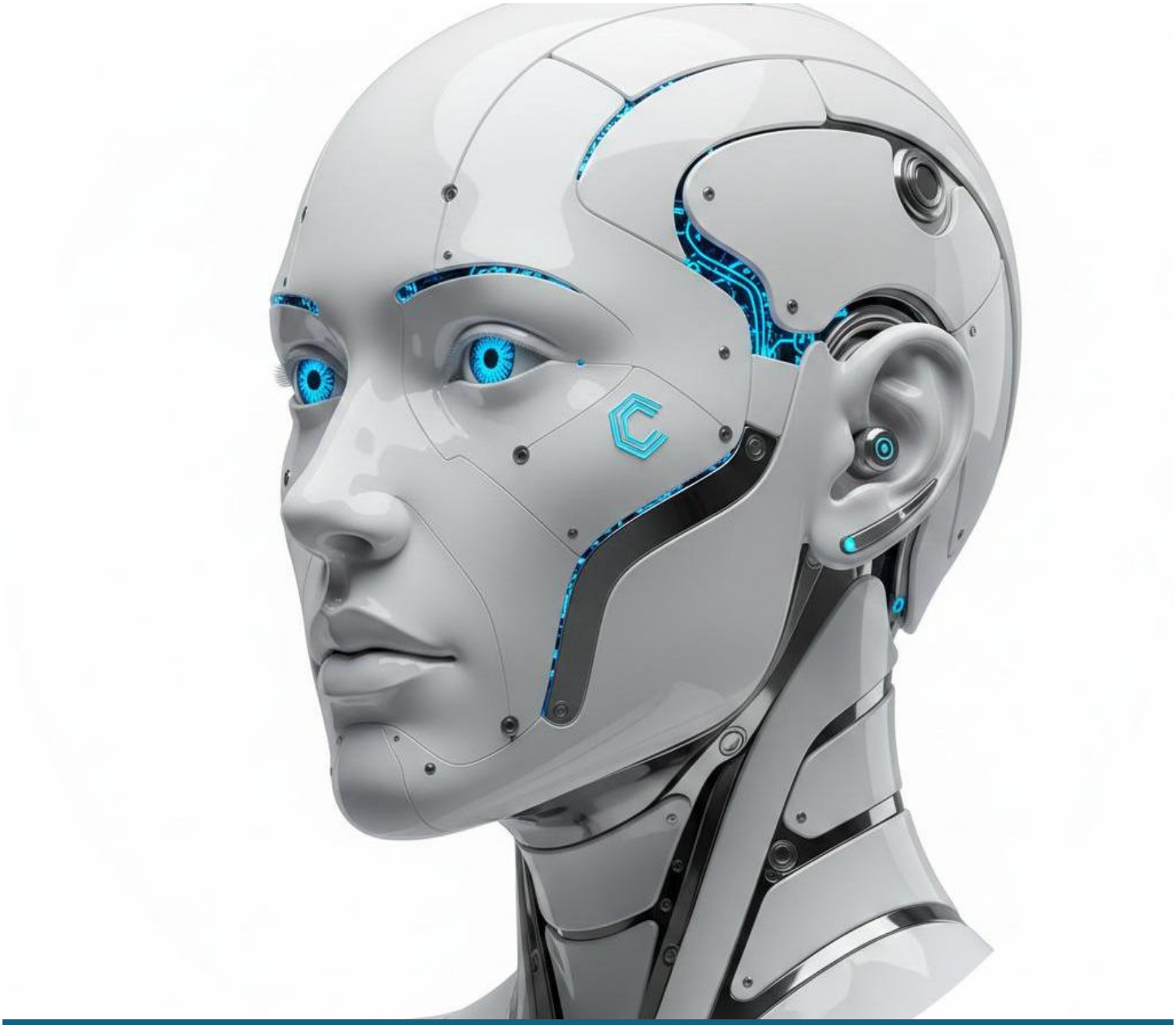


The Underserved SME Cyber Insurance Market

A Practical Guide for Insurance Brokers & Agents to tap into the $50B SME Proactive Cyber Insurance market

Barnaby Grosvenor

Sponsored by Cygienic.com

Preface

The Author

Barnaby Grosvenor is a seasoned Global Chief Information Security Officer with over 30 years of experience in cybersecurity, risk management, and digital transformation. He has advised boards and executive teams, building resilient security programs for Fortune 500 companies, financial institutions, and startups. A trusted industry voice and a founder himself, Barnaby brings deep enterprise expertise into the SME world.

