Covered or Exposed?

What Your Business Doesn't Know About Cyber Risk

Co-presented by **Katie Hensley, AIC** — Cottingham & Butler
Steve Long, CEO/Co-Founder — UnRavl

Cottingham & Butler + UnRavl

Before We Begin

All attendees are in “LISTEN ONLY” mode.

You can type in questions by clicking on the question box on the top right of your GoToWebinar panel.

Q&A at the end of the webinar.

A recorded copy of the webinar and slides will be made available to all attendees.

Cottingham & Butler + UnRavl

Today's Agenda

45 minutes to change how you think about cyber risk

1	**Application Accuracy** Why inaccurate answers on your application = denied claims *~10 min*
2	**Lurking Threats** Hackers in your system — silently watching *~8 min*
3	**Ransomware Response** Who to call, what NOT to do *~10 min*
4	**Compliance ≠ Protection** Why passing audits isn't enough *~7 min*
5	**The Cloud Myth** Shared responsibility exposed *~7 min*
6	**AI & Emerging Risks** Deepfakes, AI phishing & policy gaps *~7 min*

Cottingham & Butler + UnRavl

Your Presenters

Katie Hensley, AIC

Cottingham & Butler

Cyber insurance specialist helping businesses identify coverage gaps before a loss forces the issue. Katie brings deep expertise in policy language, underwriting requirements, and claims advocacy.

Steve Long

CEO/Co-Founder · UnRavl

20+ years in cybersecurity. Former Electronic Warfare & Naval Strike Systems operator. Now delivers battle-tested resilience strategies to private sector clients facing real-world adversaries.

Application Accuracy

Why inaccurate answers on your cyber insurance application can result in denied claims when you need coverage most

Cottingham & Butler + UnRavl

The Stakes: A Denied Claim

Application errors are the #1 reason cyber claims get denied

40%

Denied Claims

of denied cyber claims cite application inaccuracies as the primary cause

If you say you have a control in place and a breach reveals you don't — the insurer can **void your claim entirely**, regardless of the loss amount.

Common Application Errors

- Overstating security controls that aren't fully deployed
- Misrepresenting the scope of multi-factor authentication (MFA)
- Failing to disclose prior incidents or known vulnerabilities
- Inaccurate employee count affecting premium and coverage limits
- Underreporting sensitive data types (PII, PHI, payment data)

Cottingham & Butler + UnRavl

What You Must Get Right

Your application is a legal document. Every answer carries underwriting weight — and potential claim consequences. These four areas receive the highest scrutiny from insurers.

MFA Coverage

Document exactly where MFA is deployed. "We use MFA" isn't enough — specify email, VPN, remote desktop, and privileged accounts. Partial deployment is a red flag for underwriters.

Backup Verification

Confirm backups are tested, off-site, and air-gapped. Insurers increasingly require immutable backup proof — not just a policy that backups exist.

Incident History

Disclose all prior incidents, even "minor" ones. A previous breach you didn't report can void future claims — even if the events appear unrelated.

Vendor Risk

Third-party access to your systems must be disclosed. Supply chain attacks are now a primary underwriting concern and a leading cause of enterprise breaches.

