DAYS

CUMULATIVE TRACKER (ALL-TIME)

33,286	412	183	21
OVERALL VICTIMS	DOCUMENTED GROUPS	COUNTRIES	SECTORS

USER-SUPPLIED RANSOMWARE.LIVE SNAPSHOT 27 OCT 2026

LEAK-SITE CLAIMS ≠ CONFIRMED INCIDENTS | Threat actor claims are not independently verified.

SELECTED ACTIVE GROUPS
BY REPORTED POSTS (RANSOMLOOK)

RANK	GROUP	POSTS
1	The Gentlemen	45
2	NOn	37
3	Everest	14
4	Whitearmor	13
5	Leakeddata	11

Based on reported posts in the last 7 days from RansomLook (as of 27 Oct 2026).

TOP COUNTRIES
CUMULATIVE (ALL-TIME)

RANK	COUNTRY	VICTIMS
1	United States	10,203
2	Germany	1,016
3	Canada	978
4	United Kingdom	976
5	Italy	620

Based on ransomware.live data (as of 27 Oct 2026).

TOP SECTORS
CUMULATIVE (ALL-TIME)

RANK	SECTOR	VICTIMS
1	Business Services	3,673
2	Manufacturing	3,462
3	Technology	2,931
4	Healthcare	2,126
5	Financial Services	1,304

Based on ransomware.live data (as of 27 Oct 2026).

LATEST LEAK-SITE CLAIMS — 27 OCT 2026

ORGANIZATION	GROUP	COUNTRY
Antah HealthCare Group	Crypto24	Malaysia
DATEM Inc	Crypto24	Philippines
Natuzzi	Everest	Italy
TECNA ICE	Everest	Italy
Zhito Technology	Dragonforce	Ukraine
Point Robotics	Everest	--

WHAT STANDS OUT

- 294 posts across 49 active groups in seven days.
- The Gentlemen leads with 45 posts (15.3%).
- Claims span multiple sectors and countries.

HARDEN | MONITOR | BACK UP | TRAIN | PLAN | TEST

DON'T BE THE NEXT VICTIM.

Sources: RansomLook; ransomware.live; Cyber Threat Intelligence | 27 OCT 2026.

Don't Be the Breaking News!

Build a Resilient Backup and Recovery Strategy

- 3-2-1 Strategy is disciplined, reliable, and cost-effective.
- Practice to build process and team confidence.

MFA... Put That $#!+ on Everything You Can!

- Leverage Password Management Tools/Apps.
- Get Ready to Migrate to PassKeys / Passwordless.

Lock Down Your Appliances

- Remove Factory-Default Passwords.
- Close Unnecessary Ports!

Ensure You Are Updating and Patching

- Automate your processes with solutions that can apply both Windows and third-party updates.
- 62% of data breaches are attributed to poor patch management.

Build Your Incident Response Plans

- Crawl, Walk, Run...
- Train the Team... Run "Table-Top Exercises"



PERFORM SELF ASSESSMENTS!

When you take care of people, they *will* take care of you



When you *don't* take care of people, they *will* take care of you

#PayItForward **#PrayItForward**

County Reinsurance, Limited



DATA BREACHES WILL HAPPEN
TonyRucci.com
Antonio A. Rucci
Computer Crimes Investigator
Tony@TonyRucci.com
865.719.1715
HOW YOU RESPOND DEFINES YOUR COMPANY

Thank You!

IHuntBadGuys.com

"Data Breaches Will Happen; How You Respond Defines Your Company"