

Cyber & Terror Response: How Starr Companies is addressing the security concerns of middle-market businesses

An Interview with
David Norfleet, Senior Vice President and Chief Underwriting Officer;
and Reggie Gibbs, Senior Underwriter and Product Manager, Starr Companies

EDITORS' NOTE *David Norfleet is Senior Vice President and Chief Underwriting Officer of Starr Surplus Lines, a Division of Starr Companies. Prior to joining Starr, Norfleet served in leadership positions in the insurance industry for more than 30 years. He holds a Bachelor of Science degree from the University of Richmond.*

Reggie Gibbs is a Senior Underwriter and Product Manager for Starr Companies, providing leadership for the company's Cyber and Terror Response Product. Prior to joining Starr Companies in 2010, Gibbs worked for Business Executives for National Security (BENS) as well as served as an infantry officer in the U.S. Marine Corps. He holds Master of Arts degrees from Georgetown University and the University of Kentucky, and a Bachelor of Arts degree from The Citadel.



David Norfleet



Reggie Gibbs

COMPANY BRIEF *Starr Companies (starrcompanies.com), is a global, privately held insurance and investment organization. Through its operating insurance companies, Starr Companies provides commercial property and casualty, and accident and health insurance products worldwide. Starr Companies underwrites a wide variety of specialty and international lines including aviation, marine, energy, environmental, crisis management, excess casualty insurance, accident and health, and political risk insurance. Starr Companies also provides a broad spectrum of insurance-related services, including claims handling and settlement, reinsurance, risk assessment, loss control, and worldwide travel assistance service.*

■

“Our product provides a blend of first-party and third-party casualty insurance coverage for incidents resulting from cyber-attacks, workplace violence, political violence, and terrorism.” – Reggie Gibbs

■



■

“We have contracted with highly regarded experts to support our clients with post-event crisis response, ensuring that in the event of a claim, they can restore business operations as soon as possible.” – David Norfleet

■

How is Starr addressing the emerging threats related to cyber-attacks, political violence, terrorism, and workplace violence?

Reggie: We recently introduced CYBER & TERROR RESPONSE, a new offering that provides an integrated solution for middle-market businesses. This new offering is designed to enhance existing general liability and/or property policies by covering security-related perils that severely impact, interrupt, and/or damage businesses’ physical locations, operations, and employees.

Our product provides a blend of first-party and third-party casualty insurance coverage for incidents resulting from cyber-attacks, workplace violence, political violence, and terrorism.

In addition, the policy also provides post-event services that may be necessary to help a business restore operations following a covered event such as crisis counseling, medical care, public relations, security analysis, and advisory services.

Will you tell us more about the crisis response services that are part of the offering? What happens after the claim?

Reggie: We have two crisis consultants that we retain. One is an expert in “hard security” measures (force protection, active security guards) and cyber extortion. Starr has worked with this agency for a very long time with some of our other product lines and they are truly first-in-class. This responder would manage any type of physical security issues. They would

also handle any cyber extortion issues since much of what they do is manage data breaches. They would provide security following an event and be there to assist the client with minimizing further damage.

For example, we may deploy certified crisis responders who, after an incident of workplace violence, have the experience and ability to respond to support a company’s staff and business.

We have another consultant that specializes in public relations and crisis communication. Following an insured event, this responder would be there to help the insured communicate with family members and relatives. They would help them get psychiatric care and help them manage any type of medical fallout from the event. The two crisis consultants work together.

■

“This Cyber & Terror Response product is evidence of our listening to trends and the needs of the market. We are the first company to put something this comprehensive in the market. This product and the introduction of it is a good example of the responsiveness and flexibility that Starr exhibits.” – Reggie Gibbs

■



■

“Political violence & terrorism and workplace violence are becoming part of the proactive conversation because of the increased incidents in the U.S.” – David Norfleet

■

David: Another important point is that we will provide not just the reactive component of crisis management but also the proactive avoidance planning as well.

On the cyber side, we don't have a loss control service per se, but we have a list of reliable vendors we can provide clients. There isn't just a single service these companies need. There are various items they could utilize to build their information security posture. These could range from security assessments to ensuring compliance with PCI or HIPPA, or the various regulatory agencies.

This could be something really basic, like help with developing a business continuity plan or an incident response plan. We can provide templates for them and point them to vendors that can help with those as well.

The scope of pre-breach services that a client may be looking for can vary tremendously depending on the client's level of sophistication and need. Some companies don't have as much confidential information as others, so their needs may differ depending on their exposures.

But we are able to provide them with a host of vendors that can provide those services.

Is it typical for insurance policies to have service agreements included?

David: We believe that our consulting services are unique. We have contracted with highly regarded experts to support our clients

with post-event crisis response, ensuring that in the event of a claim, they can restore business operations as soon as possible.

You are combining three seemingly unrelated risks into one product. Why?

David: For us, it is perfectly clear. It is about security and restoring operations for our clients.