The fastest-growing frontier in insurance

Proactive Cyber Insurance represents a new era of coverage where policies are dynamic, continuously adapting to the real-time risk landscape. Using AI, both insurers and policyholders can monitor threats as they develop, giving a live view of exposure and risk.

Premiums are no longer static, they can adjust in real time based on the actual risk profile of the business, rewarding proactive risk management and helping prevent losses before they happen. In this model, insurance becomes not just a safety net, but an active tool for risk reduction and informed decision-making.

Why this book - and whom it will help

Written for insurance brokers and agents who want to build real confidence in cyber insurance and participate in the $50B cyber market. You don’t need to become a cybersecurity expert, just understand the risks that matter and how to turn them into insurable, sellable policies.

A simplified, no-jargon approach to proactive cyber insurance

Cyber insurance can feel overwhelming, expensive, and full of confusing terminology. This handbook strips it back to the essentials, focusing on clear explanations, real-world examples, and practical steps you can take to add value with cybersecurity to your existing client base.

Building a client insurance portfolio

This handbook will take you from having little or no cyber insurance clients to a portfolio of new recurring revenue streams. You'll learn how CyberIQ tooling assesses client cyber risks like an underwriter, produces clear client reports, helps you place policies for businesses, and ultimately generates additional revenue by offering ongoing cyber monitoring licences alongside insurance cover.

Summary A broker-friendly playbook for breaking into the Proactive Cyber Insurance market, powered by CyberIQ Score Cards™ tooling that removes technical barriers and turns cyber risk into insurable, sellable outcomes.

What you'll walk away with

- How to assess an SME cyber risk, to binding an insurance policy.
- The confidence to discuss cyber risk with clients.
- New potential reoccurring revenue streams.
- Free access to CyberIQ.

CyberIQ Score Cards™

Chapter 1. The SME Cyber Insurance Opportunity

Imagine waking up to find your business wiped out by a cyberattack - no access, no clients, no way back. It's exactly what hit Mt Gox, Travel Ex and Medic Secure, to name but a few. Many SME businesses don't recover - downtime, lost revenue and reputation damage shut many within 6–12 months. **Yet despite 50% of SME's targeted by cyberattacks, 80% still lack basic cyber hygiene or insurance.**

Theres nothing to see here!

Let's start by setting the scene. Many companies don't realise they're already under attack. The most common SME response is, "We're too small to be a target," or "We don't have anything valuable." Unfortunately, this mindset is exactly why so many SMEs get caught out – and then close.

Cyberattacks routinely cause hundreds of thousands of dollars in damage, often hitting SMEs before they've had a chance to properly scale. If cybersecurity is ignored, the only alternative is having serious cash on hand to absorb the fallout - because when an incident happens, it becomes a business problem, not a technical one.

SME cyber insurance is the fastest-growing play

The cyber insurance market has evolved into one of the fastest-growing segments of the global insurance industry, with estimates showing the total market expanding rapidly

year-over-year. Current forecasts put the global cyber insurance market value at tens of billions of dollars, with projections of continued strong growth through the decade. For example, research suggests the global cyber insurance market could grow from around **$30B in 2025 to more than $50B by 2030**, reflecting a **CAGR above 25 %** in the long term.

Within this vast opportunity, the **SME segment represents a significant and underserved portion**. SMEs now account for roughly **10-20 % of global cyber insurance demand or premium revenue**, roughly **$4B in 2025**, despite making up over 90 % of all businesses worldwide. Yet penetration among SMEs remains low: estimates indicate **only 10–20 % of SMEs carry dedicated cyber insurance**, leaving a sizeable protection gap and a clear opportunity for brokers to educate, onboard, and insure this market.

This handbook is intended to help you bridge that gap. The SME cyber insurance market is **underserved for many reasons**, including perceived complexity, cost concerns, and lack of awareness - but that also means there's **significant new revenue to capture**. By understanding how to assess risk, structure policies, and introduce additional services (like ongoing cyber monitoring licences), today's brokers can be part of the solution while building new, recurring revenue streams in this expanding market.