Cottingham & Butler + UnRavl

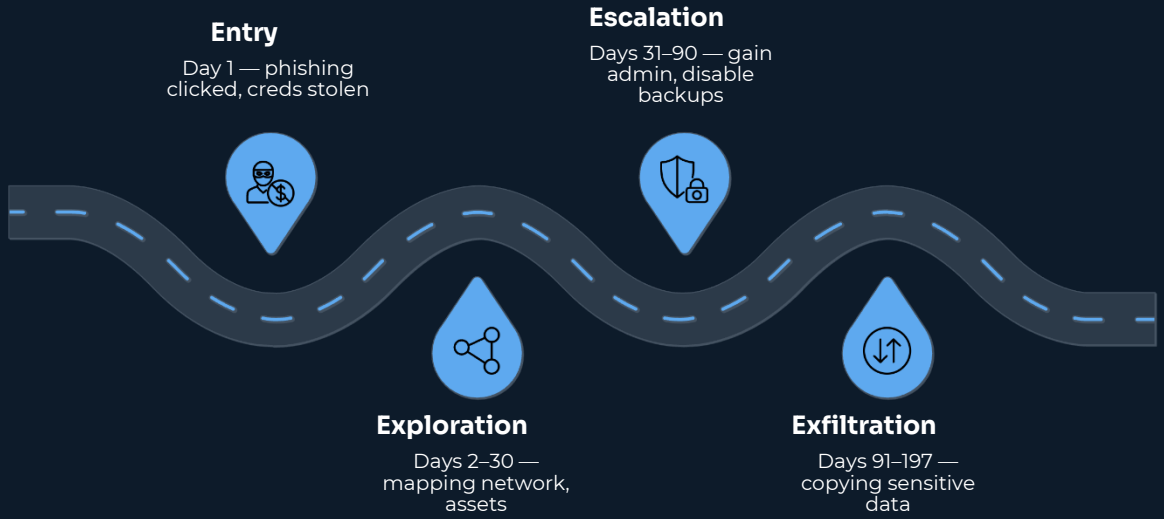
Lurking Threats

How threat actors sit silently inside your network for weeks, months — or even years — before striking

Cottingham & Butler + UnRavl

The Silent Attacker: Dwell Time

⚠ **Average time between breach and detection: 197 days.** By the time you know, the damage is already done.



How They Get In

Phishing emails, unpatched software, stolen credentials from third parties, and remote desktop exploits are the top entry vectors — often targeting the most overlooked gaps in your environment.

What UnRavl Looks For

Behavioral analytics and threat hunting detect anomalous lateral movement — not just known malware signatures. Most attacks are invisible to traditional tools.

Why It Matters for Your Coverage

Insurance alone won't help if the damage is already done. Early detection fundamentally changes the outcome — and can mean the difference between a manageable claim and a catastrophic loss.

Cottingham & Butler + UnRavl

Ransomware Response

Who to call, what NOT to do, and how the right coverage changes the outcome

The First 24 Hours: Your Response Framework

Every minute counts. The decisions made in the first hour of a ransomware event will determine your recovery timeline, your legal exposure, and whether your insurance claim is honored.

1

Don't Pay — Yet

Contact your insurer **first**. Paying ransom without prior authorization **voids coverage** in most policies. Insurers have negotiators — use them.

2

Call Your Insurer

Use your 24/7 breach hotline immediately. They engage your forensics team, legal counsel, and professional ransom negotiators within hours.

3

Isolate Systems

Disconnect affected machines from the network. **Do NOT shut down** — powering off destroys forensic evidence critical for investigation and claims.

4

Preserve Evidence

Don't wipe logs. Document everything. Screenshot ransom notes. Thorough documentation directly protects your insurance claim and any legal proceedings.

5

Notify Stakeholders

Alert legal, HR, and leadership immediately. HIPAA and PCI-DSS impose **72-hour notification windows** — missing them creates regulatory liability on top of the breach.

6

Activate Recovery Plan

Your IR plan should be **printed and practiced** before this moment arrives. Cloud backups must be verified as clean and restorable before you rely on them.

Cottingham & Butler + UnRavl

Compliance ≠ Protection

Why passing your audit doesn't mean your business is actually secure

Cottingham & Butler + UnRavl

The Compliance-Security Gap

Compliance frameworks like SOC 2, HIPAA, and PCI-DSS were designed for **accountability** — not adversarial resilience. You can be fully compliant and still be breached. Understanding the gap is critical.

Compliance Gives You:

Real Security Requires:

⚠ Compliance is the floor, not the ceiling. Hackers don't wait for your annual audit cycle — they probe your defenses every single day.

Cottingham & Butler + UnRavl

The Cloud Myth

"My data is in the cloud — I'm protected." Why this assumption is your biggest blind spot.

