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

EGB Insurance is a unique entity owned by Emrys Analytics INC., an AI analytics company. EGB is focused on underwriting and managing claims for Healthcare and Repository cyber risks in North America.

Working closely with clients 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, resulting in accurate premiums which allow us to be the lowest bidder **75%** of the time;
- Designed analytics that provide the Healthcare Industry and Repository companies with detailed, actionable data about their cyber risk they cannot get anywhere else;
- Created processes that help these clients 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 and risk management, leading to added value for all parties involved. Our clients 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 coupling that with a risk management program that differentiates them from their competition.

Neither clients nor brokers can obtain this advantage 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, and we have found that we are the **lowest** bidder approximately **75**% of the time because of this. 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 client 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.

Repercussions of a Cyber Incident and/or Breach

A breach brings financial and reputational damage as well as disruption to the victim. A portion of this financial damage comes directly from the costs of the actual incident including legal fees, regulatory fines and response services such as identity protection plans. However, it is often overlooked that this is only a fraction of the eventual cost to the client. The second, and more significant cost is the "Reputational Risk" a client faces, something that's not insurable. Reputational risk often leads to the loss of revenue resulting from the turnover of customers following a privacy incident. A study done by IBM and the Ponemon Institute titled *2016 Cost of Data Breach Study: Global Analysis*, determined the following:

- Data breaches cost the most in the United States and the average total organizational cost in the US was $7.01 million.
- Regulated industries, such as healthcare, have the costliest breaches because of fines and the higher than average rate of lost business and customers.
- Healthcare Organizations had an average cost of $355 per record. An incident response team reduced the cost of a data breach by $16 per record. For the second year, this study showed the relationship between how quickly an organization can identify and contain data breach incidents and financial consequences

These findings highlight the importance of a client incorporating a holistic breach management program into their defenses to accompany their insurance policy.

In-House Breach Management Team – Caerleon Security

In addition to our accurate premiums, EGB Insurance makes available a breach management team, Caerleon Security[1]. They get as involved in the process as the client would like. They can offer options and suggestions for the client to help them understand their vulnerability and prepare for a potential breach. Specifically, Caerleon offers the following at greatly discounted rates:

- Deep dive assessments (deeper than we need to go for insurance underwriting) providing the insured with a very detailed 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.

Using these advantages, clients gain the ability to re-assess their vulnerability whenever they need to. Whether a proposed change is significant, 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 client's risk, they can also benefit in the form of a reduced premium.

For when an incident occurs, Caerleon offers the following:

- Comprehensive breach response services at a reduced hourly rate. The result is an additional layer of breach management expertise for the client and a significant improvement in a carrier's claim management goals.
- An Incident Management Playbook, which guides an insured through every action required in the face of an incident or event, ensuring proper compliance with a mosaic of regulations. The playbook is explained further in the next section.

For very large and experienced clients there might be a team of IT security experts well trained in breach response and risk mitigation. But for the vast majority of clients, no one expects them to incur the cost of maintaining and keeping up to standards a team of people they might use once a decade. For the vast majority, the smart solution is to have on standby experts to help when needed – like a fire department.

