Getting to Know Tom Powledge, Vice President of Cisco Managed Security Services

After more than six months leading the Managed Security Services portfolio at Cisco, Tom sat down with the social media team to discuss his path to Cisco, the evolution of the security market, and the future of security.

Q: After nearly 20 years at Symantec, why did you decide to move to Cisco?

TP: Cisco has all of the pieces necessary to solve the biggest security problems facing businesses today and into the future. Cisco's position in the network, its broad security product portfolio, its strong and continued investment in security, and its pivot toward driving business outcomes and solving customer problems place this company in a unique position to lead the charge toward the next generation of security. Looking at the fastest growing segments of security, such as network security and managed security, Cisco is strong in those areas and is moving in the right direction to align with evolving customer needs.

On a personal level, I was thrilled to have the opportunity to work in such an innovative group. As a part of a company that builds the cloud, mobility, collaboration, and Internet of Everything technologies driving change in the security market, we have a unique opportunity to proactively build security services that enable the secure adoption of these innovations. Our ability to integrate with networking technologies and all types of connected devices allows us to feed huge amounts of data from across an entire customer network into our big data platform for detecting, investigating, and analyzing threats. This level of innovation signifies the next generation of security, so it's a really exciting position to be in. I'm eager to take what I've learned throughout 19 years in security and put that knowledge and experience to work in building up Cisco's resources into a next-level suite of managed security services.

I see firsthand how genuine Cisco is in serving customers as a strategic partner. I knew coming in that Cisco had that reputation, but I didn't appreciate the depth of Cisco's relationships with customers and the lengths we go to understand and solve their challenges. Cisco really is serious about developing resources to equip customers to attain their business outcomes – we don't just build things to sell, we look for problems to solve.

Q: You mention Cisco's alignment with the major growth areas in security – how has the security landscape evolved since you started out and what are the big trends moving forward?

TP: When I started working in security in '96, security revolved around viruses and protection at the endpoint. Viruses infected individual computers through hardware. The Blaster worm, Melissa, Nimda, Code Red – these threats that were out there in the early 2000s were developed by kids in their basements. Today, the actors producing threats aren't just individuals hacking as a hobby. They are complex organizations sponsored by nation-states or criminal enterprises that are hacking for commercial gain. Hacking is a business now, and we have to view adversaries as sophisticated organizations: they have access to resources, they are hierarchical, they do R&D. The level of sophistication has surpassed anything we would have predicted 20 years ago.

Q: How has the increasing sophistication of hacker operations impacted the security market?

TP: Sophisticated threats require even more sophisticated tools for detection and defense. The reality is that breaches are inevitable. It's no longer primarily a question of prevention (although that is still important), but of detection and response. Every organization will experience a breach – so how quickly can you identify it, plug the gap, assess the damage, and secure your perimeter? Like diseases, not all threats are preventable, but diagnosing them quickly and treating them effectively is the best way to reduce risk and ensure the continued health of your network. The demand for these tools is resulting in huge growth in network security and managed security as organizations look for help. That's another one of the reasons I was attracted to this opportunity, because Cisco is investing in managed security at the right time and in the right ways to be an innovative leader in the market for next-generation security resources.

Q: How are these market shifts affecting individual organizations?

TP: Moving forward, security is now a board-level issue. Three or four years ago, security was on the radar for IT leaders, but it didn't have the visibility it has now. A growing list of high-profile cybersecurity breaches have caused corporate boards and CEOs to take notice of the damage that hacking activity can inflict on a business. Security is now a #1 concern for organizations and governments all around the world. As more devices connect to the internet, the variety of attack surfaces and level of complexity will increase. There will be more things to secure and more things to worry about. Organizations are really struggling to keep up with the pace of change. They can't do it alone – not with the rapid development of new technologies and the huge amount of fragmentation in the security market.

Q: How does your understanding of these market and threat trends influence your strategy for steering Cisco Managed Security Services?

TP: Our strategy is to serve our customers' emerging and underserved needs. Most [managed security service providers (MSSPs)] focus on providing outsourced task management. We do that, too – and we do it well – but our priority is building solutions that will help solve our customers' biggest problems, and not simply replacing their operations. Our first step is to listen to the customer, and then we work to alleviate their pain and enable them to take advantage of new business opportunities. For example, organizations of all types are struggling to detect threats quickly and accurately. They spend huge amounts of time wading through long lists of alerts trying to figure out which are legitimate and which are false positives. So, we designed a service that uses big data analytics to weed out false positives and confirm a limited number of high-fidelity incidents with great accuracy and detail. As a result, the customer is able to manage risk appropriately, act quickly to resolve threats, and reallocate resources from monitoring activities to core business initiatives.

Q: What is the value of a service like this beyond traditional security measures like security information and event management (SIEM)?

TP: It is incredibly difficult and costly for individual organizations to develop and maintain these types of capabilities internally. The reality is that SIEM technology just doesn't cut it anymore – the threat landscape is evolving so quickly that technology alone can't keep up. You need to harness the wealth of data coming through the network and through security technologies to get ahead of the curve. Cisco has deep expertise on and roots in the network, so we can access huge amounts of data and analyze activity over the entire network to find and investigate anomalies. The proliferation of endpoints introduces a growing variety of attack vectors hackers can manipulate, but these devices are also sources of information for us. The more data we can harness, the more power our big data tools have to pinpoint malicious activity. We can leverage that information to hunt out threats quickly, accurately, and proactively. That's why big data analytics are so critical for security. We are oriented toward solving the problems of the future, and we are developing solutions for threat detection, identity, and other major security areas that will continue to increase in importance as the Internet of Everything becomes a reality.

Q: What excites you the most about the work you do in managed security services?

TP: Solving our customers' problems. They genuinely need help with security, and we can do it. We can provide them with the right combination of technologies and services to help them be successful. I'm excited about working for a company that has the resources necessary to make headway in this tough security climate. Cybersecurity and information security is also immensely important on a societal level. Security really matters – to individuals who need to protect their bank accounts, to businesses holding sensitive information, and to governments securing critical infrastructure. For 20 years, that's what has always kept me going in security and what has always been exciting: I've always felt a sense of purpose in my work knowing that what I am working on really matters and will really help people.

Tom Powledge is Cisco's vice president of Managed Security Services. Prior to his current role, Powledge served as vice president of Symantec's Information Security Group, where he was responsible for the strategy, development and delivery of the information security product portfolio and managed services. Powledge has more than 17 years of experience in the software industry and is a graduate of Harvard Business School and the University of California, Santa Barbara. In his spare time, Tom travels with his family and participates in triathlons.

Follow Tom's blog to learn more about his vision for the future of managed security services.

For more information and resources on Cisco's entire portfolio of managed security services, please visit the Managed Security Services homepage.