EGB's Cyber Program from the Point of View of Brokers & their Clients

EGB Insurance is a recently established MGA owned by Emrys Technologies Inc., an AI analytics company. EGB is focused on underwriting and managing claims for healthcare cyber risks in North America.

Working closely with hospitals and their brokers, we have:

- Created analytics that assess the vulnerability of a client based on both their inherent risk and the effectiveness of their controls;
- Designed analytics that provide hospitals and healthcare facilities with detailed, actionable data about their cyber risk they cannot get anywhere else;
- Created processes that help these facilities reduce the uncertainties of cyber risk; and
- Established relationships with insurers who recognize the need for high quality cyber risk management to be combined with competitive cyber insurance premiums.

Our unique approach integrates insurance with a hospital's risk management and leads to added value for all parties involved. Our hospitals are able to make better informed risk management decisions and brokers are able to offer a policy that is the most competitively priced (for most clients) while providing a program that differentiates them from their competition.

Neither hospitals nor brokers can obtain these advantages anywhere else.

Table of Contents

Cyber Risks Can Be Underwritten Rationally & Profitability

Cyber risks are increasing every day and getting more complicated by the minute. There are not enough historical claims to use traditional underwriting methods and carriers are having difficulty controlling the claims when they occur.

The result is that virtually every carrier – recognizing that they don't have a good understanding of the risk itself, nor do they have any meaningful control of the claims – price their policies with a huge risk margin in the premium.

EGB takes a different approach, which drives value for all parties involved. Our premiums are based on the following pillars:

- Data-driven analysis of an applicant's inherent risk.

- Detailed assessment of the vulnerability of each applicant.

Armed with these two sets of information, we first calculate (with a proprietary underwriting engine) the applicant's actual risk without any additional premium margin. We share the risk calculation with both the hospital and our insurance partners; and we add the insurer's required margin to the applicant's actual risk to develop a premium for the limit and deductible of their choice.

In addition to our accurate premiums, the following ensures we effectively mitigate the impact of a breach:

- Our policy requires that we be involved in any incident well before it reaches the deductible.
- Our response team is trained to focus on the litigation risk and regulation compliance of an event. These make up 50%+ of all cyber claims by value.
- Our customized incident management playbook provides an insured with actionable step-by-step instructions, reducing their reputational damage, something that isn't insurable.

The rest of this document goes into more detail on each of the elements of our program.

Helping Hospitals Assess, Prepare, and Respond to a Breach

Many different processes, skills, and teams (internal and external) need to be carefully coordinated - before, during and after a cyber incident - if cyber risk and claims are to be effectively managed and mitigated.

Preparing

EGB supports hospitals in the strategic stage of cyber risk management by providing a completely transparent breakdown of the amount of cyber risk the hospital has, where the main hot spots are, and what the hospital could do to alleviate these. Based on this input, a hospital can – for many of them this is the first time they will be able to do this – set a risk appetite and design a process that ensures their risk remains in some agreed relationship with their risk appetite.

In addition to supporting a hospital's strategic risk management planning, EGB is also able to play a supporting role in the day to day decision making of cyber risk management – whether it is in designing or implementing new preventative, detective or corrective controls – or whether it is in the planning or training that goes into preparing to respond to a breach.

The support involves EGB re-running our assessment application (how we identify the vulnerability of a hospital's system) in the light of any significant changes that the hospital may be considering. This allows a hospital to make changes based on a cost/benefit analysis they cannot get elsewhere. EGB, through its sister company Caerleon Security, can also provide more in-depth services as noted below.

Helping to Manage a Breach

Our policy encourages a hospital to reach out to us early in the response process and offers options as to how they want to manage a breach. Specifically:

- The policy requires that we join their response team well before the costs of dealing with a breach hits the deductible. This provides an additional layer of breach management expertise for the hospital (at no cost to them) and a significant improvement in a carrier's claim management goals.

- The policy offers two options as to who does the actual breach management:
    - The client can tell us in advance who is going to be the breach manager, IT Forensic, compliance, and notification specialists along with parameters of what they are going to charge; or
    - The client can choose to use members of our panel to be their response team as soon as it is clear that an incident has a significant probability of being insured. Once an incident crosses the deductible, the breach response costs are simply taken over by the carrier, simplifying claims management for the benefit of both hospital and carrier.
    - How the client chooses to manage breaches will be reflected in the premium for the benefit of both the client and the carrier: the objective is to give the hospital control of their premiums, at the same time allowing the carrier to more accurately price their risk.

Preparing for Litigation, Reduce Damage to a Client's Reputation, and Claims Management

Once the immediate breach investigation and response have been addressed, there remains the potentially most expensive and awkward part of the process; defending allegations of negligence from plaintiffs' attorneys or regulators. A key part of our integrated cyber risk management strategy is that much of our '*before*' work is designed to support this trickiest of '*after*' roles.

