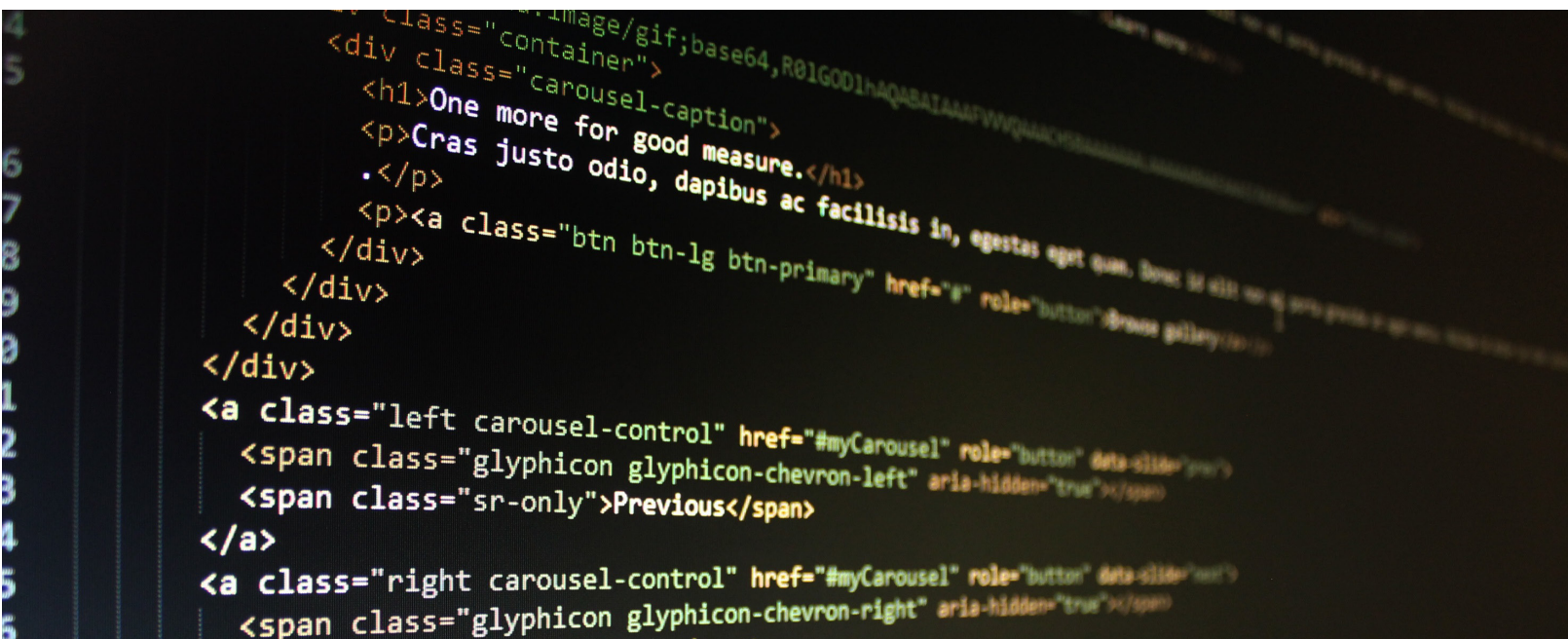




COLLIER

Security Solutions



THE SURGING THREAT OF CYBERCRIME

the cost of vulnerability

A new generation of highly sophisticated cyberthreats is wreaking havoc worldwide for private and government organizations— not only in the damage they cause, but in costs.

In the first six months of 2017, two major cyberattacks hit computer networks around the world, closing hospitals, government offices, and manufacturing plants. Experts estimate global ransomware damage costs alone will exceed \$5 billion in 2017—up from \$325 million just two years ago.