Reasons why SME markets are underserved

- Lack of affordable distribution cyber risk tooling
- Lack of awareness and value from both client and insurer
- Limited professional cyber insurance underwriters
- Overcomplicated insurance survey forms
- Long process for small commissions
- Limited distribution and sales agents

How CyberIQ Score Cards™ can bridge the gap

- **Lack of affordable distribution cyber risk tooling**
  Traditional cyber insurance relies on manual processes and slow data collection. AI-driven tools like CyberIQ change this by automating risk assessments and delivering usable data in minutes or hours - not days or weeks. In an SME market, speed matters. This is a volume game with an affordable tool that can be distributed to agents.

- **Lack of awareness and value**
  Many SMEs don't fully understand their cyber risk or assume insurance is only for large enterprises. Brokers and agents are the critical link. With the right tools like CyberIQ, we can deliver reports, and clear insights, to demonstrate real risk and present cyber insurance as a practical, necessary solution. SME will then see value and start to become more aware of their risks.

- **Limited professional underwriter capacity**
  Cyber underwriters are stretched so insurers need to fill this gap with technology – tools like CyberIQ to provide 80-90% of what the underwriter requires to bind a policy - significantly reducing underwriter workload, turnaround time, and friction in the quoting process.

- **Overly complicated surveys**
  Long, technical questionnaires are a major blocker. The reality is only a small number of key questions are required. The rest of the assessment can be handled automatically through tools like CyberIQ's AI-powered data collection and analysis.

- **Processes that don't scale for small clients**
  Traditional underwriting processes aren't built for SME economics. AI shortens the entire journey - smaller surveys, automated risk assessments, and faster decisions, making cyber insurance viable for SMEs.

Summary The market opportunity is significant for insurers, brokers, and platforms willing to move now. SME cyber insurance is still in its early stages, with low penetration and rapidly increasing demand driven by regulation, supply-chain pressure, and real-world attacks.

Success in this market depends on simplifying distribution, automating risk assessment, and using tooling designed for high-volume, low-premium policies.

Chapter 2. Tips to Win SME Cyber Insurance Deals

Selling cyber insurance to SMEs is not the same as selling to large enterprises. Time is limited, budgets are tight, and patience for complexity is low. Winning deals in this market comes down to doing a few things exceptionally well - and avoiding some common, costly mistakes.

The insurers and brokers who succeed understand what SMEs care about, keep the process simple, and focus on practical risk reduction rather than fear or jargon. Just as importantly, they know what *not* to do. The following tips outline how to build trust, move faster, and consistently close SME cyber insurance deals.

How to respond to reluctant SME clients

Client: I don't have a cyber budget

Agent: Most businesses allocate up to 10% of their IT budget - or roughly 1–3% of total revenue - to cybersecurity. To stay competitive and avoid costly surprises, those investments need to be smart, targeted, and risk-driven. We can help you here.

Client: I'm too small to be hacked

Agent: About 50% of cyberattacks now target SMEs. Cybercriminals often see smaller businesses as the easiest way in, either directly, or as a stepping stone to bigger targets in the supply chain.

Client: I don't have much technology or value to steal

Agent: The hackers don't always just want your data or client list - they want your systems and resources.

- **Botnets, proxies & malware farms:** Hackers use automation to sweep up thousands of small companies at once, turning compromised systems into botnets. Your tech and resources are quietly hijacked and used to attack others.
- **Impersonation & pivot attacks:** Your email, logins, and cloud access are valuable on their own. Attackers use them to impersonate you, pivot into customers and partners, or move money - hiding behind your trusted identity.
- **Resources and accounts** – Many SME breaches happen early and remain undetected for months. Attackers quietly abuse compromised accounts to spin up cloud services for further attacks, cryptocurrency mining, or illicit hosting, often only discovered when usage bills spike.

Client: I can't afford cyber insurance

Agent: Can you afford to lose your business? Cyber risk is a business risk, not an IT issue. Cyber insurance can start from as little as $99 per month, while the cost of recovering from a cyberattack often runs into the hundreds of thousands, and in many cases, millions, before factoring in lost revenue, cash flow disruption, or reputational damage.

Client: It's an IT problem

Agent: Cybersecurity risks are business risks because they impact where it hurts most: revenue, cashflow, customers, and reputation. A cyber incident can stop sales, delay product launches, trigger regulatory fines, void contracts, and erode customer trust overnight.

Client: Cybersecurity is too expensive.

