AMBRIDGE GROUP
ZEROGAP PRE-BREACH SERVICES

Elevating Cyber Insurance Through Proactive Measures

Learn more at
www.ambridge-group.com

Inquire at:
zerogap@ambridge-group.com

Pre-Breach Services

A different approach to Cyber Insurance

ZeroGap enhances traditional cyber insurance by pairing coverage with curated pre- breach services that help organizations identify vulnerabilities, improve preparedness and reduce the likelihood and severity of cyber events.

Rather than waiting until an incident occurs, ZeroGap is designed to deliver immediate, practical value from day one.

ZeroGap Service Partners

Identity Assurance& Fraud Prevention:

SureMark DIGITAL

A real-time identity assurance platform that enables employees to verify who they are interacting with before taking sensitive action—across phone, video, or messaging.

- Prevents executive impersonation and fraudulent payment requests
- Provides cryptographic proof of identity for critical approvals
- Protects against deepfake, vendor, and social engineering attacks
- Works across all communication channels with no integrations required

Result: Reduced exposure to impersonation-driven financial loss.

Human Risk Reduction:

PONDURANCE

A fully managed security awareness program focused on reducing phishing and social engineering risk—the leading cause of cyber incidents.

- Continuous employee training and simulated phishing campaigns
- Behavioral analytics and risk scoring across users and departments
- Real-time dashboards with measurable improvement tracking
- Ongoing program management and expert support

Result: Lower susceptibility to phishing and human error-driven events.

Legal Advisory & Breach Readiness:

McDonald Hopkins®

Pre-breach legal and regulatory readiness services that help organizations prepare for and respond to cyber incidents effectively and compliantly.

- Data privacy risk assessments with legal advisory support
- Development of formal incident response plans
- Interactive breach simulations and tabletop exercises
- Guidance aligned with evolving regulatory requirements

Result: Faster, more controlled and defensible response to incidents.

Security Budget Optimization:

MOXFIVE

A structured assessment of your technology and security environment to identify gaps, redundancies, and opportunities for improvement.

- Identification of duplicated or misaligned security spend
- Insights and risk-based analysis benchmarked against real incident data
- Prioritized roadmap to strengthen resilience and efficiency

Result: Stronger security posture with more efficient use of resources.

ambridge | SureMark DIGITAL

Enroll Now

www.suremark.digital/ambridge-enroll

SureCircle™ Identity Assurance Enterprise

Real-Time Identity Verification for High-Stakes Transactions

THE PROBLEM

Executive impersonation is the fastest-growing vector in corporate fraud. AI-generated voice clones, real-time video deepfakes, and spoofed caller IDs now enable attackers to convincingly impersonate your CFO, your bank, your vendor — anyone in your chain of trust. In 2024, U.S. cybercrime losses reached $16.6 billion, with deepfake-enabled fraud surging 700% in early 2025. Detection tools cannot keep pace. The only sustainable defense is cryptographic proof of identity at the point of interaction.

THE SOLUTION

The SureCircle™ Identity Assurance platform lets your team cryptographically confirm the identity of anyone they're speaking with — on any call, any video meeting, any channel — before acting on a request. Think of it as HTTPS for human communication: just as the padlock icon tells you a website is authenticated, a SureCircle™ Identity Assurance verification tells you the person on the other end is who they claim to be.

Every member of your organization's verified network — executives, financial gatekeepers, IT leadership, key external contacts — receives a SureMark Credential backed by elliptic-curve cryptography, protected by your device's built-in secure enclave. During any live interaction, any employee can issue a 30-second identity challenge. The result is definitive: verified or not. No guesswork, no judgment calls, no reliance on voices or faces that AI can now replicate flawlessly.