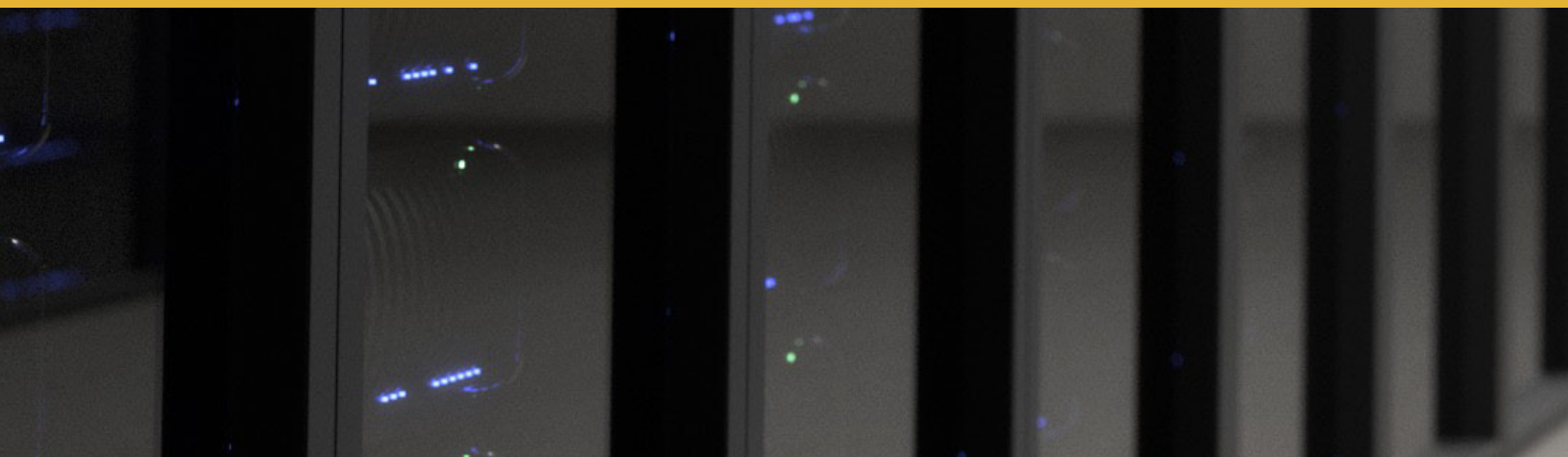
When you mix in the different forms of risks—malicious malware, insider threats, data theft, and other forms of advanced espionage, the total cost of global cybercrime, according to Cybersecurity Venture, will reach \$6 trillion annually by 2021. That staggering number is double the estimate of \$3 trillion just two years ago.



With 25 years of experience engineering and protecting information technology, Collier is well aware of the damage data compromise can inflict. Collier and its partners deliver cybersecurity defenses that create a fortress around your most sensitive data in a way that is sustainable, covers your organization's endpoints, and is powered by visibility, a high-speed response, and streamlined cost.

Our chosen partner analysts have spent hundreds of thousands of hours each year responding to intrusions and data breaches. "We chose our partners by evaluating which companies are called upon for breach response. Those companies are uniquely qualified to put that knowledge back into preventive intelligence," says company president, Steve Collier.

Collier's security defenses are based on a revolutionary intelligence platform that not only simplifies but fully integrates into your existing system. While no solution is foolproof, the platform provides advanced intelligence matched with context and analytics that helps your organization prevent breaches; contain malware; catch SPAM, phishing and viruses; and in the end, reduce overall costs.



MINIMIZING THE RISK

creating a fortress around your assets

When Collier reviews a client's cyber needs, it examines them from every security angle. Our obsession for exploring information technology challenges from multiple dimensions gives us entirely new perspectives with new solutions.

Collier's commitment is to educate clients on all forms of threats to networks and endpoints from thieves, hackers, and even the potential for advanced and persistent risks from state-sponsored espionage.

As Collier engages a customer, it provides a strategic roadmap that outlines top priorities, including:

MAPPING and understanding the client's entire network, including security rules and limitations.

APPLYING and updating the best practices to keep security systems running smoothly.

FORTRESSING "crown jewels"—the data most critical to operations and the organization's economic well-being.

PROVIDING a more holistic view of threat analysis to detect what others miss.

HUNTING for threats strategically by applying behavioral analytics to identify unusual activities.

PROVIDING, jointly with its partners, full incident response (IR) management and technical advice in the event of an attack.

As cyber criminals and freelance hackers create more advanced weapons, prevention and security become even more critical. Collier's security operations support gives a unified, coordinated posture that is critical to lowering the risk of breaches, stopping intrusions in their tracks, and ultimately reducing the overall cost of protecting your organization.