What Is the Future of Security Incident Response?

An interview with CyberSponse CEO Joseph Loomis

With the common theme in today's security management conversations being "your security will fail" and "expect to be breached," there's no question that there has been increased interest in the area of incident response. The industry is realizing that the addition of regulations, people, or even product features, is not going to cut it - a next generation incident response offering is needed.

To get a view of what the next-generation incident response solution might look like, Web Security Journal sat down with entrepreneur and life-long incident response veteran, Joseph Loomis, a cooperative member with the FBI and DEA's divisions on Cybercrime and founder and CEO of Phoenix-based CyberSponse.

WSJ: Tell us a little bit about yourself - why does incident response interest you enough to start a company that appears to be all IR all the time?

Joseph Loomis: The desire to help people and businesses in need is in my bones. In fact, my experience with incident response goes all the way back to my childhood days when my father and his friends saw a gap in community protection and emergency "incident" response, and in turn created an entirely new fire department for our town. What I saw was that most people aren't aware that nearly every medical emergency - even if not fire related - is responded to by the fire department. My father and his friends came up with their own incident response program - they saw the need and made it a reality. They took the bull by the horns, figured it out, and worked on it until they got it right. Watching them, I repeatedly got to see how people responded during traumatic/chaotic events.

Like my father, I too served six years in the military, an experience that allowed me to help individuals, organizations, and countries alike. Shortly after completing my service with the armed forces and attending the University of Florida for Electrical Engineering, I was working for an electronics manufacturer in California. While working as the director of engineering, I saw the need for businesses to protect their assets in the online world. In response to this need, I founded NetEnforcers, a company chartered with protecting online brands and intellectual property. After successfully growing the company and securing customers like Apple, Microsoft, Cisco, Samsung, LG and Pfizer, I sold NetEnforcers, both debt-free and very profitable. Soon after, I began to look for the next area where I could help the world become a better place. As a formally licensed Private Investigator and a cooperative member with the FBI & DEA's divisions on Cybercrime, I have been fortunate to connect with other entrepreneurs and security industry experts that share the same goals as I do. In 2011, I looked to Spyro Malaspinas, a proven, trusted, and innovative information security leader and a long time friend, to partner with me as a co-founder for CyberSponse - a Phoenix-based company chartered with helping organizations successfully respond to the inevitable security breach. Together Spyro and I developed the business case that would make CyberSponse a reality.

WSJ: What do you see as the biggest challenge faced by organizations with respect to security incident response?

Loomis: As you can imagine, my exposure to fire response, medical response, and military response presented me with far worse situations than a firewall breach. It's safe to say that these experiences taught me how to remain calm under pressure, to recognize how important planning is, and to appreciate how critical communication is during a crisis. Relating this back to cybersecurity, I find the biggest challenge in IR is having the right information available to the right people on the IR team at the right time, and being able to communicate and collaborate throughout the entire response process.

For example, most IR programs involve the use of panicky conference calls and drawn-out email communications, both of which seem to get in the way when something really serious is happening. If you haven't been through it, it may be hard for you to understand. But think about it for a minute - speed of communication is critical during an incident. Even if the right people are included in an email thread, if the critical person is not looking at their email program when it really matters, something can get missed. Similarly, oftentimes the IR leads don't have a clear view of who's doing what and when, regardless of the communication methods used.
WSJ: If you were to pick one big thing that has to change for IR, what would that be?
Loomis: Collaborative communication. The problem is that most IR personnel only know the email/conference call method to incident response. The improvement of standard IR methods needs to be the focus of organizations. In my mind, this is exactly where IR necessitates transformation. New methods of communication need to be leveraged; we need to move things from an ad-hoc model where organizations are forced to jump the tracks, to a cohesive experience that enables teams to communicate and collaborate. We could look to "The Computer Incident Response Planning Handbook" by Neal K McCarthy as a starting point for how to begin this transformation as it is a great source for what works during IR..

WSJ: What prompted you to tackle these challenges with your founding of CyberSponse?
Loomis: I know from first-hand experience that leadership, coordination, communication, planning, and collaboration are key elements to controlling a chaotic situation. Reaching out to old friends that were familiar with security, Spyro included, we decided to form CyberSponse. After digesting the business model and vetting it and the technology plans with some great contacts in the security world, I elected to personally invest over what will be 2M when we hit the market. Our founding management team has been developed through a close network of experienced and trusted friends and partners. And, rather than building an engineering team from the ground up, we looked to a development genius who already had an experienced and functional team, Paul Janisko. He quickly joined the march, and right from the start, we found ourselves with a solid plan, a solid team, and a solid solution to a problem that is not going away. We are well positioned to succeed and intend to make CyberSponse a reality very soon, a reality that will change the face of IR forever, a reality that will seen by the world at the upcoming launch at RSA 2013 in San Francisco.

WSJ: How will CyberSponse shape the future of incident response?
Loomis: While our solution is far from simple to develop, simply put, CyberSponse is going to bring the efficiency, economics, transparency, and analytics that IR has needed for a long time. No more relying solely on ticketing systems, no more conference calls lasting 6 hours, no more meetings to have meetings. The CyberSponse solution has been tailored to handle the future of IR, designed specifically to streamline the use of a variety of technologies such as SMS, instant messaging, secure document collaboration, and mobile (to name a few). One example I can share pre-launch is that the CyberSponse system will offer built-in tools and training which will help teams become more prepared for a breach when it occurs. Also, by partnering with cutting edge providers like FireHost, Carbon Black, and Blackhills InfoSec, CyberSponse is going to put the power of IR back in the hands of the IR team in a way they’ve never experienced before, giving them the ability to respond with confidence from wherever they are.

WSJ: What does the future hold for CyberSponse?
Loomis: Legacy technologies like email and ticketing systems are holding the IR teams back, forcing them to operate outside even the best laid out IR plans. In fact, best practices such as NIST SP800-61 and ISO-27035 call for organizations to stay out of email when an incident occurs - not use it as the main tool for communication. With several patents pending, this is the future for CyberSponse - we will bring the IR teams up to date with a next generation IR solution so they can actually follow industry standards, guidelines, regulations, and more - while becoming more effective and efficient in their IR programs while doing so. CyberSponse will provide the perfect solution for companies small and large, leveraging a cyber-response community we help build where companies help each other fight cyber-crime and respond to cyber-attacks.

The final thought that I would add with respect to standards and regulations is the IR audit trail. CyberSponse, effectively operating as a secure bunker for all IR activities, will keep track of everything IR related and keep it secure within the bunker. Organizations will be able to see and report on what Resource A did and what Resource B forgot to do - even if one of those resources is an external service provider bound to an IR SLA. This will be an auditors dream - and will help the organization improve upon future IR activities.