Agent: Be wary of flashy tools or promises of "ultimate protection". No tool, not even AI, can eliminate risk entirely. However, here are four basic things that you can do for FREE:

- Free Built-in firewalls and antivirus from Microsoft or Apple operating systems are usually sufficient enough for Startup workstations.
- Free application patch updates- simply ensure auto updates are set on your key applications. You may need to consider servers as a manual update but build that into your maintenance process – it's also free.
- Free Two-factor authentication (2FA): Google or Microsoft authenticator code for servers and for your mobile clients to access servers.
- Free cyber hygiene practices as covered in Chapter 3 and 4.

What does a good cyber insurance policy look like?

Most cyber insurance policies offer broad coverage, but the details matter, especially for SMEs. We don't recommend any single insurer, and you should always shop around for the best option in your market. That said, a strong cyber insurance policy should include the following fundamentals:

- **Ransomware coverage** – including extortion payments, negotiation support, and recovery costs.
- **Clearly defined business interruption cover** – with transparent triggers and realistic limits for downtime and lost revenue.

- **Immediate access to cyber security experts** – covering incident response, forensic investigation, IT recovery, and legal support.
- **24/7 breach response hotline** – cyber incidents don't wait for business hours.
- **Coverage limits aligned to your business size and risk** – avoid both underinsurance and unnecessary over-coverage.
- **Industry-specific coverage** – confirm your sector is explicitly covered, especially if you handle regulated or sensitive data.
- **Regulatory and legal cost coverage** – including notification costs, fines (where insurable), and legal defence.
- **Third-party liability protection** – for claims from customers, partners, or suppliers affected by a breach.
- **Social engineering and phishing cover** – many losses occur without "technical hacking."
- **Clear exclusions and conditions** – understand what security controls are required to keep the policy valid.
- **Pre-incident support** – some insurers offer risk assessments, training, or monitoring as part of the policy.

A good cyber insurance policy doesn't just pay out after an incident, it helps you respond faster, reduce impact, and stay in business when something goes wrong.

CyberIQ Score Cards™ : the ultimate sales tool

CyberIQ is not just a central platform for managing client cyber risks—it's also a powerful tool to **drive sales, build trust, and retain clients**. Here are practical ways to use it in your sales process:

- **Pre-scan for ASM grade** – Run a quick asset surface mapping (ASM) scan to highlight vulnerabilities. A low grade can spark conversation about potential risks and the need for insurance coverage.
- **Instant risk assessments** – Fully onboard a company and perform scans in minutes. This allows you to share real-time risk insights and tailored insurance quotes during client meetings.

- **Client-facing tool** – SMEs often have limited cyber capabilities. Offering CyberIQ as an affordable, easy-to-use platform gives them immediate value and positions you as a trusted advisor.
- **Stickiness and renewal leverage** – Once clients start using CyberIQ, it encourages ongoing engagement. You can track progress and naturally manage policy renewals.
- **Demonstrate measurable improvements** – Show clients how their risk profile evolves over time. Visual progress reports reinforce the value of both your advisory and the insurance coverage.
- **Upsell opportunities** – Use risk assessments to identify additional coverage gaps or premium add-ons that align with the client's evolving needs.
- **Client education and credibility** – Walk clients through actionable insights, helping them understand risks in plain language. This builds trust and strengthens your advisory role.
- **Benchmarking and competitive advantage** – Show SMEs how they compare to peers in their industry or region, reinforcing the need for proactive coverage.
- **Quick wins for cold leads** – Even before a full policy discussion, you can offer **instant insights** that demonstrate your expertise and open the door to deeper conversations.

Using CyberIQ in your sales workflow transforms cyber insurance from a "nice-to-have" into a tangible, visible solution that clients can see, understand, and rely on.

CyberIQ: Delivering value to your clients

- **Client-facing platform** – Many SMEs have limited cyber capabilities and little visibility into their risks. CyberIQ provides an affordable, easy-to-use platform that gives them immediate insight into their security posture.
- **Empowers decision-making** – Clients can see where their risks lie, prioritize actions, and make informed decisions about mitigation or insurance coverage.
- **Actionable guidance** – CyberIQ doesn't just show problems; it provides practical, step-by-step recommendations to improve their security posture, even without a dedicated IT team.