But, in addition to preparatory work, we also have legal and network security expertise in-house, and we have partnerships with firms such as Baker Hostetler, Kivu Consulting and ID Experts - amongst others - who provide us with their expertise. We also have contracts in place to handle the more commoditized elements of a breach response, such as letter mailing, and call center services.

We have chosen our vendors for the combination of the quality of their work and their costs; the quality of their work is our primary motivator. As noted above, we do not insist that our policyholders use the incident response teams we know and trust, but they are rewarded with a lower premium if they do.

Our policy acknowledges that some hospitals will have existing relationships with their vendors or will have other vendors they would like us to work with in the event of a breach. We are happy to discuss each hospital applicant's particular preferences before a policy incepts so that it can be considered in the premium for the benefit of both hospital and carrier.

Comparison with other Carrier's Breach Team or Risk Management Products

	Caerleon Security	Other Response Teams
Level of engagement and client benefit	Strategic. As immersive a solution as the client wants: • Quantitative Vulnerability Assessments. • Risk reduction using cost / benefit analysis. • Incident preparation on all levels, not just IT. • Interface with ERM Program. • Helping to interface with C-Suite & Board. Comprehensive Incident Response with lawyers, PR, and notification experts.	Tactical & narrowly focussed – looking to block threats and the IT portion of breaches. Focused on IT, not minimizing the reputational risk or the risk of litigation for the client.
Market Focus	All commercial clients including education and municipals.	Military, government, law enforcement and Fortune 500 companies.
When do we engage?	When cyber risk becomes a priority for the Board or is required by a policy.	When IT looks for new security software or there is a breach.
Who is the customer?	Board, C-suite	IT security buyer
Who do we interact with at the insured?	Every part of the entity involved in managing cyber risk: IT, Legal, PR, Privacy, Security, etc., as requested by the hospital.	IT security buyer
Can they offer protection from the financial impact of cyber risk?	Yes	No
Breach support offered	All facets - from PR to legal compliance, notification, and defense.	Usually IT forensics only

Other Advantages to a Client

Through EGB Insurance's in-house breach management team, Caerleon Security[1], hospitals gain the ability to re-assess their vulnerability whenever they need to. Whether a proposed change is significant,

[1] www.caerleonsecurity.com

like the potential introduction of a new business model or is less dramatic, such as the possible implementation of a new BYOD policy, Caerleon can re-run the control assessment to show how the change might impact the hospital's risk rating. If the change produces a reduction in the hospital's risk, they can also benefit in the form of a reduced premium.

Applicants who buy EGB's insurance will also be able to enjoy discounts on Caerleon's advisory services. These include, but are not limited to:

- Deep dive assessments (deeper than we need to go for insurance underwriting) providing insureds with a deep understanding of their vulnerability.
- Advice on how best to deploy their budget to reduce their vulnerability. This is a formal, prioritized cost / benefit study of all available improvements.
- An Incident Management Playbook, which guides an insured through every action required in the face of an incident or event, which ensures proper compliance with a mosaic of regulations.

At its most involved, Caerleon can support a hospital as it maintains a state of 'constant readiness' to manage a privacy or security breach. 'Constant readiness' means that a hospital is always as always as up to-date as it can reasonably be in terms of best practice prevention controls or patching or employee training or any one of the number of elements a plaintiff's attorney might look at – with the benefit of hindsight – to put together a 'hard to defend' picture of the hospital's alleged negligence in how they managed cyber risk up to the point where a potential breach is discovered.

EGB's Program Summarized

Cyber risks are the most visible and fastest growing risks facing the health care industry. Our specifically tailored policies, integrated approach and accurate pricing, positions EGB to be the pre-eminent MGA in this growing market.

Even though both the Affordable Care and HITECH Acts are imposing massive change on every hospital, cyber risk remains one of the most visible and fastest growing risks facing the health care industry. At a strategic level, EGB is specifically positioned to support hospitals as they navigate the information system challenges posed by the Affordable Care and HITECH acts, where our risk measurement accuracy and transparency, and our integrated approach positions EGB to be the pre-eminent MGA in this growing market.

Tactically, the very public nature of many cybersecurity breaches has brought cyber security protections and insurance to the attention of Boards and C-Suites. Executives, concerned with reputational and financial damage to their organizations, are seeking out measures to protect their organizations and themselves holistically. Our integrated risk management underwriting and companion insurance policies are tailored specifically to these clients.

Underwriting cyber policies for healthcare facilities, using data-driven analytics to accurately price insurance applicants based on their actual risk leads to a more accurate premium that is, in 75% of cases, the lowest bid; understanding the hospital's risk management processes and supporting their decision making processes throughout the year, ensures their risk and insurance are always in sync.