WHAT SURECIRCLE™ IDENTITY ASSURANCE PROTECTS AGAINST

- **CEO & Executive Impersonation**
  Deepfake voice and video attacks targeting wire transfers and financial authorizations
- **Bank & Financial Impersonation**
  Fraudulent calls claiming suspicious activity to harvest account credentials
- **IT & Helpdesk Impersonation**
  Social engineering attacks seeking credentials, MFA codes, and remote access
- **Vendor & Supplier Fraud**
  Payment routing changes and invoice manipulation through impersonated contacts

ENROLLMENT & ONBOARDING

01 **IT Admin Setup**

Your designated IT administrator provisions your organization's SureCircle™ Identity Assurance tenant through our enterprise admin console. Circle membership, credential policies, and role tiers are configured to match your organizational structure.

02 **Executive & Gatekeeper Enrollment**

C-suite members, financial officers, IT leadership, and key external contacts each receive a SureMark Credential tied to their verified identity. Enrollment takes under five minutes per person via the SureCircle™ Identity Assurance mobile app (iOS and Android).

03 **Team Training & Go-Live**

Your team receives access to a comprehensive training manual aligned with SANS and NIST frameworks, covering real-world attack scenarios and the SureCircle™ Identity Assurance three-step verification protocol: Pause, Challenge, Confirm. Your dedicated SureMark Customer Success Manager partners with your team throughout deployment and beyond.

YOUR DEDICATED PARTNER

Every SureCircle™ Identity Assurance deployment includes a dedicated Customer Success Manager who partners with your team from initial configuration through ongoing optimization. Whether you need support with Circle architecture, employee training, or integration into existing workflows, your CSM is a direct line to the SureMark team.

Jordan Gutt · Customer Success
jordan.gutt@suremark.digital

THE CRYPTOGRAPHIC ADVANTAGE

The SureCircle™ Identity Assurance platform was built by the co-inventors of blockchain technology — the foundational cryptographic work that underpins digital trust infrastructure worldwide. Every SureMark Credential is secured by elliptic-curve public-key cryptography, protected by your device's built-in secure enclave, ensuring that verification is cryptographically definitive, not probabilistic.

AMBRIDGE GROUP × SUREMARK DIGITAL

A Joint Commitment to Proactive Cyber Defense

Ambridge Group and SureMark Digital have partnered to bring real-time, cryptographic identity verification directly into the cyber insurance ecosystem. As part of your policy, you now have access to the SureCircle™ Identity Assurance platform — a Virtual Private Identity Network (VPIN) that enables your team to verify the identity of executives, financial contacts, and critical vendors at the moment it matters most: before a transaction is authorized, before credentials are shared, before trust is exploited. This is not another training module or awareness campaign. It is an operational protocol — built on the same cryptographic foundations as blockchain itself — designed to make impersonation-based fraud structurally impossible within your organization's verified network. Together, Ambridge and SureMark are setting a new standard: identity-first security as a condition of coverage and a pillar of resilience.

MCDONALD HOPKINS COMPLIMENTARY PRE-BREACH SERVICES

RISK ASSESSMENT | INCIDENT RESPONSE PLAN | VIRTUAL BREACH RESPONSE WORKSHOP

McDonald Hopkins has partnered with *Ambridge* to offer you the following complimentary pre-breach services:

Risk Assessment

The strengthening of your data privacy and cybersecurity defenses begins with a data privacy risk assessment. After completing our Risk Assessment Questionnaire, a McDonald Hopkins data privacy attorney will review the results with your team, discuss areas of potential improvement/exposure, and help establish next steps.

Incident Response Plan

An Incident Response Plan is a critical component to proactive planning for data privacy compliance. We will work with your team to create an appropriate Incident Response Plan that can be used should you experience a data security incident. This is the "go to" document that identifies the appropriate internal and external resources to properly deal with a data breach. The plan will help clarify what steps should and should not be taken, detail the timing of certain necessary actions, and identify who should be on your Incident Response Team (a group of decision makers both within and outside your organization).

Virtual Breach Response Workshop

Our interactive Virtual Breach Response Workshops are designed for professionals who are on the front line of data breach risk management, including critical members from an organization's Incident Response Team from compliance, risk, legal, IT, information security, finance, business, human resources, and communications. The hour-long workshop helps you to be better prepared to respond to a data privacy incident and safeguard the organization. Prior to the workshop, our team will review your Incident Response Plan and recommend revisions, if needed. If you do not have an Incident Response Plan, one will be provided to you.