- **Continuous visibility** – Clients can monitor their risk over time, track improvements, and see how changes reduce exposure. This turns cyber risk from a vague worry into something measurable.
- **Builds trust with your advisory** – By giving clients access to a professional-grade tool, you position yourself as a proactive, value-adding advisor, not just an insurance salesperson.
- **Supports regulatory and stakeholder confidence** – CyberIQ helps clients demonstrate due diligence to investors, partners, and regulators, showing that cybersecurity is taken seriously.
- **Long-term engagement** – Clients using CyberIQ naturally stay connected with you, providing opportunities for renewals, upsells, or advisory services as their business grows.

In short, CyberIQ turns cyber risk from a blind spot into a **visible, manageable, and actionable asset**, giving clients peace of mind while strengthening your relationship and advisory role.

When clients should consider cyber insurance

If your client's likelihood of a cyberattack exceeds their company's risk tolerance, and improving compliance or attack surface risks will take time to resource, it's worth considering a cyber insurance policy. This helps protect the business while they work to strengthen controls and reduce exposure.

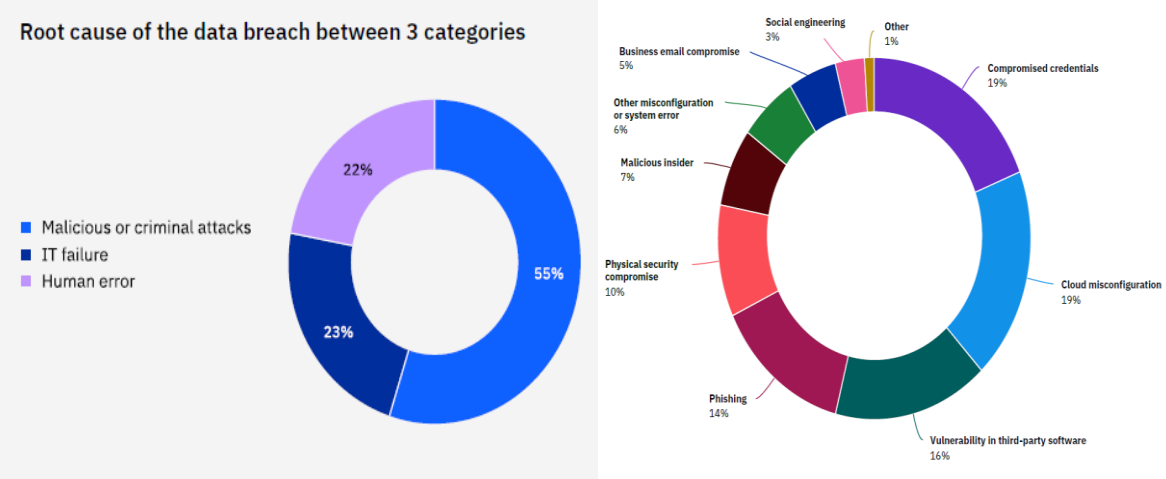
Chapter 3. Know Your Cyber Risks

Highly sophisticated attacks start with basic weaknesses that were never addressed. Simple, repeatable practices like keeping systems properly updated, patching known vulnerabilities, securing access, managing passwords, and monitoring changes dramatically reduce the chances of something going wrong in the first place.

To summarise the landscape, IBM publishes an annual report analysing the sources of cyber incidents. The findings are clear. Fifty-five percent of incidents involve malicious attacks - often exploiting poorly maintained or unpatched systems. A further 23% result from IT failures or system errors, while 22% are caused by human error.

Together, these figures highlight a simple truth: most cyber incidents are preventable with the right visibility, processes, and leadership attention.

IBM cost of a data breach 2024 and 2020



What hackers really want

- **Botnets, proxies & malware farms:** Hackers use automation to sweep up thousands of small companies at once, turning compromised systems into botnets. Your tech and resources are quietly hijacked and used to attack others.
- **Impersonation & pivot attacks:** Your email, logins, and cloud access are valuable on their own. Attackers use them to impersonate you, pivot into customers and partners, or move money - hiding behind your trusted identity.
- **PII and IP:** Most startup breaches happen early and go unnoticed. Many companies stay compromised for months before realizing it – Today, the most sort after attack is still personal data and company IP.

The Top 5 cyberattacks targeting SMEs and how to stop them

If a large share of cyber incidents come from the same top 5 five attack paths, then prevention is about tackling those risks early - before they turn into problems. The good news is this doesn't require heavy spending, or complex security programs. Most of these risks can be reduced with simple, preventative measures and a small number of well-chosen tools. In other words, smart basics go a long way.