Cottingham & Butler + UnRavl

The Shared Responsibility Model

What AWS, Azure, and Google Cloud are NOT responsible for

☁️ Cloud Provider Covers

- Physical infrastructure & data centers
- Host OS and hypervisor patching
- Network controls at the infrastructure level
- Service availability (uptime SLAs)

🏢 Your Business Covers

- Data classification and encryption
- Identity & access management (IAM)
- Application-level security configuration
- Endpoint and device protection
- Monitoring, logging, and incident response
- Compliance and regulatory obligations

⊗ Manufacturers in defense, automotive, and healthcare: moving to the cloud does **not** automatically satisfy CMMC, ITAR, or HIPAA obligations. You still own the data protection layer — entirely.

Cottingham & Butler + UnRavl

AI & Emerging Risks

How AI is reshaping the cyber threat landscape — and what that means for your coverage and controls

Cottingham & Butler + UnRavl

AI Is Changing the Threat Landscape

For attackers AND defenders — and your insurance policy may not have caught up

⚠ AI-Powered Threats

Deepfake Social Engineering

Voice and video cloning used to impersonate executives, authorize wire transfers, or bypass MFA voice verification checks.

AI-Generated Phishing

Hyper-personalized spear-phishing at scale — no spelling errors, perfect tone, trained on your LinkedIn profile and email patterns.

Automated Vulnerability Scanning

AI tools that scan for and exploit unpatched systems faster than any security team can realistically patch them.

Polymorphic Malware

Malware that rewrites its own code to evade signature-based detection — adapting and mutating in real time.

✓ What You Need to Address

AI Use Policy

Employees using AI tools (ChatGPT, Copilot, etc.) may inadvertently expose sensitive data. A formal policy is now an underwriting requirement.

Verify Before You Act

Any wire transfer, credential change, or urgent request — even from a known voice — must be verified through a second, independent channel.

Review Your Policy

Most policies written before 2024 don't explicitly cover AI-enabled fraud. Ask specifically about social engineering and deepfake coverage endorsements.

Train Your Team

AI phishing defeats traditional awareness training. Simulate AI-generated attacks and update your program at least quarterly to stay effective.

Cottingham & Butler + UnRavl

Key Takeaways

1 Application Accuracy Is Your First Line of Defense

Get your application wrong and your claim can be denied entirely — regardless of how large your loss is. Accuracy isn't optional; it's the foundation of your coverage.

2 Attackers Are Patient — Proactive Detection Is Not Optional

The breach you think didn't happen may already be in progress. With an average dwell time of 197 days, waiting for alerts is not a strategy.

3 A Response Plan on Paper Is No Plan at All

Know who to call, what not to do, and what your policy requires — before ransomware hits. Practice your plan or you won't execute it under pressure.

4 Compliance Satisfies Auditors — Security Protects Your Business

Passing your SOC 2 or HIPAA audit is the minimum bar. Real protection requires continuous monitoring, testing, and controls that go beyond the checklist.

5 The Cloud Shifts Responsibility — It Doesn't Eliminate It

You own your data's security at the application and identity layer. No cloud provider agreement changes your regulatory obligations or your exposure.

Cottingham & Butler + UnRavl

Questions & Next Steps

Ready to find out if you're covered or exposed? Take one of these three steps with our team today.

Review Your Application

Request a policy review with Katie to audit your current cyber insurance application for accuracy gaps — before your insurer finds them during a claim.

Get a Threat Assessment

UnRavl offers a no-obligation threat hunt to detect hidden adversaries already in your environment. Most clients are surprised by what we find.

Benchmark Your Controls

Compare your current security posture against what insurers actually require for your industry — and close the gaps before renewal season.

Katie Hensley — Cottingham & Butler

kahensley@cottinghambutler.com
563.581.2244

Steve Long — UnRavl

info@unravltech.ai
(866) 384-6538 ext 5

Cottingham & Butler + UnRavl

Thank You

Covered or Exposed? You decide.

Presented by **Cottingham & Butler** | **UnRavl** · June 2, 2026

www.cottinghambutler.com | www.unravltech.ai