# As Cyber-Attacks Grow, So Do Defenses

## Service providers look to shore up all parts of the network

BY CRAIG KUHL

Few companies in the cable and telecommunications industries have escaped the cyber attacks that continue to wreak havoc on just about every layer of the supply chain.

Varying degrees of security breaches at Comcast, Cox Communications, Time Warner Cable and other cable providers have raised the red flag in the cybersecurity space and prompted a new mantra: Now is the time to raise the level of security.

**TAKEAWAY**

As Internet protocol-driven networks become a bigger piece of cable's technology puzzle, cybersecurity concerns are growing.

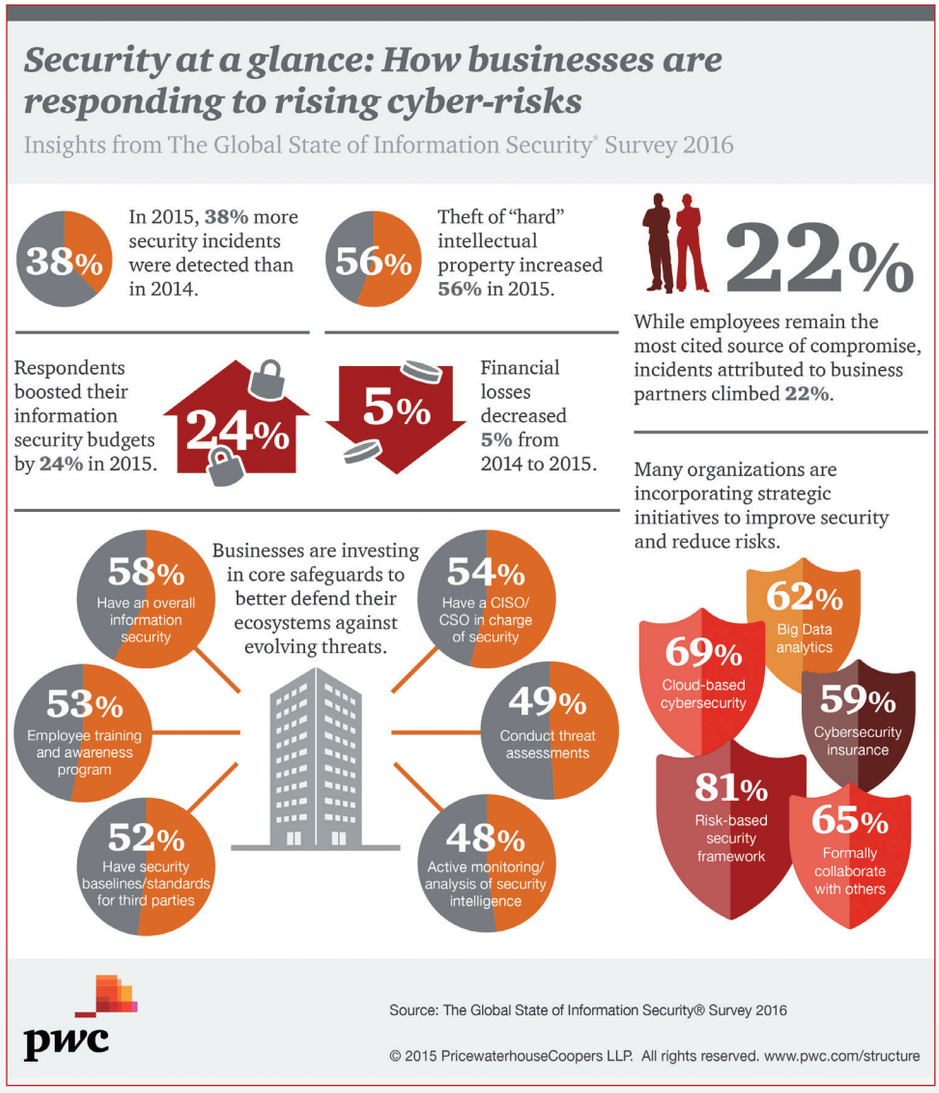
"A fundamental evolution is taking place and the security implications are numerous," Michela Menting, research director at consulting firm ABI Research, said. "Above all are the issues raised by the transition to all-[Internet protocol] networks, which are already highly exploited by threat actors and will be a boon for malicious cyber-agents — and all sectors are vulnerable.

"Investment in security services and corresponding hardware and software is not something they can ignore or put off, except at great cost to their services, reputation and client base," she said.

Cybersecurity concerns have become so paramount that in its Charter Communications-Time Warner Cable merger order, the Federal Communications Commission required Charter to submit a plan to manage its increasing security risks during the transition.

And according to the Hewlett Packard Enterprise/Ponemon Institue "2015 Cost of Cyber Crime" study, hacking attacks cost U.S. firms, on average, some $15.4 million a year. Globally, U.K. insurance firm Lloyds estimates that cyber-attacks are costing businesses a staggering $400 billion a year.