1. Email phishing prevention

No.1 cyberattack vector is email-phishing: 70-90% of cyberattacks start from a phishing email or social engineering – the main reason is because its cheap and easy.

We can address this challenge in several ways using CyberIQ's modules - specifically the Cyber Library and ASM. These tools help identify risks, track vulnerabilities, and provide actionable guidance so you can proactively strengthen your security posture.

- **User Awareness:** Provide staff with a simple guide to help them recognize suspicious emails before they click. CyberIQ has email phishing user awareness material you can adapt and use – simply send a PDF format to staff.
- **Social Engineer:** Add new processes to double check things before a new request is made to transfer money, change data, share any credentials, or give access to someone – the old CEO scam email requesting urgent money transfer simply needs a call back and a share the secret code process. If a company has changed its bank details via email, again a call them and check before making the change.
- **Technical Protection:** Use CyberIQ's ASM module to scan your email systems and check whether phishing emails from outside your company can be detected and blocked. Start with basic configurations like SPF, DKIM, and DMARC settings - your email provider can help ensure these are correctly set up. Regularly verifying these settings strengthens your defences against common email-based attacks.

2. Data leak prevention

We can detect potential leaks of your company's confidential data using CyberIQ's Data Leak module. This feature scans across public and hidden sources - including the dark web, shared documents, and code repositories - to uncover exposed credentials, sensitive files, or other critical information before attackers can exploit it.

Data Leak Checks: CyberIQ lets you search for potential leaks by targeting specific keywords or domains. For example, user credentials often appear on hacker paste sites or in other dark web locations. Simply enter your company domain, and the system

scans for exposed assets. You can also extend the search to areas like developer code repositories, where system configurations or access credentials may have been accidentally left behind.

3. Weak password, stolen credentials prevention

We can use CyberIQ's Email Breach Scanner to detect whether any company email credentials have been exposed - either through your own applications or third-party services used by your staff.

Email Credential Scanner: This feature scans your domain against online cyber services that track compromised email accounts. If any company emails are flagged as compromised, the system immediately notifies you – the request would be to notify staff so they can reset their passwords and prevent unauthorized access. Regular use of this tool helps reduce the risk of account takeover and keeps your business protected.

4. Website and application security flaws Prevention

Here, we use the ASM (Attack Surface Manager) tool to scan all external servers for vulnerabilities, potential compromises, and data privacy risks. The tool also provides a standard cyber rating for each server, helping you prioritise which issues need attention first and giving a clear overview of your external security posture.

Attack Surface: Your attack surface is the most common entry point for attackers and should be a primary focus for identifying misconfigured or unpatched internet-facing systems. While internal (non-internet-facing) servers should also be assessed, external systems carry the highest risk - and weaknesses exposed externally often indicate similar gaps internally.

5. The 3rd party supply chain risk prevention

Using CyberIQ's ASM module**,** we can anonymously scan third-party, externally facing servers to assess their cybersecurity posture. In addition, we can send the target a compliance survey to gather self-reported security information. All results are consolidated in the Portfolio dashboards, giving you a clear, consolidated view of your supply chain's overall cyber exposure and helping you identify areas that need attention.

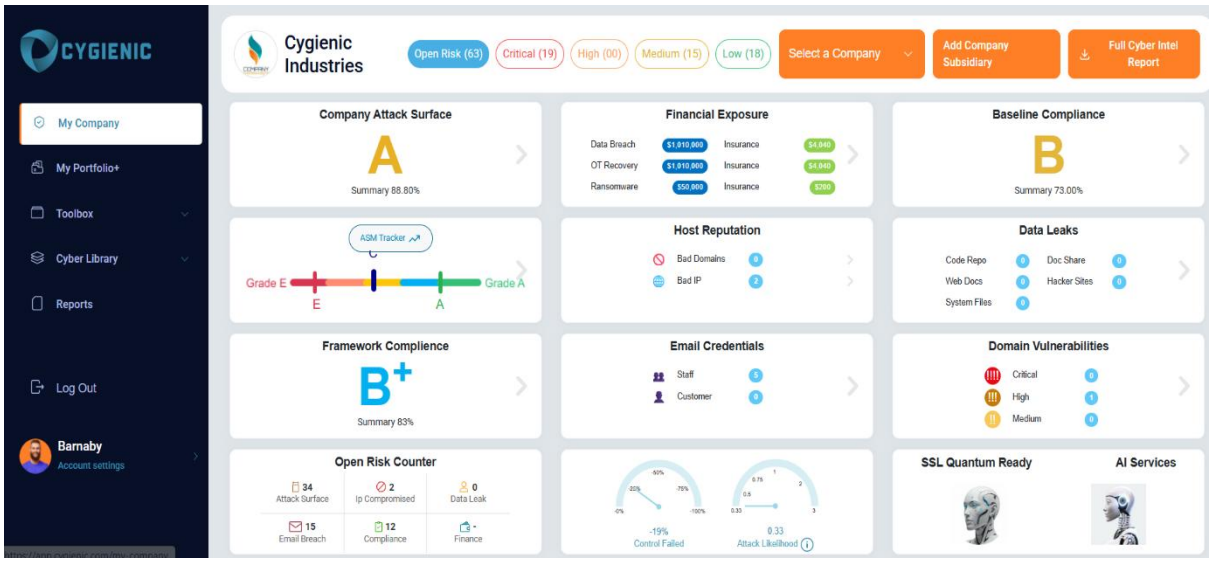
3rd Party Portfolio: Assess your third-party ecosystem using a two-pronged approach. First, run non-intrusive, passive attack-surface scans on suppliers and partners to identify externally visible weaknesses - without touching their systems Second, issue a