During the Breach Response Workshop, we review the latest trends and updates regarding applicable notification laws and offer multiple responses to data breaches. We then conduct an interactive tabletop exercise and provide you with a real-world scenario of a privacy incident. The hypothetical facts will also change throughout the mock incident just as they would in a real world incident. Our job is to lead your organization through a mock response to the incident based on your Incident Response Plan, while identifying any gaps in your plan.

If you are interested in any of these pre-breach services, email MH-AmbridgeIncident@mcdonaldhopkins.com

The Data Privacy and Cybersecurity team at McDonald Hopkins has counseled clients in nearly every industry, responding to thousands of data breaches and privacy incidents *each year*. As a Platinum Breach Coach®, we work closely with law enforcement, forensic investigators and third-party cybersecurity vendors to offer organizations efficient and effective incident response services in compliance with the numerous and rapidly changing state, federal, international and industry-specific privacy and breach notice laws. We also offer Cyber Savvy pre-breach services that focus on proactively managing personal, sensitive and confidential information and minimizing the risk of a data privacy incident. Our experienced team provides client support during investigations by state, federal and international regulators, and we have significant experience in privacy litigation prosecution (indemnification) and defense (single plaintiff and class action).

McDonald Hopkins®

Incident Response Hotline
855-MH-DATA1 (855-643-2821)
IR@mcdonaldhopkins.com

Managed Security Awareness Training

EXCLUSIVE FOR AMBRIDGE POLICYHOLDERS

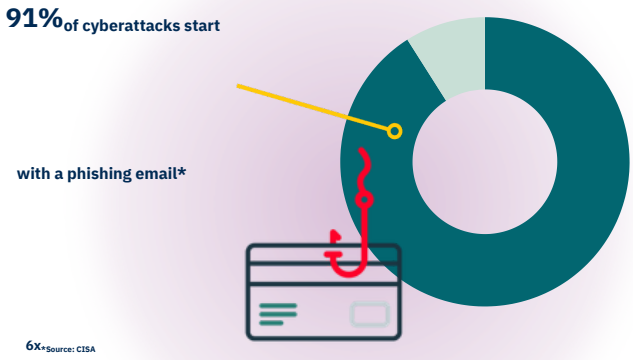
PONDURANCE®

ambridge®

Your employees are your first line of defense against cyber threats – and also your greatest vulnerability.

Phishing, social engineering, and business email compromise are the leading causes of cyber insurance claims. Technical controls alone cannot protect against human error. That's why Ambridge Partners has partnered with Pondurance to offer their policyholders a fully managed security awareness training program — at an extremely competitive price that makes it accessible to organizations of every size.

Ambridge believes so strongly in protecting their policyholders that they're investing in this program alongside you.



WHY SECURITY AWARENESS TRAINING?

- **Reduce your #1 risk:** Phishing and social engineering drive over 90% of cyber insurance claims. Training directly addresses this.
- **Protect company, employee, and customer data:** A single click on a malicious link can expose sensitive data across your entire organization and your clients.
- **Build a security-first culture:** Regular training and simulated phishing campaigns create lasting behavioral change — not just one-time awareness.
- **Strengthen your insurance posture:** Demonstrating proactive security measures may help reduce claims exposure and, as a result, may support more favorable underwriting evaluations and policy terms.
- **Meet compliance requirements:** Many frameworks and regulations require ongoing security awareness training for all employees.

WHAT'S INCLUDED

Ongoing Security Awareness Training

Regularly updated modules covering phishing, social engineering, password hygiene, data handling, and more.

Simulated Phishing Campaigns

Realistic phishing tests that measure your team's susceptibility and track improvement over time.

Risk Scoring & Behavioral Analytics

See which employees and departments are most at risk, with actionable data to focus your efforts.

