CSO
FROM IDG

What it takes to be a

security incident responder

THINKSTOCK

What it takes to be a **security incident responder**

A wide range of **technical skills** and **curiosity** about the mechanics and goals are key for effective incidence response.

BY BOB VIOLINO

CYBER SECURITY RESPONSE teams are keeping busy these days, with an abundance of hacking and other attacks launched against organizations on a regular basis. The professionals who make up these teams are skilled in evaluating and responding to such attacks in a timely manner and can minimize damage for organizations.

"The demand for cyber security incident responders remains high," says Debbie Henley, president and co-founder of Redbud, an information security recruitment firm. Two of every three placements by Redbud are either directly or indirectly related to filling an incident response role. "When an organization reaches out to us it's normally because they are struggling to find qualified professionals on their own," she says.

Driving the demand is not only the increase in cyber criminal activity, but the fact that more organizations are realizing the need and are rushing to fill out—or start in many cases—their cyber defense teams, Henley says. "With a global cyber security workforce shortage of 1.5 million projected unfilled roles by 2020, incident responders [are] a big part of that," Henley says. "The shortage is staggering."

Outsourcing of incident management is certainly a viable security approach, Henley says. "Based on the requests Redbud receives for incident responders, it appears that about 65 percent of incident response management is handled in house, so it is certainly a mix," she says.

The skills needed for a quality incident responder can be categorized into two main groups: personal skills and technical skills. "The greater one's technical skills, the better the incident responder," Henley says.

Among the desirable skills are a good grasp of basic security principles such as confidentiality, authentication, access control and privacy; security vulnerabilities; physical security issues; protocol design flaws; malicious code; implementation flaws; configuration weaknesses and user errors or indifference.

Responders should also know about the Internet of Things (IoT), risk management, network protocols, network applications and services, malicious code, programming skills and intruder techniques.

IT security professionals who become leaders or members of response teams sometimes take circuitous routes to these positions. For example, Rob Sherman, director of incident management at packaged bakery foods provide Flowers Foods, originally sought to work as an administrator for Unix and Windows operating systems.

While attending Mt. Vernon Nazarene college as a business administration and computer science major, Sherman quickly found out that he wasn't interested in a programming career, so he put his degree on hold. Sometime after Sherman decided to complete a management degree in business at Wilmington College, and later "fell into" a job as a computer forensic investigator at financial services

firm GE Capital in 2006, eventually becoming chief forensic investigator.

Among Sherman's responsibilities were to lead his team on analysis and recovery from multiple incidents, conducting digital forensic analysis and electronic discovery. While working in this position, he obtained a masters degree in digital forensic management at Champlain College.

Among Sherman's responsibilities were to lead his team on analysis and recovery from multiple incidents, conducting digital forensic analysis and electronic discovery.

"If you think of an MBA mixed with legal courses, compliance courses and digital forensic courses, that is what that degree was," Sherman says. He received a second masters degree, in digital forensic science, to show prospective employers that he was not "just a manager," but a technical contributor as well.

"When I was going through my second masters degree, many of my friends asked me, 'Why would you get a second degree?'" Sherman says. "They also pointed out that it won't make me any more money. I didn't complete my second masters degree for more money, or recognition. I did it for myself."

Working in the IT field taught Sherman that technology is constantly changing, that within six months what was new is now old. "Well, I believe that cyber security puts that to shame," he says. "There is always a new threat, new vulnerability, a new indicator of compromise."

As a child, Sherman had a deep curiosity about how things worked, "That eventually morphed into an analytical mindset," he says. Once he began working he kept wondering about how things worked. He wanted to know how IT departments and administrators worked and what they did.

In 2011, he joined General Electric as a senior cyber investigator. In this post, he learned about the need to keep digging for information when responding to incidents. "This has solidified my work ethic in both digital forensics as well as incident response," Sherman says.

Shortly after that, Sherman joined NASA's Glenn Research Center as incident response manager. There his team addressed internal and external threats, and assisted with security projects as well.

CAREER PROFILE

Security incident responder

CORE KNOWLEDGE | Authentication, access control, security vulnerabilities, physical security issues, protocol design, malicious code, implementation flaws, configuration weaknesses and user errors or indifference

POTENTIAL EMPLOYERS | Any company starting or growing a cyber defense team, security services outsourcing firms

NATIONAL MEDIAN SALARY | **$70,589** (according to Payscale)

He updated senior leadership on technical areas, and worked closely as a "coach" among security specialists, he says.

As response manager, Sherman gathered meaningful metrics for senior leadership, providing a monthly "gap analysis" to the threats being addressed. With this information, his team was able to secure the environment further for the protection of NASA. In 2016, Sherman began his current position at Flower Foods, where he oversees security incident management.

"Protecting to a fire fighter may be teaching fire safety, or training, or learning new tools. The same can be said with incident response for protection. Thinking on your feet, using tools, having an incident commander, and bringing in the right response in a timely fashion all fall within incident response."

–ROB SHERMAN, DIRECTOR OF INCIDENT MANAGEMENT, FLOWERS FOODS

One of Sherman's most important criteria for where to work is the level of importance the organization places on cyber security. "If the leadership of the organization does not have a focus on security, it becomes an uphill battle from the start," he says.

Throughout his career progression, Sherman has done what is necessary to reach a director of incident management role. "I have learned many technologies [since] the beginning of my career, and slowly morphed into what I believe is a 'coaching leader' style," he says. "When I work with my team I believe it is as important to lead as well as dig in when necessary."

Sherman had worked as a fire fighter early on, which he says set the stage for his roles as an incident responder. "I used my fire-fighting skills to mimic incident response," Sherman says. "A fire fighter's main duty is to protect. Protecting to a fire fighter may be teaching fire safety, or training, or learning new tools. The same can be said with incident response for protection. Thinking on your feet, using tools, having an incident commander, and bringing in the right response in a timely fashion all fall within incident response."

Mentors have played a key role in Sharman's career. One is Curtis Rose, owner of Curtis W. Rose & Associates, a provider of computer forensics and litigation services. "Curtis taught me how to think differently, and to really have a strong work ethic," Sherman says. "One of the key lessons he taught was to understand what made 'it' tick. If something occurred on a computer, understand what made it occur, how did got there, and why it got there."

As investigations can take various turns during their progression, Rose "time and again has brought me back to basics," Sherman says. "In my opinion [having someone to talk with] is one of the most important aspects of being in digital forensics/incident response."

Although Sherman is not currently pursuing another degree, he is constantly learning. For example, he takes SANS Institute courses that are non-vendor specific security training. "I have always stated that my security mantra is 'you don't know what you don't know,'" he says. "This is why I have a strong circle of colleagues and friends in cyber security, part of multiple organizations, and continually teach myself something new."

Sherman says his number one professional goal is always to protect others. "Protecting others may simply mean protecting a person's data," he says. "Protecting that data means protecting their job, and the organization's or company's best interest. My future career goal is to continually strive to be a better investigator, a leader that others want to follow."

And what's Sherman's personal goal? "To take a well-deserved vacation," he says. ■