simple cyber compliance questionnaire (with optional financial surveys) to assess the maturity and credibility of their responses.

Summary Don’t panic - this is the only technical chapter in the handbook. Focus on understanding the top five cyberattacks and how CyberIQ helps protect your clients. For anything more technical, our support team is always there to help.

CyberIQ Score Cards™ Using a single platform to manage these preventative steps is the most effective way to reduce cyber risk. CyberIQ does exactly that - clearly highlighting where risks exist throughout your business and giving you a practical, structured way to manage and reduce them over time. It’s not just about identifying issues; it’s about maintaining visibility and control, so risks are addressed before they become incidents.

CyberIQ Score Cards™



Chapter 5. Keeping Your Client Base

As your cyber insurance client base grows, retention becomes just as important as acquisition. The real opportunity is keeping clients renewing with you year after year. SMEs are far more likely to stay loyal when they clearly see ongoing value, not just at policy inception, but throughout the year.

Adding clients to your CyberIQ account delivers that value by giving them continuous visibility into their cyber risk, clear improvement actions, and tangible proof that you're actively supporting their business, not just selling a policy.

The Proactive Cyber Insurance value-add service

SMEs are increasingly looking for more than just a policy—they want real value from their cyber insurance. This is where Proactive Cyber Insurance makes a difference. By combining traditional cyber insurance with practical cybersecurity support, you give clients more than protection: you give them actionable insights, ongoing risk management, and confidence that their business is being safeguarded.

When clients see tangible benefits beyond the policy itself, they are more likely to trust you, stay loyal, and view your service as indispensable.

Regular automated risk reports

Using CyberIQ can help automate much of this process, providing dashboards, risk scores, and ready-to-share reports so you can deliver consistent, professional updates without it becoming a full-time burden.

This allows you to focus on growing clients while maintaining confidence that your cybersecurity reporting is reliable.

Continuously Monitor Risk

Continuous monitoring reduces the day-to-day burden on you and your team, ensures nothing slips through the cracks, and provides instant visibility when risks arise. By building automated monitoring into your cybersecurity strategy, you can stay ahead of threats while keeping your focus on scaling the business.

Summary

As your cyber insurance client base grows, retention becomes just as important as acquisition, and SMEs are far more likely to stay loyal when they see ongoing value beyond the initial policy. Proactive Cyber Insurance, combined with CyberIQ, delivers this by providing continuous visibility into client risks, actionable improvement steps, and automated dashboards and reports that make risk management simple and professional.

Continuous monitoring ensures threats are identified in real time without adding extra workload, allowing you to support clients effectively, build trust, and maintain long-term relationships while focusing on growing your business.

CyberIQ Score Cards™ - **Get started with your free trial of CyberIQ today.**

To sign up, please contact **sales@cygienic.com** and have your insurance registration number and company email ready. CyberIQ gives you immediate access to powerful tools that help you assess and manage client cyber risks, generate automated reports, and deliver real value to your cyber insurance clients.

For more information about how CyberIQ can support your business and enhance your cyber insurance offerings, visit www.cygienic.com/cyber-insurance.

CyberIQ Score Cards™ 2026