There's also the shaken confidence of clients and subscribers about the safety of their data. And not everyone is convinced the cable industry is prepared for any attacks.




"Cable networks are archaic in many respects, as they extend the life of existing systems, and frankly, the security posture of networks and the less time spent on security leads to a lot of holes," Chris Simkins, CEO and co-founder of supply chain analysis and risk management firm Chain Security, said.

PricewaterhouseCoopers (PwC), a consultancy moving deeper into the cybersecurity space, believes cable companies are getting the message that shoring up their networks should be of the highest priority.

"There's a lot going on with MSOs and we're seeing the awareness lev-

el rising," Mark Lobel, a principal in PwC's U.S. advisory practice and Cybersecurity Technology, Information, Communications & Entertainment leader, said. "But cybersecurity is like a chess game with no kings, and trying to stay ahead of who's across the board."

And just who is across the board?

"There are many threat vectors," Irfan Saif, a principal in Deloitte's Cyber Risk Services practice, said. "There are service-disruption actors, those looking at the backbone to propagate malware and those who want to compromise customers. It's a broad range of threat actors and companies must be cognizant of them all."

"It's one thing that cable is carrying 60% of the Internet traffic, but now there are data centers and multiple services with different touch points in cable."

RICK MICHAELS, CEA

That will require a holistic approach, Saif noted. "You must understand what behavior is considered normal and what indicates a threat of attack and what are the crown jewels that require higher-grade protection."

Cisco Systems, another player in the cybersecurity space, concurred with Saif's assessment.

"The best approach is a holistic look at security and where each layer builds on top of each other — firewalls, advanced malware protection, email and core technologies like conditional access, DRM and anti-piracy technology — a breadth of security," Cisco senior product and solutions marketing manager Sam Rastogi said.

Another less glamorous threat, but just as dangerous, comes from the inside.

"Employees or vendors with access to information is a growing concern," Rastogi sad. "Who's accessing information and how, and is there abnormal activity? A risk-based program with alerts, authentication measures and more will give companies more insight."

CableLabs, the cable industry's research and development consortium, is accelerating its cybersecurity activity with two initiatives: It's working with the Wi-Fi Alliance to ensure links to hotspot access points are secure, and it's reaching more deeply into home managed access points.

"The level of engagement is very high and there are real questions being asked," The mindset is changing," CableLabs principal security architect Steve Goeringer said.

That's a good thing, said Rick Michaels, CEO of CEA, a cable industry-focused investment bank. "It's one thing that cable is carrying 60% of the Internet traffic, but now there are data centers and multiple services with different touch points in cable. Cybersecurity should be of paramount interest to the cable industry."

Most cable companies are understandably reluctant to discuss their cybersecurity strategies. Comcast, which in March hired Noopur Davis as senior vice president of product security and privacy, offered a statement from Myrna Soto, senior vice president and global chief information security officer: "We've committed extensive resources with a focus on risk management and built resilient and smarter networks with many security layers that are monitored continuously. Using automation, tooling and analytics is key."

Arris, another key equipment supplier to cable networks, said in a statement (in part): "Security remains a top priority at Arris, as it does for all manufacturers of Internet and network-connected devices" and that it "employs a variety of protective measures to help ensure the safe and reliable operation of our devices including, but not limited to, DOCSIS compliance, vulnerability scanning, and monitoring programs." It works "actively with security organizations and our service provider customers to identify and quickly resolve any potential vulnerabilities to protect the subscribers who use our CPE devices."

Breaches cut across both residential and business markets, added Sander Smith, president of Sericon Technology.

"It's clear that very soon we'll see consumers filling their home networks with IoT devices, and these devices will be rushed to market with very little thought given to security."

"Prior security strategies depended on physical walls and isolated networks. They have become irrelevant with video being driven by IP."

STEVE CHRISTIAN, VERIMATRIX

Yet even with the increase in cyber attacks (PwC reported a 38% increase in 2015 vs. 2014), there is cautious optimism that with emerging cybersecurity innovations, an expanding community of cybersecurity companies and a heightened awareness among service providers, security is being strengthened.

"We're seeing various levels of maturity in cable and telecom and a raising of awareness in those organizations," PwC's Lobel said. "But they can't lose focus."

The National Cable & Telecommuications Association is focusing its cybersecurity attention on two areas, senior vice president, science and technology and chief technology officer Bill Check said.

"We are leading the industry's Cybersecurity Working Group and working with the FCC's Communications Security, Reliability and Interoperability Council (CSRIC), along with various cybersecurity-related working groups," he said. "The challenge is to anticipate current and future threats and design systems of early detection and resistance, because cyber-criminals will always look for new exploits."