CISCO EXECUTIVE PERSPECTIVE

‘Smarter Defenses’

“Thanks to the tireless ingenuity of cyber-criminals, the IT threat is arriving in the boardroom. As data and applications move to the cloud, mobile transactions are becoming routine and bring-your-own-device demand is surging. To keep their assets and information safe, security professionals have to rethink their strategies,” says Christopher Young, Senior Vice President for Security and Government at Cisco.

Gone are the days when building a firewall was enough to ward off security attacks. The network perimeter as we once knew it no longer exists. It’s been erased by fast-moving developments in mobility and cloud. Today’s Generation Y expects to use third party applications and social media at work on any device, at any time and in any location.

The challenges may look much the same. We’re still trying to prevent intrusions and stop the theft of valuable company data or intellectual property. We still need strong defense consisting of next generation firewalls, policy and access control, secure virtual private networks, and email gateways. The three pillars of basic IT security haven’t changed either: first, keep would-be intruders out. Second, maintain sensitive detection and alert capabilities in case someone does get in; and third, if an attack happens, remediate it quickly to neutralize or contain the damage.

Yet cybercrime is evolving at a phenomenal rate. Any-to-any communication opens up a larger surface to attack, while business use of employee devices and third party applications creates new vulnerabilities. Networks of freelance hackers are poised to sneak in through the gaps. They operate underground offering specialist skills, malicious code, and price lists, along with customized services by negotiation.

The traditional bad guys looking for an easy payday are not the sole perpetrators. In the latest Cisco security report, we found the main sources of malware were not criminal sites or porn sites. Business and industry sites were among the top three categories where malware encounters happened, and they were 21 times more likely to occur on a consumer shopping site than a criminal one. Thieves like crowds. So it’s no surprise that they head for the busiest places online, link their malware to popular topical newsfeeds, and make heavy use of malvertising.

The security landscape is ever-changing. Of countries commonly identified as sources of cyber-attack, China has slipped down in the rankings (from second place in 2011 to sixth in 2012) while Denmark and Sweden moved up to third and fourth respectively. However, the top spot was again taken by the US.

Cyber-criminals and hacktivists continue to reshape their methods. They focus on exploiting research programs, launching tightly targeted spam campaigns, and putting their strongest efforts into developing malicious scripts and iFrames that are often found on trusted web pages. Take the case of the Mandiant Intelligence Center, a US-based research organization. In 2013, it published a report tracing a history of cyber-attacks on 140 US organizations to a People’s Liberation Army unit in Shanghai. The claim was hotly denied by the Chinese Ministry. Within days, virus-laden versions of the same document were circulating.

Getting your strategy right

If that’s a snapshot of how things look now, where will we be in three years? Cloud computing is here to stay and it complicates IT security. How can organizations enforce effective security policy if they don’t actually own and operate the data centers? In what way can even basic security be applied? The answer lies in a multitude of places: virtualized applications, bring-your-own-device (BYOD) policy, social enterprise platforms and, of course, in the cloud itself.

One thing seems clear. IT teams simply won’t have time to manage security policy and access control manually. Especially when you consider that data center traffic globally is expected to quadruple in the next five years, and cloud traffic is its fastest-growing component, with a forecast six-fold increase.

In this environment, services may reside in many clouds, making data harder to manage and control. A single vulnerability in a third party or

open source solution could impact many systems and have a dramatic effect on the business. For example, should hypervisors running virtualized workloads become compromised, there's a risk of a mass hacking or hyperjacking situation that could affect many organizations–all at the same time.

Employees using their own smartphones or tablets at work add another dimension. Although a third of millennial workers say they don't mind employers tracking their behavior online, less than half say their organizations take up the offer. On the flip-side, 90 percent of IT professionals prohibit non-work browsing on company devices, but more than a third say employees don't comply.

The primary concern is uncontrolled browsing leading to back door entry to corporate networks. And there have even been reports of a more stealth-like secondary threat, where pre-infected devices have been shipped to unwitting individuals who become assailants without knowing it. Once in the office, these devices can be quickly used for remote video and eavesdropping purposes.

Big data too multiplies the vectors of potential attack. Conversely, it could also provide a key defense by virtue of the sophisticated, comprehensive analytics it generates. Indeed, it's the Cisco view that one of the most important tools to handle security risks in the new environment is big data itself, leading to improved alerting and overall response.

The Cisco View

In 2012, nine billion devices and an estimated 50 billion other things were interconnected; by 2020, the count is set to reach 13.3 trillion. IPv6 means an exponential further rise in connectivity, as the Internet of Things evolves into the Internet of Everything. Like a planetary nervous system, this vast fabric will embrace people and processes ubiquitously–at work, at home, at play. Network intelligence points the way to the convergence, visibility, and orchestration that will help keep cyber-attacks at bay.

To a non-specialist, today's IT security agenda might look like the seemingly impossible task of building a fortified castle without walls. Everything is in constant motion: people work from home or on the move, over multiple devices, on different networks, using a wide array of virtualized applications from outside the firewall, and valuable business data streams back and forth among private, public, and hybrid clouds. So where does one draw the line?

It goes without saying that hardware and software must be kept up-to-date. Beyond that, for Cisco, the answer involves multiple elements. Above all, today it's an issue of identity assurance. This baseline control must be transferrable across any device or network. And it needs to be much more than traditional authentication and authorization. To be effective, identity management must be equipped with precise contextual awareness that can detect and respond to small but possibly significant changes.

Suppose you have an employee working on a tablet over a public Wi-Fi network in a coffee shop somewhere. You'll want to protect that employee's tablet from becoming infected in this public place and then being brought on to the corporate network to do more damage. This requires granular network policies to verify the user, the device posture, the access network and the context to determine whether to allow access and which types of information or parts of the corporate network to make available. User, device, and network behavior all need to be monitored for anomalous modes.

This huge mass of data is continually uploaded and processed, using advanced algorithms engineered to detect non-typical behavior patterns and, when found, trigger automatic alerts and initiate remediation measures if needed.

Cloud-based security

A variety of proactive measures and automation are the keys to mastering these new world security challenges. Cisco's customers and partners upload around 100 terabytes of data every day, which is analyzed within Cisco's Security Intelligence Operations. Using a cloud-based threat intelligence approach, we can assimilate telemetry information coming from multiple tracks – all at once. Situational awareness and automated analytics software sniff out anomalies and inform the management and policy layer. This is a smart, self-evolving security framework that extends the same benefits to everyone in the ecosystem.

The upshot of cloud-based security is that it now takes us just minutes to update our customer's entire infrastructure, compared to a day or so for some of our competitors. Security updates can be propagated to other organizations within minutes, too. Within a single given day Cisco blocks over 320 million attacks.

Remember, once malicious code has made its way in and is at work inside your defenses, a day is ample time for it to inflict far-reaching and, maybe, long-lasting damage on the business. So, we hope you'll join us in the formidable challenge of building a new security armory in our shared battle against cybercrime.

With endpoints and data proliferating, we face a common threat. We need to pool knowledge and collaborate because security will increasingly come down to real-time intelligence sharing and collective response. Let's work at staying safe.