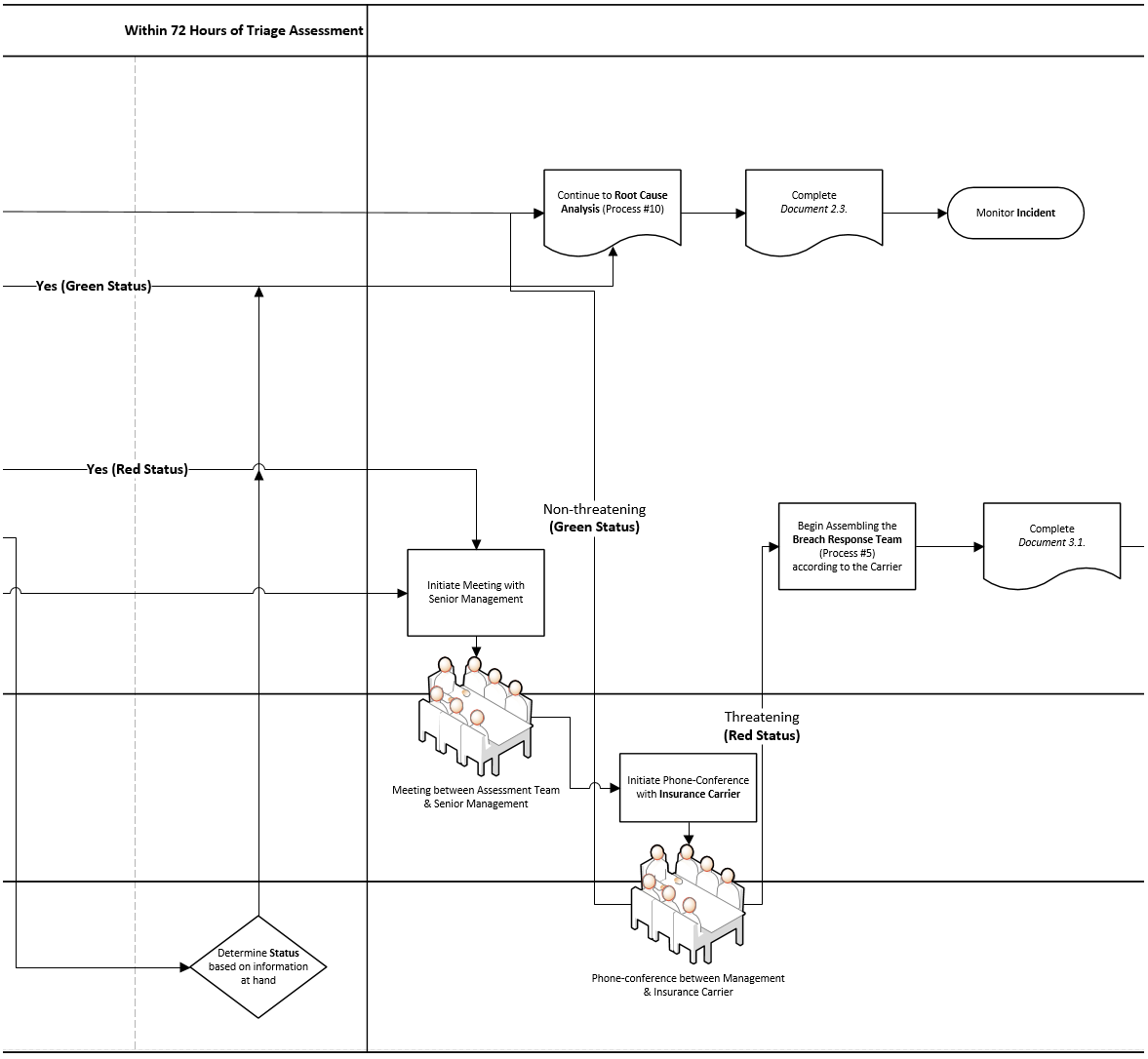
Caerleon's Incident Management Playbook

Caerleon provides a customized playbook for EGB clients: a **step-by-step process** for what a client would do in the event of an incident. Much like a fire escape route, the step-by-step incident response process will have been planned well in advance of an event. Caerleon's playbook will save you time, make your response more effective, and will reduce your financial and reputational vulnerability.

More specifically, the playbook comprehensively explains every action you must take regarding notification requirements, when to hire external vendors and lawyers, the chain of communication between all parties involved for each specific client and much more.

[1] www.CaerleonSecurity.com

A sample extract of our playbook can be viewed on the next page.



E|G|B insurance

Other Members of our Team

Our policy acknowledges that some clients will have existing relationships with vendors or will have other vendors they would like us to work with in the event of an incident.

We have legal and network security expertise in-house, and we have partnerships with firms such as Baker Hostetler, NCC Group – a world renowned cyber security and risk mitigation company, 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.

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 focused – 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

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 entity in this growing market.

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 the healthcare and repository industries , 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.

The result of EGB's unique breach management is reduced direct costs which will ultimately lower the amount of financial and reputational damage a client will experience. Secondly and most importantly, our playbook will give a client a plan to follow well before an incident happens, and our breach response team will be available right from the start. This effectively reduces the clients reputational and financial damage and the huge disruption an incident imposes on the client.