Reporting Dashboards

Clear visibility into training completion, phishing test results, and organizational risk trends.

One hour risk assessment with Pondurance vCISO and other discounted Pondurance services

THE AMBRIDGE ADVANTAGE

Ambridge Sponsors the Management Layer

Ambridge covers configuration, campaign scheduling, reporting, and support. You pay only for platform licenses.

Extremely Competitive Pricing

Platform license cost is significantly below market rate — a managed program at an unmatched price.

Not Just a Tool — A Managed Program

Pondurance handles configuration, launches, tracking, and reporting. Expert-level security awareness without the overhead.

Quarterly Executive Briefings

Exclusive webinars on AI threats, quantum risks, OT security, and programmatic cyber risk reduction.

AMBRIDGE POLICYHOLDERS: YOUR EMPLOYEES ARE YOUR GREATEST ASSET AND YOUR GREATEST RISK. PROTECT BOTH.

GET STARTED TODAY

pondurance.com

Contact your Pondurance representative or visit the Ambridge policyholder portal for details.

DATA SHEET

MOXFIVE

ambridge®

Complimentary for Ambridge Insureds

Security Stack & Spend Review

A 60-minute deep dive into your client's environment, benchmarked against real incident data.

100+ Tailored Questions **20+** Security Catagories **60** Minutes, Live Scored

Give your clients a complimentary, real, actionable cybersecurity assessment. Uncover gaps, align technology with cyber insurance requirements, and deliver meaningful value that strengthens your client relationships and your bottom line.

How it Works

1

You Make the Intro

Refer an insured or client. We handle scheduling, preparation, and delivery.

2

60-Minute Intake Session

MOXFIVE leads a structured session covering environment, tools, controls, and spend.

3

Clients Receives Deliverable

Benchmarking report, architecture recommendations and a cost-aligned roadmap.

Our Approach

Security Stack & Spend Review - Project Methodology

Intake:

Evaluating Controls Through a Prevention Lens

- **Align on Business Context & Risk Priorities**
  Structured session to understand operating environment, risk tolerance, and what matters most to the businesss.
- **Evaluate Infrastructure & Security Controls**
  Controls assessed against leading frameworks and MOXFIVE's active incident data to identify structural gaps.
- **Review Tools, Spend & Overlap**
  Every tool mapped -- patching, RMM, EDR, backups -- to surface duplication, coverage gaps, and cost opportunities.
- **Assess Network Architecture**
  Review of servers, network design, and cloud environments for structural exposure and segmentation ris k.
- **Benchmark Against top Attack Vectors**
  Score the environment against MOXFIVE's top initial access vectors from hundreds of real IR engagements.

Output:

Benchmarking Insights Against Real Incident Data

- **Comprehensive Stack & Spend Review**
  Full infrastructure and security stack analysis with duplication, gap, and risk fi ndings mapped to actual tools and spend.
- **Benchmarking & Maturity Insights**
  The environment is scored and ranked across 20+ security categories, benchmarked against industry peers and MOXFIVE's incident data.
- **Architecture & Control Recommendations**
  Prioritized improvements to architecture, processes, and controls, tied directly to identifi ed gaps.
- **Prioritized Resilience Roadmap**
  A cost-aligned sequenced roadmap so the client knows exactly what to address fi rst and why.
- **Risk & Priority Profile**
  A documented snapshot of business context, risk tolerance and priorities, the baseline for all fi ndings.