Reggie: Yes, and in terms of terrorism and workplace violence, these exposures are related. Looking at some of the recent incidents, be it the Orlando nightclub, San Bernardino, or the church shootings in Charleston, S.C., these incidents were perpetrated by individuals proclaiming allegiance to – but not “officially” a member of – known extremist organizations. In the San Bernardino shooting, the perpetrator was actually an employee. So, in standard terrorism or workplace violence insurance, coverage may have been denied because of the ambiguity. With our Cyber & Terror Response coverage, there is no question. All of these incidents would have been added.

David: The two areas Reggie discusses relate to physical security; cyber coverage relates to information security. At day's end, in terms of the clients we're targeting, an information security event can be as big of a crisis as a workplace violence incidence from a financial standpoint.

It might not be a matter of life or death, but it could be a matter of whether a business ends

up keeping their door open or suffers financially to the point where they can no longer be in business.

For example, cyber extortionists could gain access to a network and demand a certain amount of money or they will shut the system down. They might be able to afford one extortion attempt but when the second and third show up, it may prevent the company from being able to bounce back quickly or, in some cases, at all. Our coverage is there to help keep this from happening.

It's very important to talk about the services that the product comes with. For example, clients have a crisis consultant accessible to them as part of this product. This is important for smaller insureds that are less able to bounce back from the financial repercussions of dealing with a cybersecurity event.

There is significant attention on cyber exposure. Tell us more about the risks businesses face today.

David: Middle market companies often underestimate their cyber exposure and risk. There are, in fact, bad actors targeting these businesses and they need the same level of protection as larger companies.

When a breach occurs, costs are incurred fairly rapidly. Those can include: hiring a forensics investigator for a security failure; legal consultants to advise on ensuring compliance with the

■

“...our Cyber & Terror Response product provides [small to mid-sized companies] coverage that is both comprehensive, accessible and affordable.” – Reggie Gibbs

■



■

**“Cyber is now a boardroom conversation, a C-suite conversation
and a risk management conversation.” – David Norfleet**

■

various state and federal laws that surround privacy; providing credit monitoring or simply notifying affected individuals; hiring computer experts to determine whether there has been any damage to the insured's software or network. These costs could be devastating to a small to mid-size business. Not only do we provide coverage for that, but we also coordinate the services.

The second component that would follow these types of events would be third-party lawsuits. Our program has a third-party liability component that would address lawsuits from consumers or potential vendors that may have lost information as a result of our insured's data breach.

The last component is coverage to address extortion threats which, unfortunately, are occurring on a more frequent basis. We see small to mid-size businesses being extorted for more modest amounts of money than the larger companies, and on a more frequent basis. Our policy covers the cost to handle that extortion threat as well as the actual extortion cost.

Those are the three categories that we cover within this Cyber & Terror Response policy.

Why have you decided to focus on the middle-market customers?

Reggie: While many large corporations in the United States can afford and have access to cyber or political violence/terrorism coverages, many middle-market companies, particularly those located outside large metropolitan

regions, have not had access to this level of protection. For them, our Cyber & Terror Response product provides coverage that is comprehensive, accessible, and affordable.

How do you define middle-market customers?

Reggie: We generally define the middle market as around \$10 million to \$400 million in annual revenue, but we are willing to explore clients outside of this segment as well.

Are there any other things that make Starr unique in its approach?

Reggie: The approach we take is one based on flexibility and service. We listen to the needs of the broker community, which are always reflected in the insurance products we offer.

This Cyber & Terror Response product is evidence of our listening to trends and the needs of the market. We are the first company to put something this comprehensive in the market. This product and the introduction of it is a good example of the responsiveness and flexibility that Starr exhibits.

David: On the cyber side, Mr. Greenberg has taken a very personal interest in the initial development of the product in 2014, when we introduced our first primary product. Dating back to 2009, we have been writing cyber on an excess basis. He's very involved in everything we create, and very well-versed in the product and in what is going on around the world.

In addition to Mr. Greenberg, Starr has some of the best industry talent, some with over 30 years of underwriting expertise, those who have been part of the industry from when the coverage was in its infancy, a simple extension of a technology E&O product to today's stand-alone product, crisis program, D&O program, and as part of the Cyber & Terror Response program that we just introduced.

At the company level, who should be evaluating and looking at this coverage?

David: Cyber is now a boardroom conversation, a C-suite conversation, and a risk management conversation. It is a proactive conversation rather than a reactive one. Fortunately, and as a start, many IT directors have been brought in as part of the C-suite and now have direct contact with the CEO and CIO. This has led to greater cyber discussions at the executive level and it has become an even higher concern based on all the incidents they have recently read about in the press. Political violence and terrorism and workplace violence are becoming part of the proactive conversation because of the increased incidents in the U.S. It's not a conversation that anyone likes to have but it's being recognized as a conversation that is necessary for the C-Suite level with risk managers driving the discussion. That's why we believe that risk management should be an active and proactive discussion in all corporations large and small. ●

■

**“...covering security-related perils that severely impact, interrupt, and/or damage
businesses' physical locations, operations, and employees.” – Reggie Gibbs**

■