Sample Assessment Output

Security Stack & Spend Review - What your client receives

68% Overall score
Adequate security posture

67/75 Questions answered

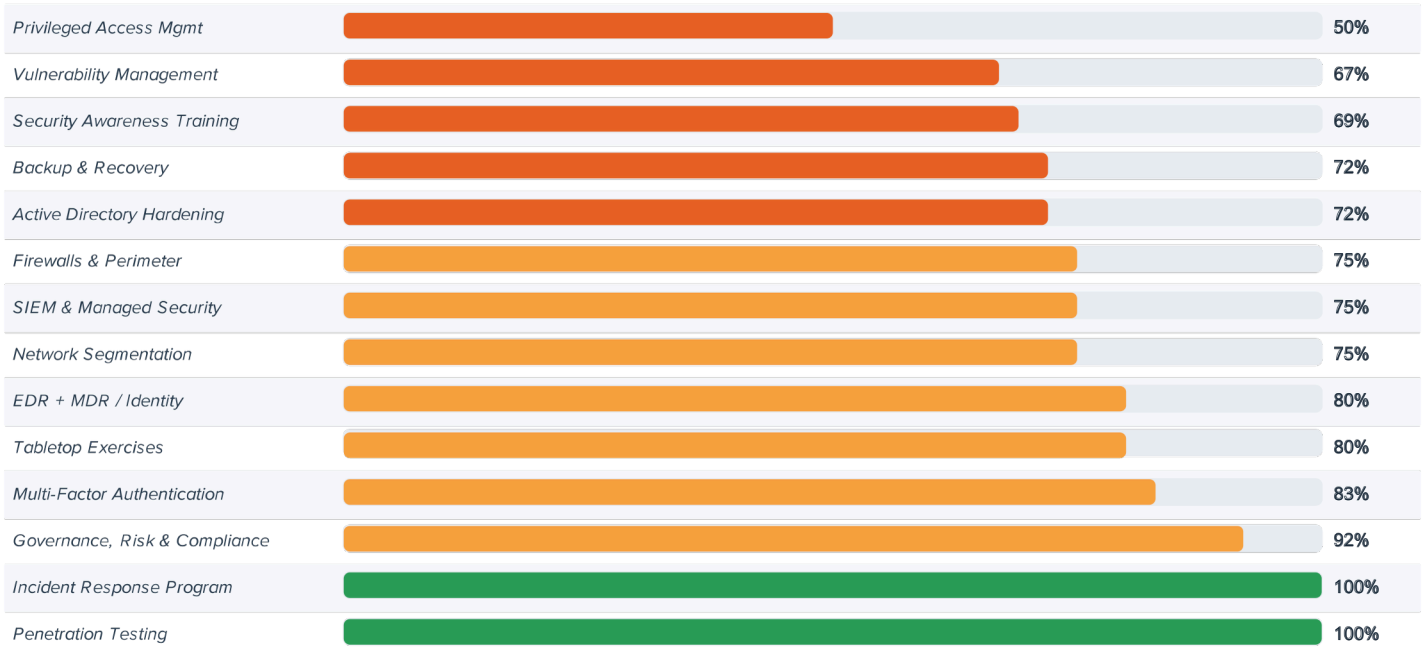
12 Gaps identified

20 Categories scored

2 Critical **3** High **5** Medium **2** Low
Gap Severity

Category Scores

Across 20 security domains (sample)



Executive Summary

✓ STRONGEST AREAS

IR Program 100% | Pen Testing 100% | Email Security 100%

⚠ FOCUS AREAS

PAM 50% | Vuln Mgmt 67% | Security Training 69%

TOP ROADMAP ACTIONS

CRITICAL Implement just-in-time privileged access (PAM)

HIGH Authenticated vulnerability scanning, full asset scope

HIGH Ransomware-specific security awareness training

What This Means For You

- Every gap is tagged by severity, so your team knows exactly where to focus first.
- Scoring reflects MOXFIVE's real-world incident data, not just compliance checkboxes.
- Focus areas link directly to recommendations in your Resilience Roadmap.

MOXFIVE is a cybersecurity company helping organizations respond to incidents and minimize the risk of future attacks. Over the last decade, our team of experts has helped thousands of businesses respond to major incidents and saw firsthand that there needed to be a better way for organizations to get the technical expertise they need when they need it most. Through a combination of our technical experts and proprietary platform, we bring order to chaos and deliver a tailored incident response approach and resilience-minded path forward for clients of all sizes, faster and more efficiently. .

www.moxfive.com

(833) 568-6695

proactive@moxfive.com

MOXFIVE ambridge